Part No. 060762-10, Rev. A
December 2021

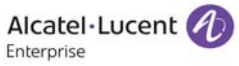
OmniSwitch 2260, 2360 AOS Release 5 CLI Reference Guide

AOS 5.1R2

Alcatel·Lucent Enterprise

www.al-enterprise.com

This user guide documents AOS Release 5.1R2
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: myportal.al-enterprise.com
Email: ebg_global_supportcenter@al-enterprise.com

Contents

BLANK PAGE

About This Guide

This *OmniSwitch 2260, 2360 AOS Release 5 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 2260
- OmniSwitch 2360

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.

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, if applicable:

- 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.

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”**

Related Documentation

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

- *OmniSwitch 2x60 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 2260, 2360 AOS Release 5 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 2260,2360 AOS Web/Configuration 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).

- 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:myportal.al-enterprise.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 duplex** **interfaces alias** **clear interfaces** **interfaces max-frame-size** **interfaces flood-limit** **interfaces flood-limit action** **interfaces ingress-bandwidth** **interfaces pause** **interfaces link-trap** **interfaces ddm** **interfaces ddm-trap** **interfaces eee** **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 transceivers** **show violation**
Interface violation commands	**violation recovery-maximum** **violation recovery-time** **violation recovery-trap** **show violation** **show violation-recovery-configuration** **clear violation**
Time Domain Reflectometry (TDR) commands	**interfaces tdr** **show interfaces tdr-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 | disable}	Enables or disables administrative state.
autoneg {enable | disable}	Enables or disables auto negotiation.
epp {enable | disable}	*Enhanced Port Performance (EPP) is not supported.*

Defaults

parameter	default
enable | disable	enable

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- If auto negotiation is disabled, auto MDIX, flow control, auto speed, and auto duplex are not accepted.
- 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, 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 5.1; command introduced.

Related Commands

interfaces speed	Configures interface speed.
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	*This parameter is not supported.*
10000	*This parameter is not supported.*
40000	*This parameter is not supported*.
100000	*This parameter is not supported*.
2000	*This parameter is not supported*.
4000	*This parameter is not supported*.
8000	*This parameter is not supported*.
max 100	Sets the maximum speed to 100 Mpbs.
max 1000	Sets the maximum speed to 1000 Mbps (1 Gigabit).
max 4000	*This parameter is not supported*.
max 8000	*This parameter is not supported*.

Defaults

parameter	default
auto	enable

Platforms Supported

OmniSwitch 2260, 2360

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 5.1; command introduced.

Related Commands

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

MIB Objects

```
esmConfTable
   esmPortCfgSpeed
```

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 2260, 2360

Usage Guidelines

- You can only configure one slot at a time. Repeat the command to configure additional slots.
- 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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

Usage Guidelines

- 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 5.1; command introduced.

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 2260, 2360

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 5.1; command introduced.

Related Commands

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

MIB Objects

```
esmConfTable
   esmPortCfgMaxFrameSize
```

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 2260, 2360

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 5.1; command introduced.

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

Not supported in this release.

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**".
- For the parameter **flood-limit uucast**, only "**default**" action is supported.

Examples

```
-> interfaces port 1/1/1 flood-limit bcast action shutdown
-> interfaces port 1/1/4 flood-limit 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 5.1; command not supported.

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 2260, 2360

Usage Guidelines

N/A

Examples

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

Release History

Release 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command introduced.

Related Commands

show interfaces ddm	Displays the interface DDM status.

MIB Objects

```
ddmConfiguration
   ddmTrapConfig
   ddmNotificationType
```

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 2260, 2360

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 5.1; command introduced.

Related Commands

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

MIB Objects

N/A

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command 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 2260, 2360

Usage Guidelines

N/A

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           : N/A
  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 is 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. *Not supported in this release.*
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.
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).

output definitions (continued)

Inter Frame Gap	Inter-packet gap (in Bytes). *Not supported in this release.*
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 5.1; command introduced.

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command introduced.

Related Commands

interfaces	Configures interface line speed, sets speed, and duplex mode to auto-sensing.
interfaces duplex	Configures interface duplex mode.

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 2260, 2360

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 5.1; command introduced.

Related Commands

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

MIB Objects

```
esmConfTable
   esmPortCfgAutoNegotiation
   esmPortCfgFlow
   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 2260, 2360

Usage Guidelines

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

Examples

```
-> 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 5.1; 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
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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command introduced.

Related Commands

interfaces ingress-bandwidth	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 2260, 2360

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 5.1; 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 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 2260, 2360

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-xxG-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-xxG-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-xxG-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 5.1; 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 2260, 2360

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.
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 5.1; 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 2260, 2360

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 5.1; 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 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 2260, 2360

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 5.1; command 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 2260, 2360

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) **Short** - 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 5.1; command 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
```

BLANK PAGE

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 priority-disconnect
lanpower power-rule
lanpower power-policy
lanpower class-detection
lanpower capacitor-detection
lanpower usage-threshold
lanpower update-from
lanpower fpoe
lanpower ppoe
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 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 enabled by default.

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

N/A

Examples

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

Release History

Release 5.1; command introduced.

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 enabled by default.

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

N/A

Examples

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

Release History

Release 5.1; command introduced.

Related Commands

lanpower service	Activates or stops PoE service on all ports in a specified slot.
show lanpower slot	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 **show lanpower slot** command output.

Defaults

N/A

Platforms Supported

OmniSwitch 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; command introduced.

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

N/A

Platforms Supported

OmniSwitch 2260, 2360

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 5.1; command introduced.

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 2260, 2360

Usage Guidelines

N/A

Examples

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

Release History

Release 5.1; command introduced.

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 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 2260, 2360

Usage Guidelines

N/A

Examples

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

Release History

Release 5.1; command introduced.

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 2260, 2360

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 5.1; command 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 2260, 2360

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 2-14.
- 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 5.1; command 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 2260, 2360

Usage Guidelines

- 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 5.1; command introduced.

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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; command introduced.d.

Related Commands

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

MIB Objects

```
pethMainPseTable
   pethMainPseUsageThreshold
```

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 2260, 2360

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 5.1; command introduced.

Related Commands

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

MIB Objects

N/A

lanpower fpoe

Enables fast PoE functionality.

lanpower {slot *chassis/slot*} **fpoe {enable | disable}**

Syntax Definitions

chassis/slot	The slot on which to enable or disable fast PoE.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- Fast PoE can be used to provide PoE power within a few seconds after powering on the chassis.
- Factory default switches that don't have any PoE configuration must have an initial PoE configuration completed.
- The PoE configuration cannot be modified until the switch is up and the PoE module is completely initialized.
- LLDP-based PoE devices will not function as expected until the switch has completed its bootup and the switch is in a state to respond to LLDP requests.
- When Fast PoE is enabled the vcboot.cfg should not be deleted or manually edited.
- If Fast PoE is disabled all PDs will reset due to the PoE controller having to be reconfigured.
- FPGA/CPLD upgrade may be required. Refer to the release notes.

Examples

```
-> lanpower slot 1/1 fpoe enable
```

Release History

Release 5.1; command introduced.

Related Commands

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

MIB Objects

```
alaPethMainPseTable
   alaPethMainPseFastPoE
```

lanpower ppoe

Enables perpetual PoE functionality.

lanpower {slot *chassis/slot*} **ppoe {enable | disable}**

Syntax Definitions

chassis/slot	The slot on which to enable or disable perpetual PoE.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- This feature allows the switch to provide uninterrupted power to connected power device (PD) even when the switch is rebooting.
- When Perpetual PoE is enabled the vcboot.cfg should not be deleted or manually edited.
- FPGA/CPLD upgrade may be required. Refer to the release notes.

Examples

```
-> lanpower slot 1/1 ppoe enable
```

Release History

Release 5.1; command introduced.

Related Commands

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

MIB Objects

```
alaPethMainPseTable
   alaPethMainPsePerpetualPoE
```

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 2260, 2360

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 2-19 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 5.1; command introduced.

Related Commands

N/A

MIB Objects

```
alaPethPsePortPowerActual
alaPethPsePortPowerMaximum
alaPethPsePortPowerStatus
pethPsePortPowerPriority
pethPsePortAdminEnable
pethPsePortPowerClassifications
```

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 2260, 2360

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 2-14 for more information.
Power	The PoE power status assigned to the rule. Refer to page 2-14 for more information.
At HH:MM	The time of day the power rule takes effect. Refer to page 2-14 for more information.

output definitions (continued)

Day-of-Week	The day of the week the power rule takes effect. Refer to page 2-15 for more information.
Month-of-Year	The month of year the power rule takes effect.Refer to page 2-15 for more information.
Timezone	The timezone under which the power rule takes effect. Options include **local-server**, **originator-server** and **utc**. Refer to page 2-15 for more information.

Release History

Release 5.1; command 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 2260, 2360

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 5.1; command 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 2260, 2360

Usage Guidelines

- 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 5.1; command introduced.

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 2260, 2360

Usage Guidelines

N/A

Examples

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

Release History

Release 5.1; command introduced.

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 2260, 2360

Usage Guidelines

N/A

Examples

```
-> show lanpower slot 1/1 priority-disconnect
Chas/Slot priority-disconnect
---------+-------------------
  1/1     enable
```

Release History

Release 5.1; command introduced.

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 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 2260, 2360

Usage Guidelines

N/A

Examples

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

Release History

Release 5.1; command introduced.

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

Not supported in this release.

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 5.1; command 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 2360

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 5.1.R2; 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 2360

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 5.1.R2; 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 2360

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 5.1.R2; 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 2360

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 5.1.R2; 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 2360

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 5.1.R2; 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 2360

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 5.1.R2; 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 2360

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 5.1.R2; 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 2360

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 5.1.R2; 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 2360

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 5.1.R2; 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 2360

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 5.1.R2; 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 2360

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 5.1.R2; 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
```

BLANK PAGE

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 2260, 2360

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.

Examples

```
-> mac-learning port 1/1/2 enable
-> mac-learning linkagg 10 disable
-> mac-learning vlan 10 disable
```

Release History

Release 5.1; command introduced.

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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; 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.
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 2260, 2360

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 5.1; command introduced.

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 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 8, "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 2260, 2360

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 5.1; command introduced.

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 8, "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 2260, 2360

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 5.1; command introduced.

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 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 8, "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 2260, 2360

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 5.1; command introduced.

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

Not supported in this release.

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 5.1; 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
```

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. *Not supported in this release.*
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 2260, 2360

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


 Total MAC Address In Use  = 34

-> show mac-learning
Legend: Mac Address: * = address not valid,

        Mac Address: & = duplicate static address,

Domain Vlan                      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
Total number of Valid MAC addresses above = 34
```

output definitions

Domain	The domain in which the MAC address was learned or statically configured
Vlan	This field contains one of the following values depending on the domain type associated with the MAC address: • The VLAN ID number.
Mac Address	MAC address that is currently learned or statically assigned.
Type	MAC address management status (**dynamic, static).**

output definitions

Operation	The disposition of the MAC address (**bridging**, **filtering**).
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 5.1; command introduced.

Related Commands

show mac-learning domain vlan	Displays MAC Address Table information for the VLAN 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
```

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 2260, 2360

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

 Total MAC Address In Use  = 16

-> show mac-learning domain all
Legend: Mac Address: * = address not valid,

        Mac Address: & = duplicate static address,

Domain Vlan                    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

Total number of Valid MAC addresses above = 16
```

output definitions

Domain	The domain in which the MAC address was learned or statically configured (**VLAN)**.
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.
Mac Address	MAC address that is currently learned or statically assigned.
Type	MAC address management status (**dynamic, static).**
Operation	The disposition of the MAC address (**bridging**, **filtering**).
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 5.1; 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 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 2260, 2360

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 5.1; command introduced.

Related Commands

show mac-learning	Displays Source Learning MAC Address Table information for the switch.
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 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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
```

BLANK PAGE

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**

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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
```

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.

Release History

Release 5.1; command introduced.

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 2260, 2360

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 5.1; 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
```

BLANK PAGE

6 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 2260, 2360

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 5.1.R2; command introduced.

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 2260, 2360

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 5.1.R2; command 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.

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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command introduced.

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 2260, 2360

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 5.1.R2; command introduced.

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 2260, 2360

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 5.1.R2; command introduced.

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 2260, 2360

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 5.1.R2; command 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 2260, 2360

Usage Guidelines

N/A

Examples

```
-> clear loopback-detection statistics port 1/1/2
```

Release History

Release 5.1.R2; command 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
```

BLANK PAGE

7 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 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**

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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.

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
spantree vlan mode	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 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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    Note
-----+-------+------------+---------+-------+------
    1   1/1/1      DIS           0    DIS
    1   1/1/2      DIS           0    DIS
    1   1/1/3      DIS           0    DIS
    1   1/1/4      DIS           0    DIS
    1   1/1/5      DIS           0    DIS
    1   1/1/6      DIS           0    DIS
    1   1/1/7      DIS           0    DIS
```

```
    1   1/1/8      DIS           0    DIS
    1   1/1/9      DIS           0    DIS
    1  1/1/10      DIS           0    DIS
    1  1/1/11      DIS           0    DIS
    1  1/1/12      DIS           0    DIS
    1  1/1/13      DIS           0    DIS
    1  1/1/14      DIS           0    DIS
    1  1/1/15      DIS           0    DIS
    1  1/1/16      DIS           0    DIS
    1  1/1/17      DIS           0    DIS
    1  1/1/18      DIS           0    DIS
    1  1/1/19      DIS           0    DIS
    1  1/1/20      DIS           0    DIS
    1  1/1/21      DIS           0    DIS
    1  1/1/22      DIS           0    DIS
    1  1/1/23     FORW           4   DESG
    1  1/1/24     FORW           4   ROOT
    1  1/1/25      DIS           0    DIS
    1  1/1/26      DIS           0    DIS
    1  1/1/27      DIS           0    DIS
    1  1/1/28      DIS           0    DIS
    1    0/10      DIS           0    DIS

-> spantree protocol mstp
WARNING: Changing to MSTP(802.1s) resets flat bridge priority and path
WARNING: Changing to MSTP(802.1s) resets flat bridge priority and path

-> show spantree ports
 Msti  Port   Oper Status  Path Cost  Role    Note
-----+-------+------------+---------+-------+------
    0   1/1/1      DIS             0    DIS
    0   1/1/2      DIS             0    DIS
    0   1/1/3      DIS             0    DIS
    0   1/1/4      DIS             0    DIS
    0   1/1/5      DIS             0    DIS
    0   1/1/6      DIS             0    DIS
    0   1/1/7      DIS             0    DIS
    0   1/1/8      DIS             0    DIS
    0   1/1/9      DIS             0    DIS
    0  1/1/10      DIS             0    DIS
    0  1/1/11      DIS             0    DIS
    0  1/1/12      DIS             0    DIS
    0  1/1/13      DIS             0    DIS
    0  1/1/14      DIS             0    DIS
    0  1/1/15      DIS             0    DIS
    0  1/1/16      DIS             0    DIS
    0  1/1/17      DIS             0    DIS
    0  1/1/18      DIS             0    DIS
    0  1/1/19      DIS             0    DIS
    0  1/1/20      DIS             0    DIS
    0  1/1/21      DIS             0    DIS
    0  1/1/22      DIS             0    DIS
    0  1/1/23     FORW         20000   DESG
    0  1/1/24     FORW         20000   ROOT
    0  1/1/25      DIS             0    DIS
    0  1/1/26      DIS             0    DIS
    0  1/1/27      DIS             0    DIS
    0  1/1/28      DIS             0    DIS
    0    0/10      DIS             0    DIS
```

```
-> spantree mode per-vlan
-> show spantree ports
 Vlan  Port   Oper Status  Path Cost  Role   Note
-----+-------+------------+---------+-------+------
    1   1/1/1      DIS             0    DIS
    1   1/1/2      DIS             0    DIS
    1   1/1/3      DIS             0    DIS
    1   1/1/4      DIS             0    DIS
    1   1/1/5      DIS             0    DIS
    1   1/1/6      DIS             0    DIS
    1   1/1/7      DIS             0    DIS
    1   1/1/8      DIS             0    DIS
    1   1/1/9      DIS             0    DIS
    1  1/1/10      DIS             0    DIS
    1  1/1/11      DIS             0    DIS
    1  1/1/12      DIS             0    DIS
    1  1/1/13      DIS             0    DIS
    1  1/1/14      DIS             0    DIS
    1  1/1/15      DIS             0    DIS
    1  1/1/16      DIS             0    DIS
    1  1/1/17      DIS             0    DIS
    1  1/1/18      DIS             0    DIS
    1  1/1/19      DIS             0    DIS
    1  1/1/20      DIS             0    DIS
    1  1/1/21      DIS             0    DIS
    1  1/1/22      DIS             0    DIS
    1  1/1/23     FORW             4   DESG
    1  1/1/24     FORW             4   ROOT
    1  1/1/25      DIS             0    DIS
    1  1/1/26      DIS             0    DIS
    1    0/10      DIS             0    DIS

-> show spantree ports forwarding
 Vlan  Port   Oper Status  Path Cost  Role   Note
-----+-------+------------+---------+-------+------
    1  1/1/23     FORW             4   DESG
    1  1/1/24     FORW             4   ROOT
```

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**.
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 5.1; 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
```

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 2260, 2360

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 for Cist
      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.
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.

```
-> show spantree cist ports configured
Spanning Tree Port Admin Configuration for Vlan 0
        Port  Adm Man. Config  Adm  Adm  Aut  Rstr  Rstr Role/
Port    Pri   St. Mode   Cost  Cnx  Edg  Edg  Tcn   Root Guard
------+----+----+----+-------+----+----+----+----+-----------+
 1/1       7  ENA  No        0  AUT   No  Yes   No      No
 1/2       7  ENA  No        0  NPT   No  Yes   No      No
 1/3       7  ENA  No        0  NPT   No  Yes   No      No
 1/4       7  ENA  No        0  NPT   No  Yes   No      No
 1/5       7  ENA  No        0  NPT   No  Yes   No      No
```

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 5.1; 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 2260, 2360

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     Note
-----+-------+------------+---------+-------+------
    0    1/1/1       DIS              0     DIS
    0    1/1/2       DIS              0     DIS
    0    1/1/3       DIS              0     DIS
    0    1/1/4       DIS              0     DIS
    0    1/1/5       DIS              0     DIS
    0    1/1/6       DIS              0     DIS
    0    1/1/7       DIS              0     DIS
    0    1/1/8       DIS              0     DIS
    0    1/1/9       DIS              0     DIS
    0   1/1/10       DIS              0     DIS
    0   1/1/11       DIS              0     DIS
    0   1/1/12       DIS              0     DIS
    0   1/1/13       DIS              0     DIS
    0   1/1/14       DIS              0     DIS
    0   1/1/15       DIS              0     DIS
    0   1/1/16       DIS              0     DIS
    0   1/1/17       DIS              0     DIS
    0   1/1/18       DIS              0     DIS
    0   1/1/19       DIS              0     DIS
    0   1/1/20       DIS              0     DIS
    0   1/1/21       DIS              0     DIS
    0   1/1/22       DIS              0     DIS
    0   1/1/23      FORW          20000    ROOT
    0   1/1/24       DIS              0     DIS
    0   1/1/25       DIS              0     DIS
    0   1/1/26       DIS              0     DIS
    0   1/1/27       DIS              0     DIS
    0   1/1/28       DIS              0     DIS

-> show spantree msti ports forwarding
 Msti   Port    Oper Status   Path Cost   Role     Note
-----+-------+------------+---------+-------+------
    0   1/1/23      FORW          20000    ROOT
```

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 Status	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.

output definitions (continued)

Role	The role of the port for this Spanning Tree instance. Possible port roles are: **root, designated, alternate, master**, and **backup**.
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.

```
-> show spantree msti 0 ports
Per Vlan Spanning Tree is enforced !! (Per VLAN mode)
INACTIVE Spanning Tree Parameters for Cist
      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
```

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 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.
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 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.
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.

```
-> show spantree msti 0 ports configured
Spanning Tree Port Admin Configuration for Vlan 0
        Port  Adm Man. Config  Adm  Adm  Aut  Rstr  Rstr Role/
Port    Pri   St. Mode   Cost  Cnx  Edg  Edg  Tcn   Root Guard
------+----+----+----+-------+----+----+----+----+-----------+
 1/1       7  ENA  No        0  AUT   No  Yes   No      No
 1/2       7  ENA  No        0  NPT   No  Yes   No      No
 1/3       7  ENA  No        0  NPT   No  Yes   No      No
 1/4       7  ENA  No        0  NPT   No  Yes   No      No
 1/5       7  ENA  No        0  NPT   No  Yes   No      No

-> spantree mode flat
-> show spantree msti 1 ports configured
Spanning Tree Port Admin Configuration for Msti 1
        Port  Adm Man. Config  Adm  Adm  Aut  Rstr  Rstr Role/
Port    Pri   St. Mode   Cost  Cnx  Edg  Edg  Tcn   Root Guard
------+----+----+----+-------+----+----+----+----+-----------+
 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/Root Guard	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 5.1; 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
   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 2260, 2360

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   1/1/1      DIS             0    DIS
    1   1/1/2      DIS             0    DIS
    1   1/1/3      DIS             0    DIS
    1   1/1/4      DIS             0    DIS
    1   1/1/5      DIS             0    DIS
    1   1/1/6      DIS             0    DIS
    1   1/1/7      DIS             0    DIS
    1   1/1/8      DIS             0    DIS
    1   1/1/9      DIS             0    DIS
    1  1/1/10      DIS             0    DIS
    1  1/1/11      DIS             0    DIS
    1  1/1/12      DIS             0    DIS
    1  1/1/13      DIS             0    DIS
    1  1/1/14      DIS             0    DIS
    1  1/1/15      DIS             0    DIS
    1  1/1/16      DIS             0    DIS
    1  1/1/17      DIS             0    DIS
    1  1/1/18      DIS             0    DIS
    1  1/1/19      DIS             0    DIS
    1  1/1/20      DIS             0    DIS
    1  1/1/21      DIS             0    DIS
    1  1/1/22      DIS             0    DIS
    1  1/1/23     FORW             4   DESG
    1  1/1/24     FORW             4   ROOT
    1  1/1/25      DIS             0    DIS
    1  1/1/26      DIS             0    DIS
    1    0/10      DIS             0    DIS
```

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 Status	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.
Role	The role of the port for this Spanning Tree instance. Possible port roles are: **root, designated, alternate, master**, and **backup**.
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.

```
-> show spantree vlan 1 ports
Spanning Tree Port Admin Configuration for Vlan 1
        Port  Adm Man. Config  Adm  Adm  Aut  Rstr  Rstr Role/
Port    Pri   St. Mode   Cost  Cnx  Edg  Edg  Tcn   Root Guard
-------+----+----+----+-------+----+----+----+----+-----------+
  1/1/1    7  ENA  No        0  AUT   No  Yes   No      No
  1/1/2    7  ENA  No        0  AUT   No  Yes   No      No
  1/1/3    7  ENA  No        0  AUT   No  Yes   No      No
  1/1/4    7  ENA  No        0  AUT   No  Yes   No      No
  1/1/5    7  ENA  No        0  AUT   No  Yes   No      No
  1/1/6    7  ENA  No        0  AUT   No  Yes   No      No
  1/1/7    7  ENA  No        0  AUT   No  Yes   No      No
  1/1/8    7  ENA  No        0  AUT   No  Yes   No      No
  1/1/9    7  ENA  No        0  AUT   No  Yes   No      No
 1/1/10    7  ENA  No        0  AUT   No  Yes   No      No
 1/1/11    7  ENA  No        0  AUT   No  Yes   No      No
 1/1/12    7  ENA  No        0  AUT   No  Yes   No      No
 1/1/13    7  ENA  No        0  AUT   No  Yes   No      No
 1/1/14    7  ENA  No        0  AUT   No  Yes   No      No
 1/1/15    7  ENA  No        0  AUT   No  Yes   No      No
 1/1/16    7  ENA  No        0  AUT   No  Yes   No      No
 1/1/17    7  ENA  No        0  AUT   No  Yes   No      No
 1/1/18    7  ENA  No        0  AUT   No  Yes   No      No
 1/1/19    7  ENA  No        0  AUT   No  Yes   No      No
 1/1/20    7  ENA  No        0  AUT   No  Yes   No      No
 1/1/21    7  ENA  No        0  AUT   No  Yes   No      No
 1/1/22    7  ENA  No        0  AUT   No  Yes   No      No
 1/1/23    7  ENA  No        0  AUT   No  Yes   No      No
 1/1/24    7  ENA  No        0  AUT   No  Yes   No      No
 1/1/25    7  ENA  No        0  AUT   No  Yes   No      No
 1/1/26    7  ENA  No        0  AUT   No  Yes   No      No
   0/10    7  ENA  No        0  AUT   No  Yes   No      No

-> 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
-------+----+-------+-------+----+-------+---+---+-----------------------+------
 1/1/23 FORW       4       8 DESG  1/1/23 PTP  NO   8000-94:24:e1:55:85:29
 1/1/24 FORW       4       4 ROOT  1/1/24 PTP  NO   8000-00:d0:95:ec:78:30

-> 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
-------+----+-------+-------+----+-------+---+---+-----------------------+------
 1/1/10  DIS       0       0  DIS  1/1/10  NS  NO   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
-------+----+-------+-------+----+-------+---+---+-----------------------+------
 1/1/14  DIS       0       0  DIS  1/1/14  NS  NO   0000-00:00:00:00:00:00
 1/1/15  DIS       0       0  DIS  1/1/15  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
-------+----+-------+-------+----+-------+---+---+-----------------------+------
 1/1/20  DIS       0       0  DIS  1/1/20  NS  NO   0000-00:00:00:00:00:00
 1/1/21  DIS       0       0  DIS  1/1/21  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
------+----+-------+-------+----+-------+---+---+-----------------------+------
 1/1/26  DIS       0       0  DIS  1/1/26  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 (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.
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.

```
-> show spantree vlan 1 ports configured
Spanning Tree Port Admin Configuration for Vlan 1
        Port  Adm Man. Config  Adm  Adm  Aut  Rstr  Rstr Role/
Port    Pri   St. Mode   Cost  Cnx  Edg  Edg  Tcn   Root Guard
------+----+----+----+-------+----+----+----+----+-----------+
  1/1/1    7  ENA  No        0  AUT   No  Yes   No       No
  1/1/2    7  ENA  No        0  AUT   No  Yes   No       No
  1/1/3    7  ENA  No        0  AUT   No  Yes   No       No
  1/1/4    7  ENA  No        0  AUT   No  Yes   No       No
  1/1/5    7  ENA  No        0  AUT   No  Yes   No       No
  1/1/6    7  ENA  No        0  AUT   No  Yes   No       No
  1/1/7    7  ENA  No        0  AUT   No  Yes   No       No
  1/1/8    7  ENA  No        0  AUT   No  Yes   No       No
  1/1/9    7  ENA  No        0  AUT   No  Yes   No       No
 1/1/10    7  ENA  No        0  AUT   No  Yes   No       No
 1/1/11    7  ENA  No        0  AUT   No  Yes   No       No
```

```
 1/1/12     7  ENA  No         0  AUT   No  Yes   No       No
 1/1/13     7  ENA  No         0  AUT   No  Yes   No       No
 1/1/14     7  ENA  No         0  AUT   No  Yes   No       No
 1/1/15     7  ENA  No         0  AUT   No  Yes   No       No
 1/1/16     7  ENA  No         0  AUT   No  Yes   No       No
 1/1/17     7  ENA  No         0  AUT   No  Yes   No       No
 1/1/18     7  ENA  No         0  AUT   No  Yes   No       No
 1/1/19     7  ENA  No         0  AUT   No  Yes   No       No
 1/1/20     7  ENA  No         0  AUT   No  Yes   No       No
 1/1/21     7  ENA  No         0  AUT   No  Yes   No       No
 1/1/22     7  ENA  No         0  AUT   No  Yes   No       No
 1/1/23     7  ENA  No         0  AUT   No  Yes   No       No
 1/1/24     7  ENA  No         0  AUT   No  Yes   No       No
 1/1/25     7  ENA  No         0  AUT   No  Yes   No       No
 1/1/26     7  ENA  No         0  AUT   No  Yes   No       No
   0/10     7  ENA  No         0  AUT   No  Yes   No       No

-> 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/
Port    Pri   St. Mode   Cost  Cnx  Edg  Edg  Tcn   Root Guard
-------+----+----+----+-------+----+----+----+----+-----------+
 1/1/10     7  ENA  No         0  AUT   No  Yes   No       No
Spanning Tree Port Admin Configuration for Vlan 11
        Port  Adm Man. Config  Adm  Adm  Aut  Rstr  Rstr Role/
Port    Pri   St. Mode   Cost  Cnx  Edg  Edg  Tcn   Root Guard
-------+----+----+----+-------+----+----+----+----+-----------+
 1/1/14     7  ENA  No         0  AUT   No  Yes   No       No
 1/1/15     7  ENA  No         0  AUT   No  Yes   No       No
Spanning Tree Port Admin Configuration for Vlan 12
        Port  Adm Man. Config  Adm  Adm  Aut  Rstr  Rstr Role/
Port    Pri   St. Mode   Cost  Cnx  Edg  Edg  Tcn   Root Guard
-------+----+----+----+-------+----+----+----+----+-----------+
 1/1/20     7  ENA  No         0  AUT   No  Yes   No       No
 1/1/21     7  ENA  No         0  AUT   No  Yes   No       No
Spanning Tree Port Admin Configuration for Vlan 13
        Port  Adm Man. Config  Adm  Adm  Aut  Rstr  Rstr Role/
Port    Pri   St. Mode   Cost  Cnx  Edg  Edg  Tcn   Root Guard
-------+----+----+----+-------+----+----+----+----+-----------+
 1/1/26     7  ENA  No         0  AUT   No  Yes   No       No
```

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.
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 mode** command.

output definitions (continued)

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.

Release History

Release 5.1; 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 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 2260, 2360

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	*Not supported in this release.*
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 auto-vlan-containment	Enables or disables Auto VLAN Containment (AVC).

Release History

Release 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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
```

8 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 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**
Static and dynamic	**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	*This parameter is not supported.*
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	*This parameter is not supported*.
destination-ip	Selects the destination IP hashing option.
source-and-destination-ip	Selects the source IP and destination IP hashing option.
tunnel-protocol	*This parameter is not supported*.

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 2260, 2360

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.
- 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
```

Release History

Release 5.1; command introduced.

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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	*This parameter is not supported.*
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	*This parameter is not supported.*

destination-ip	Selects the destination IP hashing option.
source-and-destination-ip	Selects the source IP and destination IP hashing option.
tunnel-protocol	*This parameter is not supported.*

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 2260, 2360

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.
- Use the **linkagg static agg size** command to create static aggregate groups. See page 8-3 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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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	Enabled

Platforms Supported

OmniSwitch 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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	Enabled
timeout enable	Enabled

Platforms Supported

OmniSwitch 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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
   alclnkaggAggPortPartnerAdminSystemPriority
```

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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
```

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 2260, 2360

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
```

output definitions

Number	The aggregate group number.
Aggregate	The type of aggregate group (**Static**, **Dynamic)**.
SNMP Id	The SNMP ID associated with the aggregate group.
Size	The number of links in this aggregate group.
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.

output definitions (continued)

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
```

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.
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.

output definitions (continued)

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.
Name	The name of this dynamic aggregate group. You can modify this parameter with the **linkagg lacp agg name** command (see page 8-15).
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 8-18).
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.

output definitions (continued)

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 8-23).
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 8-21).
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 8-20).
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 8-25).
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 8-27).
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 8-29).
Partner Oper Key	The operational key of the remote system to which the dynamic aggregation group is attached.

Release History

Release 5.1; 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 2260, 2360

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 8-38).
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 8-36).
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 8-31).
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 8-47).
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 8-43).
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 8-45).
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 8-49).
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 8-51).
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 8-52).
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 8-34).
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 8-40).
Partner Oper State	The current operational state of the partner port.

Release History

Release 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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
```

BLANK PAGE

9 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** **vc-takeover** **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 neighbors** **show configuration vcm-snapshot chassis-id**

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 2360

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 2260 and an OmniSwitch 2360.
- 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 5.1; 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 2360

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 5.1.R2; 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
   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

N/A

Platforms Supported

Not supported in this release.

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 5.1; command not supported.

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

N/A

Platforms Supported

Not supported in this release.

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 5.1; command not supported.

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

N/A

Platforms Supported

Not supported in this release.

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 5.1; command not supported.

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

Not supported in this release.

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 5.1; command not supported.

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

N/A

Defaults

N/A

Platforms Supported

Not supported in this release.

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 5.1; command not supported.

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

Not supported in this release.

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 5.1; command not supported.

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

N/A

Platforms Supported

OmniSwitch 2360

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 5.1.R2; 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

Not supported in this release.

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 5.1; command not supported.

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.

virtual-chassis vf-link-mode {auto}

Syntax Definitions

N/A

Defaults

parameter	default
vf-link-mode	**auto** (if no vcsetup.cfg file exists).

Platforms Supported

OmniSwitch 2260, 2360

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
```

Release History

Release 5.1; 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

N/A

Platforms Supported

Not supported in this release.

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 5.1; command not supported.

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

Not supported in this release.

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 5.1; command not supported.

Related Commands

reload from	Reloads the master or slave chassis from the specified directory.

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 2260, 2360

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: Status suffix "+" means an added unit after last saved topology

Local Chassis: 1
 Oper                                  Config   Oper
 Chas  Role         Status             Chas ID  Pri   Group  MAC-Address
-----+------------+------------------+--------+-----+------+-----------------
 1     Master       Running            1        100   0      94:24:e1:55:85:29

-> show virtual-chassis chassis-id 1 topology
Legend: licenses-info - A: Advanced; B: Data Center;

Oper-Chassis-ID                : 1,
Config-Chassis-ID              : 1,
Chassis-Role                   : Master,
Previous-Chassis-Role          : Unassigned,
Chassis-Status                 : Running,
Chassis-Group                  : 0,
Chassis-MAC                    : 94:24:e1:55:85:29,
Up-Time                        : 2 days 17 hours 6 minutes and 33 seconds,
Designated-NI                  : 1,
Primary-CMM                    : CMM-A,
Secondary-CMM                  : Not present,
Chassis-Type                   : OS2360,
License                        : A,
Hello-Interval                 : 15,
```

```
Oper-Chassis-Priority           : 100,
Config-Chassis-Priority         : 100,
Oper-Control-VLAN               : 4094,
Config-Control-VLAN             : 4094,
VFLink-Mode                     : Auto,
Split-Detect-Protocol           : VCSP,
Number-Of-Neighbors             : 0,
Number-Of-Direct-Neighbors      : 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 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.
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.
VFLink Mode	The VFLink mode of the chassis: **Static** or **Auto**. *Only **Auto** is supported in this release*
Split-Detect-Protocol	*Not supported in this release.*
Number-of-Neighbors	Total number of neighbor switches that are part of the active virtual chassis topology for a given chassis group.
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).

Release History

Release 5.1; 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 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

Not supported in this release.

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     OS2260  0      10       4094     4094     AB
 2     2      OK     OS2260  0      10       4094     4094     AB
 3     2      NOK    OS2260  0      10       4094     4000     AB
 4     2      OK     OS2260  0      10       4094     4094     AB
 5     2      OK     OS2260  0      10       4094     4094     AB
 6     2      NOK    OS2260  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*         OS2260     OS2260    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.
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 5.1; command not supported.

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

Not supported in this release.

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 5.1; command not supported.

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 2260, 2360

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 5.1; 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

Not supported in this release.

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 5.1; command not supported.

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

Not supported in this release.

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 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).
Slot	Slot number identifying a particular network interface module (NI).
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 5.1; command not supported.

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

Not supported in this release.

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 5.1; command not supported.

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

Not supported in this release.

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 5.1; command not supported.

Related Commands

show configuration snapshot	Displays the configured and operational parameters related to the virtual chassis feature on the switch.

MIB Objects

N/A

BLANK PAGE

10 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 2260, 2360

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 5.1.R2; command introduced.

Related Commands

show erp	Displays the ERP ring configuration for the switch.
show erp statistics	Displays ERP ring statistics.

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 2260, 2360

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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.

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 2260, 2360

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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 2260, 2360

Usage Guidelines

The specified ring identification number must be unique within a switch.

Examples

```
-> erp-ring 1 clear
```

Release History

Release 5.1.R2; 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 2260, 2360

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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
```

11 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 2260, 2360

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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

This command is supported on the following OmniSwitch platforms:

6360	6465	6560	6860	6860N	6865	6900	6900 V72/C32	6900 X48C6/T48C6/ X48C4E/V48C8	9900
Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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 2260, 2360

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.
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 5.1.R2; 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 2260, 2360

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 1/1/1 statistics
Port 1/1/1:
  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
```

```
-> show mvrp statistics

Port 1/1/1:
  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 1/1/2:
  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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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 2260, 2360

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.
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 5.1.R2; 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 2260, 2360

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 5.1.R2; command introduced.

Related Commands

show mvrp statistics	Displays the MVRP statistics for all the ports, aggregates, or specific ports.

MIB Objects

```
alaMvrpGlobalClearStats
   alaMvrpPortStatsTable
   alaMvrpPortStatsClearStats
```

BLANK PAGE

12 802.1AB 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

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 2260, 2360

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 5.1; 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 2260, 2360

Usage Guidelines

The LLDP protocol must be enabled before using this command.

Examples

```
-> lldp transmit interval 40
```

Release History

Release 5.1; command introduced.

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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

Usage Guidelines

The LLDP protocol must be enabled before using this command.

Examples

```
-> lldp reinit delay 4
```

Release History

Release 5.1; command introduced.

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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; 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

```
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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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                 = OS2360,
  System Description          = Alcatel-Lucent Enterprise OS2360-48 5.1.11.R02.,
  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 5.1; command introduced.

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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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

13 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.

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 dhcp-client** **ip static-route** **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 router database** **show ip emp-routes** **show ip config** **show ip protocols** **show ip service** **show ip service source-ip**
ARP	**arp** **clear arp-cache** **ip dos arp-poison restricted-address** **arp filter** **clear arp filter** **show arp** **show ip dos arp-poison** **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	*This parameter is not supported.*
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	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 2260, 2360

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.

Examples

```
-> ip interface Marketing
-> 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
```

Release History

Release 5.1; command introduced.

Related Commands

show ip interface	Displays the status and configuration of IP interfaces.

MIB Objects

```
alaIpInterfaceTable
   alaIpInterfaceName
   alaIpInterfaceAddress
   alaIpInterfaceVipAddress
   alaIpInterfaceMask
   alaIpInterfaceAdminState
   alaIpInterfaceDeviceType
   alaIpInterfaceVlanID
   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 2260, 2360

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).
- 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 5.1; 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 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, 2260)
enable | disable	enable
filter-string	(“ “).
server-preference	disabled
local-proxy-arp | no local-proxy-arp	**no local-proxy-arp**

Platforms Supported

OmniSwitch 2260, 2360

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.
- 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 5.1; command introduced.

Related Commands

show ip interface	Displays the status and configuration of IP interfaces.

MIB Objects

```
alaIpInterfaceTable
   alaIpInterfaceDhcpStatus
   alaIpInterfaceDhcpIpRelease
   alaIpInterfaceDhcpIpRenew
   alaIpInterfaceDhcpOption60String
   alaIpInterfaceDhcpVsiAcceptFilterString
   alaIpInterfaceDhcpServerPreference
```

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 2260, 2360

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.
  - 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 5.1; command introduced.

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 route-pref

Configures the route preference of a router.

ip route-pref static *value*

Syntax Definitions

static	Configures the route preference of static routes.
value	Route preference value.

Defaults

parameter	default
static *value*	2

Platforms Supported

OmniSwitch 2360

Usage Guidelines

Route preference of local routes cannot be changed.

Examples

```
-> ip route pref static 1
```

Release History

Release 5.1; command introduced.

Related Commands

show ip route-pref	Displays the configured route-preference of a router.

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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.

ip directed-broadcast {enable | disable}

Syntax Definitions

enable	Enables IP directed broadcasts.
disable	Disables IP directed broadcasts.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 2260, 2360

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.

Examples

```
-> ip directed-broadcast enable
-> ip directed-broadcast disable
```

Release History

Release 5.1; 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.

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***}]**

no ip directed-broadcast trusted source-ip *ip_address* **{***ip_address/mask* **|** *ip_address* **mask** *subnet_mask***}**

Syntax Definitions

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 2260, 2360

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.
- 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


-> 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 5.1; 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.

ip directed-broadcast clear [trusted-source-ip {*ip_address/mask* | *ip_address* **mask** *subnet_mask*}]**

Syntax Definitions

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 2260, 2360

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 5.1; 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.

show ip directed-broadcast [trusted-source-ip {*ip_address/mask* **|** *ip_address* **mask** *subnet_mask***}] details**

Syntax Definitions

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 2260, 2360

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 5.1; 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.

ip service {all | *service_name* **| port** *service_port***} admin-state {enable | disable}**

Syntax Definitions

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 2260, 2360

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

service name	port
ssh	22
telnet	23
http	80
https	443
ntp	123
snmp	161

Examples

```
-> ip service all admin-state disable
-> ip service ftp admin-state enable
-> ip service port 20000 admin-state enable
```

Release History

Release 5.1; command introduced

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 2260, 2360

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 5.1; 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.

ip service source-ip {Loopback0 | *interface_name***} [tftp] [telnet] [tacacs] [swlog] [ssh] [snmp] [sflow] [radius] [ntp] [ldap] [ftp] [dns] [all]**

no ip service source-ip {Loopback0 | *interface_name***} [tftp] [telnet] [tacacs] [swlog] [ssh] [snmp] [sflow] [radius] [ntp] [ldap] [ftp] [dns] [all]**

Syntax Definitions

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	This parameter is not supported.
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 2260, 2360

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..

Examples

```
-> ip service source-ip loopback0 dns
-> ip service source-ip ipVlan100 ftp
```

Release History

Release 5.1; command introduced.

Related Commands

show ip service source-ip	Displays the IP service TCP/UDP port configuration and status.

MIB Objects

```
alaIpServiceSourceIPTable
   AlaIpServiceSourceIPAppIndex
   alaIpServiceSourceIPName
```

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. 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 2260, 2360

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 5.1; command was introduced.

Related Commands

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
```

clear arp-cache

Deletes all dynamic entries from the ARP table.

clear arp-cache

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 2260, 2360

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 5.1; 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 2260, 2360

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 192.165.1
-> no ip dos arp-poison restricted-address 192.165.1
```

Release History

Release 5.1; 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 2260, 2360

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 5.1; 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 arp filter	Displays a list of ARP filters configured for the switch.

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 2260, 2360

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 5.1; command introduced

Related Commands

arp filter	Configures an ARP filter to allow or block the processing of specified ARP Request packets.
show arp filter	Displays a list of ARP filters configured for the switch.

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

Usage Guidelines

N/A

Examples

```
-> icmp messages enable
-> icmp messages disable
```

Release History

Release 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

Usage Guidelines

N/A

Examples

```
-> ip tcp half-open-timeout 7
```

Release History

Release 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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
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
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. 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-2260,
  HostName                       =   OS2260,
```

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. 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. **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.)
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.

output definitions (continued)

Option-60	The option-60 string that will be included in DHCP discover or request packets.
HostName	The system name of the OmniSwitch.

Release History

Release 5.1; command introduced

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.
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
   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 2260, 2360

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 5.1; 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. show ip routes [summary]

Syntax Definitions

summary	Displays a summary of routing protocols that appear in the IP Forwarding table.

Defaults

By default, all routes are displayed.

Platforms Supported

OmniSwitch 2260, 2360

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 5.1; command introduced.

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.

show ip route-pref

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 2360

Usage Guidelines

N/A

Examples

```
-> show ip route-pref
  Protocol    Route Preference Value
------------+------------------------
  Local                 1
  Static                2
```

Release History

Release 5.1; command introduced.

Related Commands

ip route-pref	Configures the route preference of a router.

MIB Objects

```
alaIprmRtPrefTable
  alaIprmRtPrefEntryType
  alaIprmRtPrefEntryValue
```

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.

show ip router database [protocol *type* | **gateway** *ip_address* | **dest {***ip_address/prefixlen* | *ip_address***}]**

Syntax Definitions

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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command introduced

Related Commands

ip interface dhcp-client	Configures the router primary IP address.

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 2260, 2360

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 5.1; 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.

show ip service source-ip

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 2260, 2360

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
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 5.1; 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 2260, 2360

Usage Guidelines

N/A

Examples

```
-> show ip dos arp-poison
 IP Address                          Attacks
-------------------------------------+------------
192.165.1                              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 5.1; 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 2260, 2360

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 5.1; command introduced

Related Commands

arp	Adds a permanent entry to the ARP table.

MIB Objects

```
ipNetToMediaTable
   ipNetToMediaIfIndex
   ipNetToMediaNetAddress
   ipNetToMediaPhyAddress
   ipNetToMediaType
ipNetToMediaAugTable
   ipNetToMediaSlot
   ipNetToMediaPort
alaIpNetToMediaTable
   alaIpNetToMediaPhyAddress
   alaIpNetToMediaProxy
   alaIpNetToMediaVRRP
   alaIpNetToMediaAuth
```

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

Usage Guidelines

N/A

Examples

```
-> show ip tcp half-open-timeout
Tcp Half-Open Timeout(Seconds): 15.
```

Release History

Release 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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
  loopback-src                                           0
  invalid-ip                                             0
  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 5.1; 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
```

14 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.

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**

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. When enabled, DHCP packets can be relayed between a client and a server across VLANs.

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 2260, 2360

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 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..

Examples

```
-> ip dhcp relay admin-state enable
-> ip dhcp relay admin-state disable
```

Release History

Release 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 packets destined for the specified IP address are relayed over the VLAN 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 2260, 2360

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 before using this command. Packets destined for the specified IP address are relayed over the VLAN.

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; 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 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 2260, 2360

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 5.1; 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 dhcp relay interface	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 2260, 2360

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 5.1; 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

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 2260, 2360

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 5.1; command introduced.
Release 5.1; **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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command introduced.
Release 5.1; **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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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

Not supported in this release.

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 5.1; 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

Not supported in this release.

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 5.1; command introduced.

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; 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

```
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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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

Not supported in this release.

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 5.1; command introduced.

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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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

Not supported in this release.

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 5.1; 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

Not supported in this release.

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 5.1; 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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; command introduced.
Release 5.1.R2; Support for IPv6.

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 2260, 2360

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 5.1; command introduced.
Release 5.1.R2; Support for IPv6.

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 2260, 2360

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 5.1; command introduced.
Release 5.1.R2; Support for IPv6.

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 2260, 2360

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 5.1; command introduced.
Release 5.1.R2; Support for IPv6.

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 2260, 2360

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 5.1; command introduced.
Release 5.1.R2; Support for IPv6.

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 2260, 2360

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 5.1; command introduced.
Release 5.1.R2; Support for IPv6.

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 2260, 2360

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.

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 5.1; command introduced.
Release 5.1.R2; Support for IPv6.

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 2260, 2360

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 5.1; command introduced.
Release 5.1.R2; Support for IPv6.

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 2260, 2360

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 5.1; command introduced.
Release 5.1.R2; Support for IPv6.

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 2260, 2360

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 5.1; command introduced.
Release 5.1.R2; Support for IPv6.

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 2260, 2360

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 5.1; command introduced.
Release 5.1.R2; Support for IPv6.

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 2260, 2360

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 5.1; command introduced.
Release 5.1.R2; Support for IPv6.

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 2260, 2360

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 5.1; command introduced.
Release 5.1.R2; Support for IPv6.

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 2260, 2360

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 5.1; command introduced.
Release 5.1.R2; Support for IPv6.

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
```

15 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 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 bridge	**show ipv6 multicast bridge**
show ip multicast bridge-forward	**show ipv6 multicast bridge-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 or on the system if no VLAN is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***]] admin-state [enable | disable]**

no ip multicast [vlan *vlan_id***[-***vlan_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.
enable	Enable IP Multicast Switching.
disable	Disable IP Multicast Switching.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 2260, 2360

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. 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, as needed, is recommended to conserve switch resources.
- If IPMS is already enabled on the system, then the VLAN configuration will override the system's configuration.
- 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 or the specified VLAN.

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
```

Release History

Release 5.1; command was introduced.

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 of unknown multicast traffic for the specified VLAN or on the system if no VLAN 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***]] flood-unknown [enable | disable]**

no ip multicast [vlan *vlan_id***[-***vlan_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.
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 2260, 2360

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 configuration will override the system's configuration.
- 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
```

Release History

Release 5.1; command introduced.

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 or on the system if no VLAN is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***]] version [***version***]**

no ip multicast [vlan *vlan_id***[-***vlan_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.
version	Default IGMP protocol version to run. Valid range is 1–3.

Defaults

parameter	default
version	2

Platforms Supported

OmniSwitch 2260, 2360

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.
- If the default IGMP protocol version is already configured on the system, then the VLAN 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 or the specified VLAN. 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
```

Release History

Release 5.1; command introduced.

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. The group limit is applicable to all VLAN instances associated with the specified port.

ip multicast port *chassis/slot/port* **max-group [***num***] [action {none | drop | replace}]**

Syntax Definitions

chassis	The chassis identifier.
slot|port	The slot and port number (3/1).
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 2260, 2360

Usage Guidelines

- If group memberships are already registered on a port/VLAN 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 instance.
  - IP multicast memberships are pruned by a leave or when IP multicast is disabled on the specific VLAN or globally disabled for the switch.
- If the *num* and **action** parameters are not specified, then the limit is removed.
- 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.
  - Group limit configured for a specific VLAN.
  - Group limit configured for the IPMS profile assigned to a VLAN.
  - Group limit configured for a VLAN within a specific VRF context.
  - Group limit configured for the IPMS profile assigned to a VLAN 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
```

Release History

Release 5.1; command introduced.

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.

MIB Objects

```
alaIpmsIntfTable
   alaIpmsIntfConfigType
   alaIpmsIntfAddressType
   alaIpmsIntfMaxGroupLimit
   alaIpmsIntfMaxGroupExceedAction
```

ip multicast max-group

Configures the maximum group limit learned per port for the specified VLAN or per port on the system if no VLAN is specified. The limit is applied to each port that is a member of the given VLAN and the specified action is taken when the limit is exceeded.

ip multicast [vlan *vlan_id***[-***vlan_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.
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 2260, 2360

Usage Guidelines

- If a VLAN is not specified, this command configures the global maximum group limit applied to all VLAN 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.
- Configuring a maximum group value will have no affect on existing group memberships until the memberships are refreshed on the port/VLAN instance
- If the *num* and **action** parameters are not specified, then the limit is removed.
- The maximum group configuration on a VLAN 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.
  - Group limit configured for a specific VLAN.
  - Group limit configured for the IPMS profile assigned to a VLAN.
  - Group limit configured for a VLAN within a specific VRF context.
  - Group limit configured for the IPMS profile assigned to a VLAN 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
```

Release History

Release 5.1; command was introduced.

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 ports or for VLAN instances of a given port.

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.

ip multicast static-neighbor vlan *vlan_id* **{port** *chassis/slot/port* | **linkagg** *agg_id***}**

no ip multicast static-neighbor vlan *vlan_id* **{port** *chassis/slot/port* | **linkagg** *agg_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.

Defaults

N/A

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- Use the **no** form of this command to remove an IGMP static neighbor entry on the specified port for the specified VLAN.
- Creating an IGMP static neighbor entry on the specified port/VLAN, 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**).

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
```

Release History

Release 5.1; command was introduced.

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.

ip multicast static-querier vlan *vlan_id* **{port** *chassis/slot/port* | **linkagg** *agg_id***}**

no ip multicast static-querier vlan *vlan_id* **{port** *chassis/slot/port* | **linkagg** *agg_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.

Defaults

N/A

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- Use the **no** form of this command to remove an IGMP static querier entry on the specified port for the specified VLAN.
- Creating an IGMP static querier entry on the specified port/VLAN, 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**).

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
```

Release History

Release 5.1; command was introduced.

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.

ip multicast static-group *ip_address* **vlan** *vlan_id* **{port** *chassis/slot/port* | **linkagg** *agg_id***}**

no ip multicast static-group *ip_address* **vlan** *vlan_id* **{port** *chassis/slot/port* | **linkagg** *agg_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.

Defaults

N/A

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- Use the **no** form of this command to remove an IGMP static group entry on the specified port for the specified VLAN.
- Creating an IGMP static group entry on the specified port/VLAN, 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**).

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
```

Release History

Release 5.1; command was introduced.

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 or on the system if no VLAN is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***]] query-interval [***seconds***]**

no ip multicast [vlan *vlan_id***[-***vlan_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.
seconds	IGMP query interval in seconds. Valid range is 1–65535.

Defaults

parameter	default
seconds	125

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- IP Multicast Switching and Routing must be enabled to set the IGMP query interval on the system and/or the specified VLANs.
- If the IGMP query interval is already configured on the system, then the VLAN 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 or the specified VLAN. 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
```

Release History

Release 5.1; command was introduced.

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 or on the system if no VLAN is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***]] last-member-query-interval [***tenths_of_seconds***]**

no ip multicast [vlan *vlan_id***[-***vlan_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.
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 2260, 2360

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.
- If the IGMP last member query interval is already configured on the system, then the VLAN 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 or the specified VLAN. 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
```

Release History

Release 5.1; command was introduced.

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 or on the system if no VLAN is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***]] query-response-interval [***tenths_of_seconds***]**

no ip multicast [vlan *vlan_id***[-***vlan_id2***]] 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.
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 2260, 2360

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.
- If the IGMP query response interval is already configured on the system, then the VLAN 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 or the specified VLAN. 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
```

Release History

Release 5.1; command was introduced.

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 or on the system if no VLAN is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***]] unsolicited-report-interval [***seconds***]**

no ip multicast [vlan *vlan_id***[-***vlan_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.
seconds	IGMP unsolicited report interval in seconds. Valid range is 1–65535.

Defaults

parameter	default
seconds	1

Platforms Supported

OmniSwitch 2260, 2360

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.
- If the IGMP query response interval is already configured on the system, then the VLAN 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 or the specified VLAN. 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
```

Release History

Release 5.1; command was introduced.

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 or on the system if no VLAN is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***]] router-timeout [***seconds***]**

no ip multicast [vlan *vlan_id***[-***vlan_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.
seconds	IGMP router timeout in seconds. Valid range is 1–65535.

Defaults

parameter	default
seconds	90

Platforms Supported

OmniSwitch 2260, 2360

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
```

Release History

Release 5.1; command was introduced.

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 or on the system if no VLAN is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***]] source-timeout [***seconds***]**

no ip multicast [vlan *vlan_id***[-***vlan_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.
seconds	IGMP source timeout in seconds. Valid range is 1–65535.

Defaults

parameter	default
seconds	30

Platforms Supported

OmniSwitch 2260, 2360

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
```

Release History

Release 5.1; command was introduced.

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 2260, 2360

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 5.1; command was introduced.

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 or on the system if no VLAN is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***]] robustness [***robustness***]**

no ip multicast [vlan *vlan_id***[-***vlan_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.
robustness	IGMP robustness variable. Valid range is 1–7.

Defaults

parameter	default
robustness	2

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- IP Multicast Switching and Routing must be enabled to set the IGMP robustness variable on the system and/or the specified VLANs.
- If the IGMP robustness variable is already configured on the system, then the VLAN 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 or the specified VLAN. 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
```

Release History

Release 5.1; command was introduced.

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 or on the system if no VLAN is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***]] spoofing {enable | disable}**

no ip multicast [vlan *vlan_id***[-***vlan_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.
enable	Enable IGMP spoofing.
disable	Disable IGMP spoofing.

Defaults

parameter	default
enable | **disable**	**disable**

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- Use the **no** form of this command to remove an IGMP spoofing configuration and return the specified VLAN or system to the default behavior.
- If the IGMP spoofing is already enabled on the system, then the VLAN 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
```

Release History

Release 5.1; command was introduced.

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 or on the system if no VLAN or is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***]] spoofing static-source-ip** *ip_address*

no ip multicast [vlan *vlan_id***[-***vlan_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.
ip_address	A static source IPv4 address to use for spoofing.

Defaults

N/A

Platforms Supported

OmniSwitch 2260, 2360

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
```

Release History

Release 5.1; command introduced.

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 or on the system if no VLAN is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***] zapping [{enable | disable}]**

no ip multicast [vlan *vlan_id***[-***vlan_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.
enable	Enable IGMP zapping.
disable	Disable IGMP zapping.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- If the IGMP zapping is already enabled on the system, then the VLAN 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 or the specified VLAN.

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
```

Release History

Release 5.1; command was introduced.

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 or on the system if no VLAN is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***]] querier-forwarding [enable | disable]**

no ip multicast [vlan *vlan_id***[-***vlan_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.
enable	Enable IGMP querier forwarding.
disable	Disable IGMP querier forwarding.

Defaults

parameter	default
enable | **disable**	**disable**

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- If the IGMP querier forwarding is already enabled on the system, then the VLAN 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 or the specified VLAN.

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
```

Release History

Release 5.1; command was introduced.

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 or on the system if no VLAN is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***]] proxying [enable | disable]**

no ip multicast [vlan *vlan_id***[-***vlan_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.
enable	Enable IGMP proxying.
disable	Disable IGMP proxying.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- If the IGMP proxying is already enabled on the system, then the VLAN 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 or the specified VLAN.

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
```

Release History

Release 5.1; command was introduced.

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 2260, 2360

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.
- 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 5.1; command was introduced.

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 or on the system if no VLAN is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***]] zero-based-query [enable | disable]**

no ip multicast [vlan *vlan_id***[-***vlan_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.
enable	Enable IGMP zero-based querying.
disable	Disable IGMP zero-based querying.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- The IGMP zero-based query status set for a specific VLAN 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 or the specified VLAN.

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
```

Release History

Release 5.1; command introduced.

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 or on the system if no VLAN is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***]] forward-mode {asm | ssm | mac | auto}**

no ip multicast [vlan *vlan_id***[-***vlan_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.
asm	Sets the IPMS forwarding mode to ASM (the bridge lookup is based on the packet group destination IP address).
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).
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 2260, 2360

Usage Guidelines

- The forwarding mode set for a specific VLAN overrides the forwarding mode set for the system.
- If multicast routing is enabled on a VLAN, the following conditions apply:
  - 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.

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
```

Release History

Release 5.1; command introduced.

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 or on the system if no VLAN is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***]] update-delay-interval** *milliseconds*

no ip multicast [vlan *vlan_id***[-***vlan_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.
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 2260, 2360

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 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.

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
```

Release History

Release 5.1; command was introduced.

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 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 2260, 2360

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
--------------+---------------+---------------+---------------
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
--------------+---------------+---------------+---------------
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 5.1; command 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

Not supported in this release.

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 5.1; 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 instances) or to a specific VLAN 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***]**

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 2260, 2360

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**
[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**

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" proxying enable
-> no ip multicast profile "IGMPv3 with Zapping" proxying
-> no ip multicast profile "IGMPv3 with Zapping"
```

Release History

Release 5.1; command introduced.

Related Commands

ip multicast apply-profile	Assigns an IPMS configuration profile globally for the switch or to a specific VLAN.
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) or to a specific VLAN 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***]] apply-profile** *profile_name*

no ip multicast [vlan *vlan_id***[-***vlan_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.
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 2260, 2360

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**) to apply the specified profile to multiple VLANs 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”
-> no ip multicast apply-profile
-> no ip multicast vlan 20 apply-profile
-> no ip multicast vlan 20-15 apply-profile
```

Release History

Release 5.1; command 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 or on the system if no VLAN is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***]] admin-state [enable | disable]**

no ipv6 multicast [vlan *vlan_id***[-***vlan_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.
enable	Enable IPv6 Multicast Switching and Routing.
disable	Disable IPv6 Multicast Switching and Routing.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 2260, 2360

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. 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, as needed, is recommended to conserve switch resources.
- If the IPv6 Multicast Switching and Routing is already enabled on the system, then the VLAN configuration will override the system's configuration.
- 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 or the specified VLAN.

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
```

Release History

Release 5.1.R2; command introduced.

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 or on the system if no VLAN 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***]] flood-unknown [enable | disable]**

no ipv6 multicast [vlan *vlan_id***[-***vlan_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.
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 2260, 2360

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.
- 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.
- 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
```

Release History

Release 5.1.R2; command introduced.

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 or on the system if no VLAN is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***]] version [***version***]**

no ipv6 multicast [vlan *vlan_id***[-***vlan_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.
version	Default MLD protocol version to run. Valid entries are 1 or 2.

Defaults

parameter	default
version	1

Platforms Supported

OmniSwitch 2260, 2360

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.
- If the default MLD protocol version is already configured on the system, then the VLAN 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 or the specified VLAN. 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
```

Release History

Release 5.1.R2; command introduced.

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 of the port.

ipv6 multicast port *chassis/slot/port* **max-group [***num***] [action {none | drop | replace}]**

Syntax Definitions

chassis	The chassis identifier.
slot|port	The slot and port number (3/1).
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 2260, 2360

Usage Guidelines

- If group memberships are already registered on a port/VLAN 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 instance.
  - IP multicast memberships are pruned by a leave or when IP multicast is disabled on the specific VLAN 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.
- The maximum group configuration on a port will override the VLAN 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.
  - Group limit configured for a specific VLAN.
  - Group limit configured for the IPMS profile assigned to a VLAN.
  - Group limit configured for a VLAN within a specific VRF context.
  - Group limit configured for the IPMS profile assigned to a VLAN 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
```

Release History

Release 5.1.R2; command introduced.

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.

MIB Objects

```
alaIpmsIntfTable
   alaIpmsIntfConfigType
   alaIpmsIntfAddressType
   alaIpmsIntfMaxGroupLimit
   alaIpmsIntfMaxGroupExceedAction
```

ipv6 multicast max-group

Configures the maximum group limit learned per port for the specified VLAN or per port on the system if no VLAN is specified. The limit is applied to each port that is a member of the given VLAN and the specified action is taken when the limit is exceeded.

ipv6 multicast [vlan *vlan_id***[-***vlan_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.
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 2260, 2360

Usage Guidelines

- If a VLAN is not specified, this command configures the global maximum group limit applied to all VLAN 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.
- Configuring a maximum group value will have no affect on existing group memberships until the memberships are refreshed on the port/VLAN 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 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.
  - Group limit configured for a specific VLAN.
  - Group limit configured for the IPMS profile assigned to a VLAN.
  - Group limit configured for a VLAN within a specific VRF context.
  - Group limit configured for the IPMS profile assigned to a VLAN 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
```

Release History

Release 5.1.R2; command introduced.

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.

ipv6 multicast static-neighbor vlan *vlan_id* **{port** *chassis/slot/port* | **linkagg** *agg_id***}**

no ipv6 multicast static-neighbor vlan *vlan_id* **{port** *chassis/slot/port* | **linkagg** *agg_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.

Defaults

N/A

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- Use the **no** form of this command to remove an MLD static neighbor entry on the specified port for the specified VLAN.
- Creating an MLD static neighbor entry on the specified port/VLAN, 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**).

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
```

Release History

Release 5.1.R2; command introduced.

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.

ipv6 multicast static-querier vlan *vlan_id* **{port** *chassis/slot/port* | **linkagg** *agg_id***}**

no ipv6 multicast static-querier vlan *vlan_id* **{port** *chassis/slot/port* | **linkagg** *agg_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.

Defaults

N/A

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- Use the **no** form of this command to remove an MLD static querier entry on the specified port for the specified VLAN.
- Creating an MLD static querier entry on the specified port/VLAN, 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**).

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
```

Release History

Release 5.1.R2; command introduced.

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.

ipv6 multicast static-group *ipv6_address* **vlan** *vlan_id* **{port** *chassis/slot/port* | **linkagg** *agg_id***}**

no ipv6 multicast static-group *ipv6_address* **vlan** *vlan_id* **{port** *chassis/slot/port* | **linkagg** *agg_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.

Defaults

N/A

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- Use the **no** form of this command to remove an MLD static group entry on the specified port for the specified VLAN.
- Creating an MLD static group entry on the specified port/VLAN, 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**).

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
```

Release History

Release 5.1.R2; command introduced.

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 or on the system if no VLAN is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***]] query-interval [***seconds***]**

no ipv6 multicast [vlan *vlan_id***[-***vlan_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.
seconds	MLD query interval in seconds. Valid range is 1–65535.

Defaults

parameter	default
seconds	125

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- IPv6 Multicast Switching and Routing must be enabled to set the MLD query interval on the system and/or the specified VLANs.
- If the MLD query interval is already configured on the system, then the VLAN 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 or the specified VLAN. 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
```

Release History

Release 5.1.R2; command introduced.

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 or on the system if no VLAN is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***]] last-member-query-interval [***milliseconds***]**

no ipv6 multicast [vlan *vlan_id***[-***vlan_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.
milliseconds	MLD last member query interval in milliseconds. Valid range is 1–65535.

Defaults

parameter	default
milliseconds	1000

Platforms Supported

OmniSwitch 2260, 2360

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.
- If the MLD last member query interval is already configured on the system, then the VLAN 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 or the specified VLAN. 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
```

Release History

Release 5.1.R2; command introduced.

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 or on the system if no VLAN is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] query-response-interval [***milliseconds***]**

no ip multicast [vlan *vlan_id***[-***vlan_id2***]] 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.
milliseconds	MLD query response interval in milliseconds. Valid range is 1–65535.

Defaults

parameter	default
milliseconds	10000

Platforms Supported

OmniSwitch 2260, 2360

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.
- If the MLD query response interval is already configured on the system, then the VLAN 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 or the specified VLAN. 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
```

Release History

Release 5.1.R2; command introduced.

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 or on the system if no VLAN is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***]] unsolicited-report-interval [***seconds***]**

no ipv6 multicast [vlan *vlan_id***[-***vlan_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.
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 2260, 2360

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.
- If the MLD unsolicited report interval is already configured on the system, then the VLAN 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 or the specified VLAN. 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
```

Release History

Release 5.1.R2; command introduced.

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 or on the system if no VLAN is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***]] router-timeout [***seconds***]**

no ipv6 multicast [vlan *vlan_id***[-***vlan_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.
seconds	MLD router timeout in seconds. Valid range is 1–65535.

Defaults

parameter	default
seconds	90

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- IPv6 Multicast Switching and Routing must be enabled to set the MLD router timeout on the system and/or the specified VLANs.
- 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
```

Release History

Release 5.1.R2; command introduced.

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 or on the system if no VLAN is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***]] source-timeout [***seconds***]**

no ip multicast [vlan *vlan_id***[-***vlan_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.
seconds	MLD source timeout in seconds. Valid range is 1–65535.

Defaults

parameter	default
seconds	30

Platforms Supported

OmniSwitch 2260, 2360

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
```

Release History

Release 5.1.R2; command introduced.

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 2260, 2360

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 5.1.R2; command introduced.

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 or on the system if no VLAN is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***]] robustness [***robustness***]**

no ipv6 multicast [vlan *vlan_id***[-***vlan_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.
robustness	MLD robustness variable. Valid range is 1–7.

Defaults

parameter	default
robustness	2

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- IPv6 Multicast Switching and Routing must be enabled to set the MLD robustness variable on the system and/or the specified VLANs.
- If the MLD robustness variable is already configured on the system, then the VLAN 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 or the specified VLAN. 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
```

Release History

Release 5.1.R2; command introduced.

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 or on the system if no VLAN is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***]] spoofing {enable | disable}**

no ipv6 multicast [vlan *vlan_id***[-***vlan_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.
enable	Enable MLD spoofing.
disable	Disable MLD spoofing.

Defaults

parameter	defaults
enable | **disable**	**disable**

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- If the MLD spoofing is already enabled on the system, then the VLAN 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 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
```

Release History

Release 5.1.R2; command introduced.

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 or on the system if no VLAN is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***]] spoofing static-source-ip** *ipv6_address*

no ipv6 multicast [vlan *vlan_id***[-***vlan_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.
ipv6_address	A static source IPv6 address to use for spoofing.

Defaults

parameter	defaults
enable | **disable**	**disable**

Platforms Supported

OmniSwitch 2260, 2360

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
```

Release History

Release 5.1.R2; command introduced.

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 or on the system if no VLAN is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***]] zapping [enable | disable]**

no ipv6 multicast [vlan *vlan_id***[-***vlan_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.
enable	Enable MLD zapping.
disable	Disable MLD zapping.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- If the MLD zapping is already enabled on the system, then the VLAN 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 or the specified VLAN.

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
```

Release History

Release 5.1.R2; command introduced.

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 or on the system if no VLAN is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***]] querier-forwarding [enable | disable]**

no ipv6 multicast [vlan *vlan_id***[-***vlan_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.
enable	Enable MLD querier forwarding.
disable	Disable MLD querier forwarding.

Defaults

parameter	default
enable | **disable**	**disable**

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- If the MLD querier forwarding is already enabled on the system, then the VLAN 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 or the specified VLAN.

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
```

Release History

Release 5.1.R2; command introduced.

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 or on the system if no VLAN is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***]] proxying [enable | disable]**

no ipv6 multicast [vlan *vlan_id***[-***vlan_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.
enable	Enable MLD proxying.
disable	Disable MLD proxying.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- If the MLD proxying is already enabled on the system, then the VLAN 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 or the specified VLAN.

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
```

Release History

Release 5.1.R2; command introduced.

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 2260, 2360

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.
- 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 5.1.R2; command introduced.

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 or on the system if no VLAN is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***]] zero-based-query [enable | disable]**

no ipv6 multicast [vlan *vlan_id***[-***vlan_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.
enable	Enable MLD zero-based querying.
disable	Disable MLD zero-based querying.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- The MLD zero-based query status set for a specific VLAN 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 or the specified VLAN.

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
```

Release History

Release 5.1.R2; command introduced.

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 or on the system if no VLAN is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***]] forward-mode {asm | ssm | mac | auto}**

no ipv6 multicast [vlan *vlan_id***[-***vlan_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.
asm	Sets the IPMSv6 forwarding mode to ASM (the bridge lookup is based on the packet group destination IPv6 address).
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).
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 2260, 2360

Usage Guidelines

- The forwarding mode set for a specific VLAN overrides the forwarding mode set for the system.
- If multicast routing is enabled on a VLAN, the following conditions apply:
  - 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.

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
```

Release History

Release 5.1.R2; command introduced.

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 or on the system if no VLAN is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***]] update-delay-interval** *milliseconds*

no ipv6 multicast [vlan *vlan_id***[-***vlan_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.
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 2260, 2360

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 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.

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
```

Release History

Release 5.1.R2; command introduced.

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 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 2260, 2360

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
---------------+---------------+---------------+--------------
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
---------------+---------------+---------------+--------------
ff05::5         4444::2         ::              vlan 21
ff05::6         4444::2         ::              vlan 21
ff06::1         ::              ::              vlan 20
ff06::1         ::              ::              vlan 20
```

Release History

Release 5.1.R2; command 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 2260, 2360

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 5.1.R2; 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 VLANs) or to a specific VLAN. 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***]**

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 2260, 2360

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**
[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**

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" enable proxying enable
-> no ipv6 multicast profile "MLDv2 with Zapping" proxying
-> no ipv6 multicast profile "MLDv2 with Zapping"
```

Release History

Release 5.1.R2; command introduced.

Related Commands

ipv6 multicast apply-profile	Assigns an IPMS configuration profile globally for the switch or to a specific VLAN 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) or to a specific VLAN 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***]] apply-profile** *profile_name*

no ipv6 multicast [vlan *vlan_id***[-***vlan_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.
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 2260, 2360

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**) to apply the specified profile to multiple VLANs 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”
-> no ipv6 multicast apply-profile
-> no ipv6 multicast vlan 20 apply-profile
-> no ipv6 multicast vlan 20-15 apply-profile
```

Release History

Release 5.1.R2; command 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 or on the system if no VLAN is specified.

show ip multicast [vlan *vlan_id***]**

Syntax Definitions

vlan_id	VLAN ID number (1–4094).

Defaults

By default the status and general configuration parameters for the system are displayed.

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

Specify a VLAN ID to display the configuration information for a specific VLAN.

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,
```

```
-> 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,
```

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.

output definitions

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.
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.
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.

output definitions

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.

Release History

Release 5.1; command was introduced.

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
   alaIpmsConfigFloodUnknown
   alaIpmsConfigUpdateDelayInterval
   alaIpmsConfigForwardMode
   alaIpmsConfigQueryingStaticSourceAddress
   alaIpmsConfigSpoofingStaticSourceAddress
   alaIpmsConfigHelperAddress
```

show ip multicast port

Displays the maximum group configuration applicable for the specified port. The current number of groups learned on a port or port/VLAN instance is also displayed.

show ip multicast {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 2260, 2360

Usage Guidelines

Specify a port number to display the configuration information for a specific switch port.

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         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         Current Interface Interface Interface-Instance Interface-Instance
                            Groups  Max-group Action    Max-group          Action
---------------+------------+-------+---------+---------+------------------+------------------
1/1/52         vlan 1       0       0         none      0                  none
```

output definitions

Interface	The VLAN port.
Vlan	The VLAN 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. This limit is applicable on the given port for all VLAN instances of the port.
Interface Action	The action to be taken when the group membership limit is exceeded (**none**, **drop**, or **replace**).
Interface-Instance Max-group	The maximum group limit learned per port for the given VLAN. This limit is applied to each port that is a member of the given VLAN.
Interface-Instance Action	The action to be taken when the group membership limit is exceeded (**none**, **drop**, or **replace**).

Release History

Release 5.1; command was introduced.

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 or on the system if no VLAN 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***]] [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.
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 2260, 2360

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.
- To view the multicast forwarding database see the related **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” and “Egress Vlan” fields instead of the VLAN ID.

Examples

```
-> show ip multicast forward

Total 3 Forwards
                                                  Ingress      Egress
Group Address   Host Address   Tunnel Address Vlan          Vlan         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

-> show ip multicast forward vlan

Total 3 Forwards
                                                  Ingress      Egress
Group Address   Host Address   Tunnel Address Vlan          Vlan        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          VlaInterface
--------------+--------------+--------------+------------+------------+-----------
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	The ingress VLAN 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.
Egress Vlan	The egress VLAN 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 of the IP multicast forward.

Release History

Release 5.1; command was introduced.

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***]] [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.
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 2260, 2360

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” field instead of the VLAN ID.

Examples

```
-> show ip multicast neighbor

Total 12 Neighbors

Host Address    Vla 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

Total 10 Neighbors

Host Address    Vlan         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         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         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	The VLAN 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 of the IP multicast neighbor.
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 5.1; command was introduced.

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*]] [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.
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 2260, 2360

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” field instead of the VLAN ID.

Examples

```
-> show ip multicast querier

Total 10 Queriers

Host Address    Vlan         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
```

```
-> show ip multicast querier vlan

Total 8 Queriers

Host Address    Vlan         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         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	The VLAN 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 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 5.1; command was introduced.

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***]] [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.
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 2260, 2360

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” field instead of the VLAN ID.

Examples

```
-> show ip multicast group

Total 8 Groups

Group Address   Source Address  Vlan           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
```

```
-> show ip multicast group 225.0.1.0

Total 1 Groups

Group Address   Source Address  Vlan           Interface        Mode     Static  Count  Life
----------------+---------------+--------------+----------------+--------+-------+------+-----
225.0.1.0       0.0.0.0         vlan 21        1/1/19           exclude  no      5520   172


-> show ip multicast group vlan

Total 5 Groups

Group Address   Source Address  Vlan           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           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	The VLAN 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 on which the group membership was learned.
Mode	IGMP source filter mode.
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 5.1; command was introduced

Related Commands.

ip multicast static-group	Creates a static IGMP group entry on a specified port for the specified VLAN.

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***]] [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.
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 2260, 2360

Usage Guidelines

- Use the *ip_address* parameter to display source 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.
- To view the multicast forwarding database see the related **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” field instead of the VLAN ID.

Examples

```
-> show ip multicast source

Total 10 Sources

                                    Source        Ingress
Group Address   Host Address    Tunnel Address  Vlan
---------------+---------------+---------------+---------------
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
```

```
-> show ip multicast source 225.0.1.2

Total 2 Sources
                                      Source        Ingress
Group Address   Host Address    Tunnel Address  Vlan
---------------+---------------+---------------+---------------
225.0.1.2       21.20.20.2      0.0.0.0         vlan 21


-> show ip multicast source vlan

Total 5 Sources

                                      Source        Ingress
Group Address   Host Address    Tunnel Address  Vlan
---------------+---------------+---------------+---------------
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
---------------+---------------+---------------+---------------
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	The ingress VLAN 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 5.1; command was introduced.

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***]] [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.
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 2260, 2360

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” field instead of the VLAN ID.

Examples

```
-> show ip multicast tunnel

Total 3 Tunnels
                                  Destination      Ingress
Group Address   Host Address    Tunnel Address  Vlan
--------------+---------------+---------------+--------------
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
---------------+---------------+---------------+--------------
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	VLAN 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 5.1; command was introduced.

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 bridge

Displays the IP multicast bridge table entries that match the specified VLAN, IP multicast group address, MAC address, or all entries if no additional parameters are specified.

show ip multicast bridge [vlan [*vlan_id***[-***vlan_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.
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 2260, 2360

Usage Guidelines

- Use one of the optional parameters (*vlan_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           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          Type      Group Address     Host Address Action      UpTime
--------------+---------+-----------------+------------+-----------+--------------
vlan 10        mac       01-00-5e-09-08-07              forwarding  00d:00h:00m
```

output definitions

Vlan	The VLAN 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 5.1; command introduced.

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, 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***] | *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.
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 2260, 2360

Usage Guidelines

- Use one of the optional parameters (*vlan_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          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          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	The VLAN 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 5.1; command introduced.

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 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 2260, 2360

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,
```

Release History

Release 5.1; 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 or on the system if no VLAN is specified.

show ipv6 multicast [vlan *vlan_id***]**

Syntax Definitions

vlan_id	VLAN for which to display the configuration.

Defaults

By default, the status and general configuration parameters for the system are displayed.

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

Specify a VLAN ID to display the configuration information for a specific VLAN.

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,
```

```
-> 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,
```

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.

output definitions

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.
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.)
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.

output definitions

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.

Release History

Release 5.1.R2; command introduced.

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. The current number of groups learned on a port or port/VLAN is also displayed.

show ipv6 multicast 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 2260, 2360

Usage Guidelines

Specify a port number to display the configuration information for a specific port.

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         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         Current Interface Interface Interface-Instance Interface-Instance
                            Groups  Max-group Action    Max-group          Action
---------------+------------+-------+---------+---------+------------------+------------------
1/6/23         vlan 1003    0       0         none      0                  none
```

output definitions

Interface	The VLAN port.
Vlan	The VLAN 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. This limit is applicable on the given port for all VLAN instances of the port.
Interface Action	The action to be taken when the group membership limit is exceeded (**none**, **drop**, or **replace**).
Interface-Instance Max-group	The maximum group limit learned per port for the given VLAN. This limit is applied to each port that is a member of the given VLAN.
Interface-Instance Action	The action to be taken when the group membership limit is exceeded (**none**, **drop**, or **replace**).

Release History

Release 5.1.R2; command introduced.

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 or on the system if no VLAN 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***]] [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.
all-vrf	Display forwarding table entries for all of the VRF instances.

Defaults

N/A

Platforms Supported

OmniSwitch 2260, 2360

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.
- To view the multicast forwarding database see the related **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” and “Egress Vlan” fields instead of the VLAN ID.

Examples

```
-> show ipv6 multicast forward

Total 3 Forwards
                                                    Ingress    Egress
Group Address   Host Address    Tunnel Address  VLAN         VLAN       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         VLAN       Interface
--------------+---------------+---------------+------------+------------+---------
ff05::6         4444::2         ::              vlan 20      vlan 20      1/1/2

-> show ipv6 multicast forward vlan

Total 3 Forwards
                                                 Ingress            Egress
Group Address   Host Address    Tunnel Address  VLAN         VLAN       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               VLAN 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.
Ingress VLAN	The ingress VLAN 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	The egress VLAN 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 of the IPv6 multicast forward.

Release History

Release 5.1.R2; command introduced.

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*]] [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.
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 2260, 2360

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” field instead of the VLAN ID.

Examples

```
-> show ipv6 multicast neighbor

Total 4 Neighbors

Host Address               Vlan          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


-> show ipv6 multicast neighbor vlan

Total 2 Neighbors

Host Address               Vlan          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          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	The VLAN 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 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 5.1.R2; command introduced.

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*]] [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.
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 2260, 2360

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” field instead of the VLAN ID.

Examples

```
-> show ipv6 multicast querier

Total 4 Queriers

Host Address               Vlan          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


-> show ipv6 multicast querier vlan

Total 2 Queriers

Host Address               Vlan          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           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	The VLAN 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 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 5.1.R2; command introduced.

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***]] [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.
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 2260, 2360

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” field instead of the VLAN ID.

Examples

```
-> show ipv6 multicast group ff05::5

Group Address   Source Address Vlan         Interface Mode     Static Count  Life
--------------+--------------+------------+----------+--------+------+------+-----
ff05::5         ::             vlan 21      1/1/19     exclude  no     1      145


-> show ipv6 multicast group vlan

Total 3 Groups

Group Address   Source Address  Vlan        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         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	The VLAN 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 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 5.1.R2; command introduced.

Related Commands

ipv6 multicast static-group	Creates a static MLD group entry on a specified port for the specified VLAN.

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***]] [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.
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 2260, 2360

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.
- To view the multicast forwarding database see the related **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” field instead of the VLAN ID.

Examples

```
-> show ipv6 multicast source

Total 8 Sources
                                      Source        Ingress
Group Address   Host Address    Tunnel Address  VLAN
---------------+---------------+---------------+---------------
ff05::6         4444::2         ::              vlan 21
ff05::7         4444::2         ::              vlan 21
ff06::1         ::              ::              vlan 20
ff06::2         ::              ::              vlan 20
```

```
-> show ipv6 multicast source ff05::6

Total 2 Sources

                                    Source        Ingress
Group Address   Host Address    Tunnel Address  VLAN
---------------+---------------+---------------+---------------
ff05::6         4444::2         ::              vlan 21


-> show ipv6 multicast source vlan

Total 4 Sources

                                    Source        Ingress
Group Address   Host Address    Tunnel Address  VLAN
---------------+---------------+---------------+---------------
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
---------------+---------------+---------------+---------------
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	The ingress VLAN 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 5.1.R2; command introduced.

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***]] [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.
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 2260, 2360

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” field instead of the VLAN ID.

Examples

```
-> show ipv6 multicast tunnel

Total 4 Tunnels

                                  Destination      Ingress
Group Address   Host Address    Tunnel Address  Vlan
---------------+---------------+---------------+---------------
ff05::6         4444::2         5555::3         vlan 21
ff05::7         4444::2         5555::3         vlan 21

-> show ipv6 multicast tunnel vlan

Total 2 Tunnels

                                  Destination      Ingress
Group Address   Host Address    Tunnel Address  Vlan
---------------+---------------+---------------+---------------
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
---------------+---------------+---------------+---------------
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	VLAN 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 5.1.R2; command introduced.

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 bridge

Displays the IPv6 multicast bridge table entries that match the specified VLAN, IPv6 multicast group address, MAC address, or all entries if no additional parameters are specified.

show ipv6 multicast bridge [vlan *vlan_id***[-***vlan_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.
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 2260, 2360

Usage Guidelines

- Use one of the optional parameters (*vlan_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          Type         Group Address     Host Address  Action      UpTime
--------------+------------+-----------------+-------------+-----------+-----------
vlan 130       asm          ff05::6                         forwarding  00h:00m:04s
```

output definitions

Vlan	The VLAN 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 5.1.R2; command introduced.

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, 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***] |** *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.
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 2260, 2360

Usage Guidelines

- Use one of the optional parameters (*vlan_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          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          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	The VLAN 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 5.1.R2; command introduced.

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 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 2260, 2360

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,
```

Release History

Release 5.1.R2; command 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
```

16 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).

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 phones** **qos user-port** **qos dei** **debug qos** **debug qos internal** **clear qos log** **qos apply** **qos revert** **qos flush** **qos reset** **qos stats reset** **show qos log** **show qos config** **show qos statistics**

Port and Slice commands	**qos port** **qos port reset** **qos port trusted** **qos port default 802.1p** **qos port default dscp** **qos port default classification** **qos port dei** **show qos port**
Queue Management commands	**qos qsi qsp** **qos qsi stats** **show qos qsp** **show qos qsi** **show qos qsi summary** **show qos qsi stats** **clear qos qsi 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 2260, 2360

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 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.

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 16-29 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 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 2260, 2360

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.

Examples

```
-> qos phones priority 7
-> qos phones trusted
-> qos no phones
```

Release History

Release 5.1; command was introduced.

Related Commands

show qos config	Displays the QoS configuration for the switch.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigAutoPhones
```

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 2260, 2360

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 5.1; command introduced.

Related Commands

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.
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 2260, 2360

Usage Guidelines

- Use the **no** form of this command to disable the global DEI bit mapping (ingress) or marking (egress) configuration for the switch.
- 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.

Examples

```
-> qos dei ingress
-> qos dei egress
```

```
-> qos no dei ingress
-> qos no dei egress
```

Release History

Release 5.1; command introduced.

Related Commands

qos port	Configures a physical port for QoS.
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

Not supported in this release.

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 5.1; command not supported.

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

Not supported in this release.

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 5.1; command not supported.

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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

Not supported in this release.

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 5.1; command not supported.

Related Commands

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.

qos flush

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 2260, 2360

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.

Examples

```
-> qos flush
```

Release History

Release 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command was introduced.

Related Commands

show qos statistics	Displays statistics about the QoS configuration.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigStatsReset
```

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 2260, 2360

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 5.1; 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]
[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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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.
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

Not supported in this release.

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.

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 5.1; command not supported.

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.
show qos config	Displays global information about the QoS configuration.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSPortTable
   alaQoSPortDEIMapping
   alaQoSPortDEIMarking
```

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	*This parameter option is not supported.*
qsp_id	An existing QSet profile (QSP) ID number to assign to this instance.
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

Not supported in this release.

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.

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
```

Release History

Release 5.1; command not supported.

Related Commands

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 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 2260, 2360

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 5.1; 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 2260, 2360

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          1G       -       -   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       -       -   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          1G       -       -   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	*Not supported in this release.*
Egress Bandwidth	*Not supported in this release.*
DEI Map/Mark	The Drop Eligible Indicator (DEI) bit mapping and marking setting for the port. Configured through the **qos dei** command.
Type	The interface type, **ethernet** or **wan**.

Release History

Release 5.1; 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 log

Displays the log of QoS events.

show qos log

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 2260, 2360

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 5.1; 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 2260, 2360

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,
  Trust ports                    = no,
  Log lines                      = 10240,
  Log level                      = 5,
  Log console                    = no,
  Forward log                    = no,
  User-port filter               = spoof,
  User-port shutdown             = none,
  Phones                         = trusted,
  DEI Mapping                    = Disabled,
  DEI Marking                    = Disabled,
```

output definitions

Admin	Whether or not QoS is enabled or disabled. Configured through the **qos** command.
Trust Ports	The default trusted mode for switch ports. Configured through the **qos trust-ports** 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.

output definitions (continued)

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.
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.
Phones	Whether or not IP Phone traffic is automatically trusted or assigned a priority value. Configured through the **qos phones** command.
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.

Release History

Release 5.1; 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

Not supported in this release.

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 5.1; command not supported.

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 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_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

Not supported in this release.

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.

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 not supported.
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.

```
-> show qos qsp brief
Profile  Name          #Ports  #Queues  BW(%)  Type      Base Profile
--------+-------------+-------+--------+------+---------+-------------
1        qsp-1         58      8        100    Static    qsp-1
```

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 not supported.
Base Profile	The profile on which the QSP is based.

```
-> 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     Port 1/1/10    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
```

```
1/1/13      Phy  Port 1/1/13    1  qsp-1      Port 1/1/13    100    100       S
1/1/14      Phy  Port 1/1/14    1  qsp-1      Port 1/1/14    100    100       S
1/1/15      Phy  Port 1/1/15    1  qsp-1      Port 1/1/15    100    100       S
1/1/16      Phy  Port 1/1/16    1  qsp-1      Port 1/1/16    100    100       S
1/1/17      Phy  Port 1/1/17    1  qsp-1      Port 1/1/17    100    100       S
1/1/18      Phy  Port 1/1/18    1  qsp-1      Port 1/1/18    100    100       S
1/1/19      Phy  Port 1/1/19    1  qsp-1      Port 1/1/19    100    100       S
1/1/20      Phy  Port 1/1/20    1  qsp-1      Port 1/1/20    100    100       S
1/1/21      Phy  Port 1/1/21    1  qsp-1      Port 1/1/21    100    100       S
1/1/22      Phy  Port 1/1/22    1  qsp-1      Port 1/1/22    100    100       S
1/1/23      Phy  Port 1/1/23    1  qsp-1      Port 1/1/23    100    100       S
1/1/24      Phy  Port 1/1/24    1  qsp-1      Port 1/1/24    100    100       S
1/1/25      Phy  Port 1/1/25    1  qsp-1      Port 1/1/25    100    100       S
1/1/26      Phy  Port 1/1/26    1  qsp-1      Port 1/1/26    100    100       S
1/1/27      Phy  Port 1/1/27    1  qsp-1      Port 1/1/27    100    100       S
1/1/28      Phy  Port 1/1/28    1  qsp-1      Port 1/1/28    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 or link aggregate 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 or link aggregate. The QSAP is not configurable at this time.
QSAP Type	The type of QSAP port; Phy = physical (slot/port), Log = logical (linkagg 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 or link aggregate.
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 not supported.

Release History

Release 5.1; command 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 qsi

Displays the QSet instance (QSI) configuration for the switch. A QSI is a logical set of eight egress queues associated with each port or link aggregate (LAG) ID.

show qos qsi [port *chassis/slot/port***[-***port2***] | linkagg** *agg_id***[-***agg_id2***] | vf-link** *vfl_id***] detail**

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	*This parameter option is not supported.*
detail	Displays additional queue information for the instance.

Defaults

By default, displays the entire QSI configuration for the switch.

Platforms Supported

Not supported in this release.

Usage Guidelines

Use the **port** *slot/port*, **slot** *slot*, **linkagg** *agg_id,* parameters to display the QSI information associated with specific ports, link aggregates. These parameters can also be combined with the **detail** or **summary** parameter.

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 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, 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. 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.
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.

Release History

Release 5.1; command introduced.

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 summary

Displays a list of switch ports showing the QoS 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 (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

By default, a summary of all ports is displayed.

Platforms Supported

Not supported in this release.

Usage Guidelines

Use the **port** *chassis/slot/port* or **linkagg** *agg_id* parameters 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 1/1-3 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
```

output definitions

Port	The port or link aggregate ID number.
Profile #	The QSet profile ID number assigned to the port.
Profile Name	The QSet profile name assigned to the port.
Mode	Indicates the port is operating in the QoS mode.
Parent	The parent ID of the port.

Release History

Release 5.1; command introduced.

Related Commands

qos qsi qsp	Changes the QSet profile association for a QSet instance.
show qos qsi	Displays the QSet instance (QSI) configuration for the switch.

MIB Objects

```
alcatelIND1VfcMIB
alaVfcQsetInstanceTable
   alaVfcQsetId
   alaVfcQsetQSPId
   alaVfcQsetQSPName
   alaVfcQsetMode
```

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 2260, 2360

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 5.1; command 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
```

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 2260, 2360

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 5.1; command was introduced.

Related Commands

show qos qsi stats	Displays QSet instance statistics.

MIB Objects

```
alcatelIND1VfcMIB
alaVfcQsapTable
   alaVfcQsapClearStats
   alaVfcQsapQpId
```

17 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.

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 16, "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

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** **iec message-type priority** **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 app-mon-application-group** **policy condition app-mon-application-name** **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**
IEC 6185 traffic prioritization	**iec message-type priority** **iec message-type flush** **iec show**
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 2260, 2360

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. Consider the following recommendations regarding the default policy list:
  - 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.

– When creating a policy rule with a destination port condition on an OmniSwitch 9900, specify the **no default-list** option to ensure that this type of condition is supported on the OmniSwitch 9900. See the **policy condition destination port** command.

- 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.
- 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.

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 5.1.R2; command introduced.

Related Commands

iec message-type priority	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
```

iec message-type priority

Configures a QoS priority for the specified IEC 61850 message type. This command runs a python script that programs QoS rules that will apply traffic prioritization to IEC 61850 message packets.

iec message-type *message* **priority** *string*

Syntax Definitions

message	The message type for which a QoS rule is configured. Specify one of the supported IEC 61850 message types: goose, gse, sv, ptp, sntp, mms, all.
priority *string*	Sets the priority level. The priority string value must be set to one of the following: • "high" (maps to QoS priority queue 7) • "medium" (maps to QoS priority queue 4) • "low" (maps to QoS priority queue 1) • "default" (sets the priority to the default value for the message type)

Defaults

By default, the priority for all the supported IEC 61850 message type is set to default.

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- To set the priority for all message types at once, specify "all" as the message type value.
- A message type can be configured with only one priority.
- Use the "default" option to restore the default priority as shown in the table:

Message Type	Default Priority
GOOSE	High
GSE	Medium
SV	High
MMS	Low
SNTP	Medium
PTP	Medium

- The QoS policy condition, action, and rule names that are used to prioritize IEC 61759 traffic are predefined. The following reserved names must not be used for user policy configuration:

Function	Message Type	Condition	Action	Rule
1A. Trip	GOOSE	iec_goose_c	iec_goose_a	iec_goose_r
1B. Other	GSE	iec_gse_c	iec_gse_a	iec_gse_r
Raw Data	SV	iec_sv_c	iec_sv_a	iec_sv_r
Time Sync	PTP	iec_ptp_c	iec_ptp_a	iec_ptp_r
Time Sync	SNTP	iec_sntp_c	iec_sntp_a	iec_sntp_r
File Transfer	MMS	iec_mms_c	iec_mms_a	iec_mms_r

- Use the **iec message-type flush** CLI command to remove the prioritization for message type.

Examples

```
-> iec message-type goose priority high
-> iec message-type gse priority low
-> iec message-type mms priority medium
-> iec message-type all priority high
```

Release History

Release 5.1.R2; command introduced.

Related Commands

iec message-type flush	Removes the rule applied for the IEC 61850 message priority.
iec show	Displays the priority configured for the IEC 61850 message types.

MIB Objects

N/A

iec message-type flush

Removes the rule applied for the IEC 61850 message priority.

iec message-type *message* **flush**

Syntax Definitions

message	The message type for which rule must be flushed. Specify one of the supported IEC 61850 message types: goose, gse, sv, ptp, sntp, mms, all.

Defaults

N/A

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- This command runs a python script that programs the QoS rules for traffic prioritization.
- The “all” option flushes the priority rule for all the message types at once.

Examples

```
-> iec message-type goose flush
-> iec message-type gse flush
-> iec message-type mms flush
-> iec message-type all flush
```

Release History

Release 5.1.R2; command introduced.

Related Commands

iec message-type priority	Configures IEC 61850 message priority.
iec show	Displays the priority configured for the IEC 61850 message types.

MIB Objects

N/A

iec show

Displays the priority configured for the IEC 61850 message types.

iec show

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

6360	6465	6560	6860	6860N	6865	6900	6900 V72/C32	6900 X48C6/T48C6/ X48C4E/V48C8	9900
No	Yes	No	No	No	Yes	No	No	No	No

Usage Guidelines

The output displays only the configured message types.

Examples

```
-> iec show
Message Type      Priority
---------------+------------
goose             high
sntp               low
```

Release History

Release 5.1.R2; command introduced.Release

Related Commands

iec message-type priority	Configures IEC 61850 message priority.

MIB Objects

N/A

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 2260, 2360

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 5.1.R2; command 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 6360, OmniSwitch 6465, and 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 2260, 2360

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 5.1.R2; command introduced.

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 2260, 2360

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 6360, OmniSwitch 6465, and 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)

- On an OmniSwitch 9900, a destination port condition is supported only when the condition is part of a policy rule that was configured using the **no default-list** option (for example, **policy rule r1 condition c1 action a1 no default-list**). See the **policy condition destination port** command.

- 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 6360 and 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
  - Source MAC/MAC group
  - Destination MAC/ MAC group
  - Ethertype for IPV6
- On the OmniSwitch 6360, 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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command introduced.

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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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***]**
[inner source-vlan *vlan_id***]**
[802.1p *802.1p_value***]**
[inner 802.1p *802.1p_value***]**

[source port *chassis/slot/port***[-***port2***]]**
[source port group *group_name***}**
[destination port *chassis/slot/port***[-***port2***]]**
[fragments]
[app-mon-application-group *group_name***]**
[app-mon-application-name *app_name***]**

no policy condition *condition_name*

Syntax Definitions

condition_name	The name of the condition. Any alphanumeric string.

Defaults

N/A

Platforms Supported

OmniSwitch 2260, 2360

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 5.1.R2; command 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 {any |** *ip_address* **[mask** *netmask***]}**

policy condition *condition_name* **no source ip**

Syntax Definitions

condition_name	The name of the condition.
any	Any source IPv4 address.
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 2260, 2360

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
-> policy condition cond4 source ip any
```

Release History

Release 5.1.R2; command 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 2260, 2360

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
-> policy condition cond4 source ipv6 any
```

Release History

Release 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 6360 or OmniSwitch 6465.*

Defaults

N/A

Platforms Supported

OmniSwitch 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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.

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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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.

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

Not supported in this release.

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 5.1.R2; command not supported.

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 2260, 2360

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 5.1.R2; command not supported.

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 2260, 2360

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 5.1.R2; command 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 6360 or 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/C32, and OmniSwitch 9900.*

Defaults

N/A

Platforms Supported

OmniSwitch 2260, 2360

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 5.1.R2; command 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
   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 6900-V72/C32 and OmniSwitch 6900-X48C6/T48C6/X48C4E/V48C8.*

Defaults

N/A

Platforms Supported

OmniSwitch 2260, 2360

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).
- On an OmniSwitch 9900, a destination port condition is supported only when the condition is part of a policy rule that was configured using the **no default-list** option (for example, **policy rule r1 condition c1 action a1 no default-list**) *and* the rule is assigned to an egress policy list.

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

On the OmniSwitch 9900, a destination port condition is supported only with the
following configuration of the policy rule:

-> policy condition cond5 destination port 1/3/1
```

```
-> policy action a1
-> policy rule r1 condition cond5 action a1 no default-list
-> policy list list1 type egress
-> policy list list1 rules r1
-> qos apply
```

Release History

Release 5.1.R2; command 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
   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 2260, 2360

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 5.1.R2; command 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

Not supported in this release.

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 5.1.R2; command not supported.

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

Not supported in this release.

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 5.1.R2; command not supported.

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

This command is supported on the following OmniSwitch platforms:

6360	6465	6560	6860	6860N	6865	6900	6900 V72/C32	6900 X48C6/T48C6/ X48C4E/V48C8	9900
Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

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 5.1.R2; command 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 app-mon-application-group

Associates an Application Monitoring and Enforcement (AppMon) application group with a policy condition.

policy condition *condition_name* **app-mon-application-group** *group_name*

policy condition *condition_name* **no app-mon-application-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 AppMon application group to which the QoS policy condition applies.

Defaults

N/A

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- Use the **no** form of the command to remove an AppMon group name from a condition; however, at least one classification parameter must be associated with a condition.
- The **app-mon-application-group** policy condition is used in the rules associated with QoS default policy lists or UNP policy lists.
- Policy condition command will not support any other native QoS policy condition keywords along with AppMon application group or name keyword.
- For more information about AppMon, see the “Configuring Application Monitoring and Enforcement” chapter in the *OmniSwitch AOS Release 8 Network Configuration Guide*.

Examples

```
-> policy condition cond6 app-mon-application-group web
-> policy condition cond6 no app-mon-application-group
```

Release History

Release 5.1.R2; command 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
   alaQosConditionDpiAppGroup
   alaQoSConditionDPIAppGroupStatus
```

policy condition app-mon-application-name

Associates an Application Monitoring and Enforcement (AppMon) application name with a policy condition.

policy condition *condition_name* **app-mon-application-name** *app_name*

policy condition *condition_name* **no app-mon-application-name**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
app_name	The name of the AppMon application to which the QoS policy condition applies.

Defaults

N/A

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- Use the **no** form of the command to remove an AppMon application name from a condition; however, at least one classification parameter must be associated with a condition.
- The **app-mon-application-group** policy condition is used in the rules associated with QoS default policy lists or UNP policy lists.
- Policy condition command will not support any other native QoS policy condition keywords along with AppMon application group or name keyword.
- For more information about AppMon, see the “Configuring Application Monitoring and Enforcement” chapter in the *OmniSwitch AOS Release 8 Network Configuration Guide*.

Examples

```
-> policy condition cond6 app-mon-application-name whatsapp
-> policy condition cond6 no app-mon-application-name
```

Release History

Release 5.1.R2; command 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
   alaQoSConditionDPIAppName
   alaQoSConditionDPIAppNameStatus
```

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

Not supported in this release.

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 5.1.R2; command not supported.

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

Not supported in this release.

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 5.1.R2; command not supported.

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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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***]**
[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 2260, 2360

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 5.1.R2; command introduced.

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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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

Not supported in this release.

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 5.1.R2; command not supported.

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

Not supported in this release.

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 5.1.R2; command not supported.

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 2260, 2360

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** 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 5.1.R2; command 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.

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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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

Not supported in this release.

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 5.1.R2; command not supported.

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	Displays only network groups that have been applied.
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 2260, 2360

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 5.1.R2; command 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	Displays only policy services that have been applied.
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 2260, 2360

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 5.1.R2; command 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	Displays only policy service groups that have been applied.
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 2260, 2360

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 5.1.R2; command 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	Displays only MAC groups that have been applied.
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 2260, 2360

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 5.1.R2; command 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	Displays only policy port groups that have been applied.
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 2260, 2360

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 5.1.R2; command 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	Displays only policy map groups that have been applied.
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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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
```

```
-> show policy condition
Condition name                  : c1
Application group               = apg1

Condition name                  : c2
State                           = new,
Application name                = "jabber -init sequence",
Destination UDP port            = 17
```

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.
Source VLAN	The source VLAN.
Destination UDP port	The destination UDP port.
Application group	Name of the AppMon application group to which the QoS policy condition is applied.
Application name	Name of the AppMon application to which the QoS policy condition applied.

Release History

Release 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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	Displays only policy rules that have been applied.
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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 **iec message-type priority** 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 **iec message-type priority** 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 **iec message-type priority** 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 **iec message-type priority** 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 **iec message-type priority** command. If this field does not appear, then the validity period is not restricted to a specific date and time interval.

Release History

Release 5.1.R2; command introduced.

Related Commands

iec message-type priority	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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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.
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 5.1.R2; command 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

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 2260, 2360

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.
Destination IP/Destination Group	The IPv6 address of the destination or destination group.
VRF Name	The name of the VRF.

output definitions

Act	The name of the action.
Hit Count	The sum of packet counts from all NIs matching the corresponding rule.

Release History

Release 5.1.R2; command 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

N/A

BLANK PAGE

18 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 16, "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 2260, 2360

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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 2260, 2360

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.
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 5.1.R2; 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
   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 2260, 2360

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 5.1.R2; 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 2260, 2360

Usage Guidelines

This command displays information about policies created on directory servers only. Chapter 16, "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
```

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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
```

BLANK PAGE

19 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 test-radius-server** **aaa tacacs+-server** **aaa ldap-server** **show aaa server** **show aaa server statistics** **aaa radius-server clear-statistics**
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 ip-lockout-threshold** **aaa switch-access banned-ip release** **aaa switch-access priv-mask** **aaa switch-access management-stations admin-state** **show aaa switch-access ip-lockout-threshold** **show aaa switch-access banned-ip** **show aaa switch-access priv-mask**

Common Criteria	**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**

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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; 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 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command was introduced.

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 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 2260, 2360

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 5.1; command was introduced.

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
```

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command 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 2260, 2360

Usage Guidelines

Use the **aaa authentication** command to set the default servers.

Examples

```
-> aaa authentication telnet default
-> aaa authentication default default
```

Release History

Release 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; command 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 2260, 2360

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 5.1; command 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 2260, 2360

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 5.1; command 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 2260, 2360

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 5.1; command 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 2260, 2360

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 5.1; command 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; command 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 2260, 2360

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 os2260
```

Release History

Release 5.1; command 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 2260, 2360

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 5.1; command 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 2260, 2360

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 5.1; command 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 2260, 2360

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 192.165.1
```

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 5.1; command introduced.

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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; 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 2260, 2360

Usage Guidelines

N/A.

Examples

```
-> user password-size min 9
```

Release History

Release 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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** or **configuration snapshot** command to save user settings over a reboot.

Examples

```
-> user lockout-threshold 3
-> user lockout-threshold 0
```

Release History

Release 5.1; 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 2260, 2360

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** or **configuration snapshot** command to save user settings over a reboot.

Examples

```
-> user lockout-duration 60
-> user lockout-duration 0
```

Release History

Release 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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.
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 2260, 2360

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 5.1; command 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; command was introduced.

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 2260, 2360

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 5.1; command 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 2260, 2360

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 5.1; command 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.
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 2260, 2360

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 5.1; command 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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

Usage Guidelines

N/A

Examples

```
-> show aaa session console config
Console access admin-state: disabled
```

Release History

Release 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command was introduced.

Related Commands

user	Configures or modifies user entries in the local user database.

MIB Objects

N/A

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 –999.

Defaults

parameter	default
number	**6**

Platforms Supported

OmniSwitch 2260, 2360

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 5.1; command was introduced.

Related Commands

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 2260, 2360

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 5.1; command was 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 2260, 2360

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 5.1; command was introduced.

Related Commands

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 2260, 2360

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 5.1.R2; command introduced.

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 2260, 2360

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 5.1; command was 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 2260, 2360

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 5.1; command was 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 2260, 2360

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 5.1; command was 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
```

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

Usage Guidelines

N/A

Examples

```
-> aaa certificate verify ca-certificate ca_cert certificate cert_file
```

Release History

Release 5.1; 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 2260, 2360

Usage Guidelines

N/A

Examples

```
-> aaa certificate delete clientcert.pem
```

Release History

Release 5.1; 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 2260, 2360

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 5.1; command introduced.

Related Commands

aaa certificate view	Displays the contents of the X.509 certificate.

MIB Objects

N/A

20 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.

For commands used to configure device authentication, authorization, and accounting parameters that are used to support Access Guardian functionality, see "Chapter 19, "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 21, "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 auth-server-down** **unp auth-server-down-timeout** **unp redirect port-bounce** **unp redirect pause-timer** **unp redirect proxy-server-port** **unp redirect server** **unp redirect allowed-name** **unp 802.1x-pass-through** **unp ipv6-drop** **unp ap-mode** **unp user flush** **show unp global configuration** **show unp user** **show unp user status** **show unp user details**
UNP Profile Commands	**unp profile** **unp profile captive-portal-authentication** **unp profile captive-portal-profile** **unp profile maximum-ingress-bandwidth** **unp profile maximum-egress-bandwidth** **unp profile maximum-ingress-depth** **unp profile maximum-egress-depth** **unp profile map vlan** **show unp profile** **show unp profile map**

UNP Port Commands	**unp port-type** **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 default-profile** **unp aaa-profile** **unp port port-template** **unp direction** **unp admin-state** **unp vlan** **unp port ap-mode** **show unp port config** **show unp port bandwidth** **show unp port 802.1x statistics** **show unp port configured-vlans**
UNP Port Template Commands	**unp port-template** **show unp port-template**
Classification Rule Commands	**unp classification lldp med-endpoint** **show unp classification lldp-rule**
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**

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 2260, 2360

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 5.1; command was introduced.

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 10–1000 seconds.

Defaults

By default, the timeout value is set to 60 seconds.

Platforms Supported

OmniSwitch 2260, 2360

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 5.1; 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 authentication server down timeout value for the switch.

MIB Objects

```
alaDaUNPGlobalConfiguration
   alaDaUNPAuthServerDownTimeout
```

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 2260, 2360

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 5.1; 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

Not supported in this release.

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 5.1; 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

Not supported in this release.

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 5.1; 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 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

Not supported in this release.

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 5.1; 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 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 2260, 2360

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 5.1; command 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 2260, 2360

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 5.1; 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}{secure [enable | disable]}

Syntax Definitions

enable	Sets the AP mode default status to enabled.
disable	Sets the AP mode default status to disabled.
secure	Sets the secure ap-mode configuration.

Defaults

By default, the AP mode is enabled for the switch.

Platforms Supported

OmniSwitch 2260, 2360

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.
- Use **secure** parameter to enable or disable the secure ap-mode.

Examples

```
-> unp ap-mode disable
-> unp ap-mode enable
-> unp ap-mode enable secure enable
-> unp ap-mode enable secure disable
```

Release History

Release 5.1; command introduced.
Release 5.1R2; **secure** parameter added

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
   alaDaUNPPortApModeSecurity
```

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***]] [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).
service_id	*This parameter is not supported in this release.*
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 2260, 2360

Usage Guidelines

- Use the **port** or **linkagg** parameter to flush users on a specific port or link aggregate.
- 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.

Examples

```
-> unp user flush
-> unp user flush port 1/1/6
-> unp user flush linkagg 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 5.1; 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
```

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***]**
[maximum ingress-bandwidth *bps***[k | m]]**
[maximum egress-bandwidth *bps***[k | m]]**
[maximum ingress-depth *bps***]**
[maximum egress-depth *bps***]**

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	No list assigned
location-policy	No policy assigned
period-policy	No policy assigned
captive-portal-authentication	disabled
captive-portal-profile	No profile assigned
maximum ingress-bandwidth *bps***[k | m]**	None
maximum egress-bandwidth *bps***[k | m]**	None
maximum ingress-depth *bps*	None
maximum egress-depth *bps*	None

Platforms Supported

OmniSwitch 2260, 2360

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 ports or link aggregates.
- After a profile is created, use the **unp profile map** command to map the profile to a VLAN.
  - The profile is used to classify traffic received on UNP bridge 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 5.1; command was introduced.

Related Commands

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 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.
show unp profile	Displays the profile configuration for the switch.

MIB Objects

```
alaDaUNPProfileTable
   alaDaUNPProfileName
```

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

Not supported in this release.

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 5.1; 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

Not supported in this release.

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 5.1; 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 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

Not supported in this release.

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 5.1; command not supported.

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

Not supported in this release.

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 5.1; command not supported.

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

Not supported in this release.

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 5.1; command not supported.

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

Not supported in this release.

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 5.1; command not supported.

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 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 2260, 2360

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.
- 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.
- If a profile is mapped to a VLAN, then the profile is applied to traffic received on UNP bridge ports.

Examples

```
-> unp profile unp1-vlan map vlan 10
-> no unp profile unp1-vlan
```

Release History

Release 5.1; command was introduced.

Related Commands

unp profile	Configures a UNP profile.
show unp profile map	Displays the VLAN or service mapping configuration assigned to a UNP profile.

MIB Objects

```
alaDaUNPProfileTable
   alaDaUNPProfileName
alaDaUNPProfileMapVlanTable
   alaDaUNPProfileMapVlanVlanID
```

unp port-type

Configures UNP functionality for the specified port or link aggregate. This includes configuring the UNP port type (bridge). Traffic received on a UNP bridge port is classified using VLAN profiles and port attributes.

unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id1***[-***agg_id2***]} port-type {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).
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 2260, 2360

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.
- 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.
  - Port Mirroring destination ports (MTP).
  - STP ports.
  - Ports on which a static MAC address is configured.
  - Ports on which dynamic Source Learning is disabled.
- 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 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.

Examples

```
-> unp port 1/1-3 port-type bridge
-> no unp port 1/1
-> unp linkagg 8 port-type bridge
-> no unp linkagg 8
```

Release History

Release 5.1; 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 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

Not supported in this release.

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 5.1; command was introduced.

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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

Not supported in this release.

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command was introduced.

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 2260, 2360

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 5.1; 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 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 2260, 2360

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 5.1; 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 2260, 2360

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, 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 5.1; command was introduced.

Related Commands

show unp classification lldp-rule	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 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 2260, 2360

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.
  - 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 5.1; 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.
show unp port	Displays the UNP configuration for the port.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortIfIndex
   alaDaUNPPortDefaultProfileName
```

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 2260, 2360

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.

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 5.1; 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.

Platforms Supported

OmniSwitch 2260, 2360

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 1/1/5 802.1x-authentication
ERROR: Port Template already enforced on port, please remove it for manual config
on Port
```

Release History

Release 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 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 2260, 2360

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 5.1; command introduced.

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 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 {secure}**

no unp {port *chassis/slot/port***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} ap-mode {secure}**

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).
secure	Set the secure ap-mode configuration on port enabled or disabled.

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. Secure ap-mode is disabled by default.

Platforms Supported

OmniSwitch 2260, 2360

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
-> unp port 1/1/1 ap-mode secure
-> no unp port 1/1/1 ap-mode secure
```

Release History

Release 5.1; command was introduced.
Release 5.1R2; **secure** parameter added

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
   alaDaUNPPortApModeSecurity
```

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 is one default port template: "bridgeDefaultPortTemplate" (applied to UNP bridge ports). These template defines a default set of port parameter values that are applied at the time a port or link aggregate is configured as a UNP bridge. The default template cannot be deleted, but the template parameter values are configurable through this command.

unp port-template {*template_name* | **bridgeDefaultPortTemplate**
[802.1x-authentication]
[802.1x-authentication pass-alternate *profile_name***]**
[mac-authentication]
[mac-authentication pass-alternate *profile_name***]**
[classification]
[default-profile *profile_name***]**
[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]
[802.1x-authentication failure-policy {mac}]
[mac-authentication allow-eap {pass | fail | noauth}]
[admin-state {enable | disable}
[vlan *vlan_id* **[-***vlan_id2***] [tagged]**
[ap-mode]{secure}

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.

Defaults

The following table contains the default values for the system-defined port templates (“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
default-profile *profile_name*	none
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
admin state {enable | disable}	enabled
vlan *vlan_id* **[-***vlan_id2***] [tagged]**	none
ap-mode	enabled
ap-mode secure	disabled

Platforms Supported

OmniSwitch 2260, 2360

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.
- 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**
[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**
[802.1x-authentication failure-policy {mac}	**unp 802.1x-authentication failure-policy**
[mac-authentication allow-eap {pass | fail | noauth}]	**unp mac-authentication allow-eap**
[admin-state {enable | disable}]	**unp admin-state**
[vlan *vlan_id* **[-***vlan_id2***] [tagged]**	**unp vlan**
[ap-mode]	**unp port ap-mode**

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
-> no unp port-template port2 classification
-> no unp port-template port2
-> unp port-template pt1 ap-mode secure
-> no unp port-template pt1 ap-mode secure
```

Release History

Release 5.1; command was introduced.
Release 5.1R2; **secure** 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
  alaDaUNPPortTemplateApModeSecurity
alaDaUNPPortTemplateVlanTable
  alaDaUNPPortTemplateVlanVID
alaDaUNPPortTemplateProfileTable
  alaDaUNPPortTemplateProfile
```

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 2260, 2360

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.
  - 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.

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 5.1; 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 lldp-rule	Displays the UNP LLDP classification rule configuration.

MIB Objects

```
alaDaUNPEndPoinRuleTable
  alaDaUNPEndPoinRuleId
  alaDaUNPEndPoinProfile1
  alaDaUNPEndPoinProfile2
  alaDaUNPEndPoinProfile3
```

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

Not supported in this release.

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 5.1; command 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

Not supported in this release.

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 5.1; 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

Not supported in this release.

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 5.1; 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

Not supported in this release.

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 5.1; 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

Not supported in this release.

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 5.1; 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

Not supported in this release.

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 5.1; 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

Not supported in this release.

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 5.1; command was introduced.

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

Not supported in this release.

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 5.1; command was introduced.

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

Not supported in this release.

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.

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 5.1; command was introduced.

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

Not supported in this release.

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 5.1; 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

Not supported in this release.

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 5.1; command was introduced.

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

Not supported in this release.

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 5.1; 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
```

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 2260, 2360

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 that is mapped to the UNP profile.

Examples

```
-> show unp profile
Profile Name: unp1-vlan
    Qos Policy      = -,
    Location Policy = -,
    Period Policy   = -,
    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

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: 2

-> show unp profile unp1-vlan
Profile Name: unp1-vlan
    Qos Policy      = -,
    Location Policy = -,
    Period Policy   = -,
    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	*Not supported in this release.*
Location Policy	*Not supported in this release.*
Period Policy	*Not supported in this release.*
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	*Not supported in this release.*
Mobile Tag	*Not supported in this release.*
SAA Profile	*Not supported in this release.*
Ingress BW	*Not supported in this release.*
Egress BW	*Not supported in this release.*
Ingress Depth	*Not supported in this release.*
Egress Depth	*Not supported in this release.*
Inact Interval	*Not supported in this release.*
Mac-Mobility	*Not supported in this release.*
Kerberos Auth	*Not supported in this release.*

Release History

Release 5.1; command was introduced.

Related Commands

show unp classification lldp-rule	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
   alaDaUNPProfileCPortalAuthentication
   alaDaUNPProfileRedirect
   alaDaUNPProfileCPortalProfile
```

show unp profile map

Displays the VLAN, mapping configuration assigned to a UNP profile.

show unp profile [*profile_name***] map {vlan}**

Syntax Definitions

profile_name	The name of the UNP to display.
vlan	Displays the VLAN mapping configuration for a UNP profile.

Defaults

By default, the VLAN, mapping configuration for all profiles is displayed.

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- Enter a UNP profile name with this command to display the mapping information for a specific profile.
- Only one VLAN 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
```

Release History

Release 5.1; command was introduced.

Related Commands

unp profile map vlan	Configures the mapping of a standard VLAN to a UNP 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 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 2260, 2360

Usage Guidelines

- UNP global parameter settings determine specific actions related to the following:
  - 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
  Secure AP Mode                   = Disabled
  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	*Not supported in this release.*
Dynamic Profile Configuration	*Not supported in this release.*
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	*Not supported in this release.*
Force L3-Learning Port Bounce	*Not supported in this release.*
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.

output definitions

System-default service-mod	*Not supported in this release.*
System-default service-base	*Not supported in this release.*
System-default Multicast-Mode	*Not supported in this release..*
System-default Vlan-Xlation	*Not supported in this release.*
System-default Multicast-Group	*Not supported in this release.*
System-default far-end-ip-list	*Not supported in this release.*
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	*Not supported in this release.*
Global Mac-Mobility	*Not supported in this release.*

Release History

Release 5.1; command was introduced.

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 classification lldp-rule

Displays the UNP Link Layer Discovery Protocol (LLDP) classification rule configuration for the switch. An LLDP classification rule is used specifically for IP phones and OmniAccess Stellar Access Point (AP) devices.

show unp classification lldp-rule

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

The output display includes a built-in LLDP classification rule for access points that is assigned to a built-in profile named “defaultWLANProfile”. This rule cannot be removed from the switch configuration, but the profile designation for the rule can be changed.

Examples

```
-> show unp classification lldp-rule
MED Endpoint Profile1 Name               Profile2 Name           Profile3 Name
-------------+---------------------------+-----------------------+----------------------
IP-Phone     unp1-vlan                   -                             -
Access-Point defaultWLANProfile          -                             -

Total LLDP Rule Count: 2
```

output definitions

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.
Profile1, Profile2, Profile3	The name of the UNP profile to which the rule is applied. Configured through the **unp profile** command.

Release History

Release 5.1; command was introduced.

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

N/A

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}]**

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.

Defaults

By default, configuration information for all UNP ports or link aggregates is displayed.

Platforms Supported

OmniSwitch 2260, 2360

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**) 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
1/36       5 Bridge Enabled  Enabled  Disabled DefUnp     1XProf1    MacPAS    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         0 Bridge Disabled Disabled Enabled  unp-1001     -          -       Disabled
15         0 Bridge Disabled Disabled Disabled unp-1001     -          -       Disabled

-> show unp port 2/1/9 config
Port  2/1/9
  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                       = Disabled,
  Default Profile                 = -,
  Port Domain Num                 = 0,
  AAA Profile                     = -,
  Port Template                   = -,
  Admin State                     = Enabled,
  Dynamic Service                 = spb,
  PVLAN Port Type                 = -,
  Force L3-Learning               = Disabled,
  Force L3-Learning Port Bounce   = Disabled,
  AP Mode                         = Enabled,
  Secure AP Mode                  = Enabled,
  802.1x Parameters:
          Tx-Period         = 30,
          Supp-Timeout      = 30,
          Max-req           = 2,
```

output definitions

Port/LagID	The port or link aggregate on which UNP is enabled. Configured through the **unp port-type** command.
Port Domain	*Not supported in this release.*
Type	The type of UNP port (**Bridge**). UNP bridge ports classify traffic into VLAN 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.

output definitions

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	*Not supported in this release.*

Release History

Release 5.1; command was introduced.
Release 5.1R2; **secure** parameter added

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 2260, 2360

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

-> 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
```

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**).
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**).

output definitions

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	*Not supported in this release.*
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	*Creating and assigning port domain IDs is not supported in this release.*
AAA Profile	The name of an AAA profile assigned to the UNP port or link aggregate. Configured through the **unp aaa-profile** command.
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	*Not supported in this release.*
PVLAN Port Type	*Not supported in this release.*
Force L3-Learning	*Not supported in this release.*
Force L3-Learning Port Bounce	*Not supported in this release.*
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.

output definitions

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.

Release History

Release 5.1; command was introduced.

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.

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 2260, 2360

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 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:
  - 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	*Creating and assigning port domain IDs is not supported in this release.*
Type	The type of UNP port (**Bridge**). Configured through the **unp port-type** command.
Max Ingress Bandwidth	The maximum ingress bandwidth value applied to the UNP port.
Ingress BW Source	The source from which the maximum ingress bandwidth value was updated on the port (**QoS**).
Ingr BW Profile	*Not supported in this release.*
Max Egress Bandwidth	The maximum egress bandwidth value applied to the UNP port.
Egress BW Source	The source from which the maximum egress bandwidth value was updated on the port (**QoS**).
Egress BW Profile	*Not supported in this release.*
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.
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.

Release History

Release 5.1; command 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command introduced.

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-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.

Defaults

By default, displays a summary of the configuration information for all port templates.

Platforms Supported

OmniSwitch 2260, 2360

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.

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
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 bridgeDefaultPortTemplate
                                802.1x                    Mac-Auth         Redirect
Template Name            802.1x   Pass-Alt Profile Mac-Auth Pass-Alt Profile Port-Bounce Class.   Trust-Tag
-------------------------+--------+----------------+--------+----------------+-----------+--------+---------
bridgeDefaultPortTemplate Enabled   -              Enabled    -              Disabled    Enabled  Enabled

-> show unp port-template port-2 config

Port Template: unp-port2 config
  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                 = -,
  AP Mode                         = Enabled,

-> show unp port-template bridgeDefaultPortTemplate config

Port Template: bridgeDefaultPortTemplate
  802.1x Authentication           = Enabled,
  802.1x Pass Alternate Profile   = -,
  Mac Authentication              = Enabled,
  Mac-Auth Pass Alternate Profile = -,
  Classification                  = Enabled,
  Trust-tag                       = Disabled,
  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,
  AP Mode                         = Enabled,
```

output definitions

Port Template	The name of the port template. By default, 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	*Not supported in this release.*
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. *Creating and assigning domain IDs is not supported.*
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	*Not supported in this release.*
Force L3-Learning Port Bounce	*Not supported in this release.*
Admin State	The administrative status of the UNP port configuration (**Enabled** or **Disabled**).

output definitions

Dynamic Service	*Not supported in this release.*
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 5.1; command introduced.

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***]] [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.
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 2260, 2360

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     Bridge  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 Bridge  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**).
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 5.1; 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 unp profile	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***] [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).
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 2260, 2360

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 5.1; 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 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***]] [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.
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 2260, 2360

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
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          : -,
Redirect Url                   : -,
SIP Call Type                  = Not in a call,
SIP Media Type                 = None,
Applications                   = None

  MAC-Address: 00:00:00:00:00:02
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,
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
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,
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.
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.
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 5.1; command was introduced.

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 unp profile	Displays the UNP configuration for the switch.
show unp port	Displays the UNP configuration for the port.

MIB Objects

N/A

21 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command 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.
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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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).
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 2260, 2360

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 5.1; 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 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 2260, 2360

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 5.1; command introduced.

Related Commands

port-security	Enables or disables Learned Port Security (LPS) on the switch port(s).
clear interfaces	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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; 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.

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command introduced.

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
```

BLANK PAGE

22 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
show ip dynamic-proxy-arp

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 2260, 2360

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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 2260, 2360

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 5.1.R2; 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**

Platforms Supported

Not supported in this release.

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.
- When dynamic proxy ARP is enabled, port-group allocation will be triggered. The TCAM manager will respond as success if the port-group allocation is a success. If QoS is already using the port-groups, the TCAM manager will respond with a failure and an error is displayed.
- Dynamic proxy ARP can be enabled on only two port-groups. If QoS is already using the port-groups, an error message is displayed.

Examples

```
-> port-mapping 1 dynamic-proxy-arp enable
-> port-mapping 1 dynamic-proxy-arp disable
```

Release History

Release 5.1R1; 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.
show ip dynamic-proxy-arp	Displays the ARPs learned through dynamic proxy.

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 2260, 2360

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 5.1.R2; 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
   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 2260, 2360

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 5.1.R2; 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
```

show ip dynamic-proxy-arp

Displays the ARPs learned through dynamic proxy.

show ip dynamic-proxy-arp

Syntax definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- This command shows the information related to the router IP.
- To view the output, dynamic proxy must be enabled on the port mapping session, DHCP snooping must be enabled on the VLAN.

Examples

```
-> show ip dynamic-proxy-arp

  Router IP Addr     Hardware Addr             Vlan         Interface
-----------------+---------------------------+------------+---------------
 10.20.35.3         e9:ca:ab:e3:23:4c          500           1/1/23
```

output definitions

Router IP Addr	Displays the IP address of the router learned through option-3 in DHCPACK message.
Hardware Addr	Displays the MAC address of the router.
Vlan	Displays the VLAN associated with the router.
Interface	The exact interface on which the router IP was learned.

Release History

Release 5.1.R2; command introduced.

Related Commands

port-mapping dynamic-proxy-arp	Enables or disables the dynamic proxy ARP functionality for the port mapping session.

MIB Objects

```
alaIpNetToMediaDpaIp
alaIpNetToMediaDpaPhysAddress
alaIpNetToMediaDpaChassisId
alaIpNetToMediaDpaSlot
alaIpNetToMediaDpaPort
```

BLANK PAGE

23 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.
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.
enable	Enables port mirroring status.
disable	Disables port mirroring status.

Defaults

parameter	default
bidirectional | inport | outport	**bidirectional**
enable | disable	**disable**

Platforms Supported

OmniSwitch 2260, 2360

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..
- 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).
- 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.
- 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 5.1; command introduced.

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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
```

24 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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
```

25 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 2260, 2360

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 5.1; 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.
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 2260, 2360

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 5.1; 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***}**

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.

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 2260, 2360

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 5.1; command was introduced.

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 2260, 2360

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.
  - 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 5.1; command was introduced.

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command was introduced.

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 2260, 2360

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.

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 Chassis 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 Chassis local0.info swlogd: ChassisSupervisor fan & temp Mgr
info(5) Alert: PS1 airFlow unknown yet- duplicated 5 times!
```

```
Sep 30 13:26:16 Chassis local0.info swlogd: ChassisSupervisor fan & temp Mgr
info(5) Alert: PS1 airFlow unknown yet- duplicated 5 times!

Sep 30 13:27:16 Chassis 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 5.1; 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 2260, 2360

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 5.1; command was introduced.

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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
```

BLANK PAGE

26 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 2260, 2360

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 26-5.
- 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 5.1; 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 2260, 2360

Usage Guidelines

Decreasing the polling interval may impact switch performance.

Examples

```
-> health interval 20
```

Release History

Release 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; 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
```

27 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 5.1; command not supported.

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 2260, 2360

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 5.1; command introduced.

Related Commands

reload chassis-id	Reloads the specified chassis ID when running in virtual chassis mode.

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 2260, 2360

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 5.1; command introduced.

Related Commands

reload all	Reboots both CMMs from the ***certified*** directory.

MIB Objects

```
chasControlModuleTable
   chasControl
   chasControlVersionMngt
   chasControlActivateTimeout
   chasControlRedundancyTime
   chasControlDelayedActivateTimer
   chasControlWorkingVersion
   chasControlNextRunningVersion
```

reload 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command introduced.

Related Commands

write memory	Copies the current configuration (RAM) to the RUNNING DIRECTORY on the primary CMM.

MIB Objects

```
chasControlModuleTable
   chasControlVersionMngt
   chasControlWorkingVersion
```

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 2260, 2360

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
```

Release History

Release 5.1; command introduced.

Related Commands

show running-directory	Shows the current state of version and configuration management for a CMM.

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 2260, 2360

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.
- 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 5.1; command introduced.

Related Commands

show running-directory	Shows the current state of version and configuration management for a CMM.

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 2260, 2360

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 5.1; command introduced.

Related Commands

write memory	Copies the running primary RAM version of the CMM software to the RUNNING DIRECTORY.

MIB Objects

```
chasControlModuleTable
   CurrentRunningVersion
```

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 2260, 2360

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 5.1; command introduced.

Related Commands

reload all	Reboots the switch.

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 2260, 2360

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,
```

Release History

Release 5.1; 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 2260, 2360

Usage Guidelines

If no additional parameters are entered microcode information for the RUNNING CONFIGURATION is displayed.

Examples

```
-> show microcode
   /flash/working
   Package           Release                  Size     Description
-----------------+-------------------------+---------+--------------------
Aros.img          5.1.80.R01                62818640  Alcatel-Lucent OS
```

output definitions

Package	File name.
Release	Version number.
Size	File size.
Description	File description.

Release History

Release 5.1; 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 2260, 2360

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 5.1; 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.
hash-key	Keyword which will be decrypted and then used for encryption.

Defaults

parameter	default
enable | **disable**	**disable**

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

- When this command is enabled, the images and configuration from certified and running directories are copied into */uflash/2260/certified* and */uflash/2260/running* directories.
- When **write memory** is executed and backup is enabled, the configuration files and images from */flash/running-directory* are copied to */uflash/2260/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/2260/certified.*
- 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 5.1; command was introduced.

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.
hash-key	Keyword which will be decrypted and then used for encruption.

Defaults

parameter	default
enable | **disable**	**disable**

Platforms Supported

OmniSwitch 2260, 2360

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/2260/working* or */uflash/2260/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/2260/working* directory.
- 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 5.1; command was introduced.

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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
```

auto-config-abort

Aborts the Automatic Remote Configuration download process.

auto-config-abort

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

Use this command to stop the Automatic Remote Configuration download process.

Examples

```
-> auto-config-abort
```

Release History

Release 5.1; 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 2260, 2360

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:
  Aros.img:f0ff173eff38e43e0598663da2185a363fcba5bd407201d7537d0a6b9f58670e

Example

```
-> image integrity get-key working
This operation may take several minutes...

   Image Name                  SHA256 Key
---------------+-----------------------------------------------------------------
Aros.img          fb02e7689a060ff7ec301919e683f5a211c9a5e723f06b3a2652f96e07cffbeb"
```

Release History

Release 5.1; 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 2260, 2360

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:
  Aros.img:f0ff173eff38e43e0598663da2185a363fcba5bd407201d7537d0a6b9f58670e

Example

```
-> image integrity get-key /working
This operation may take several minutes...

Image Name                  SHA256 Key
----------------+-----------------------------------------
Aros.img           c64d6b23312a6f9c4b99642b31ed0e87e600bce58d6fdd089d09e1f8077bd208

-> image integrity get-key /flash/certified
This operation may take several minutes...

Image Name                  SHA256 Key
----------------+-----------------------------------------
Aros.img           3d4d488a73eb798325bacb5793ef0d67bdf377527278a6732270d3a4801bb44b
```

Release History

Release 5.1; 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
```

BLANK PAGE

28 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**
Monitoring Commands	**show system** **show hardware-info** **show chassis** **show cmm** **show slot** **show module** **show module long** **show module status** **show powersupply** **show fan** **show temperature** **show me** **show tcam utilization** **show tcam utilization detail** **show tcam app-groups** **show pmd-files** **show tech-support** **show mac-range** (command moved here from Chassis MAC Server).

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 2260, 2360

Usage Guidelines

N/A

Examples

```
-> system contact "Jean Smith Ext. 477 jsmith@company.com"
-> system contact engineering-test@company.com
```

Release History

Release 5.1; command introduced.

Related Commands

system name	Modifies the current system name of the switch.
system location	Specifies the current physical location of the switch.
show system	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 2260, 2360

Usage Guidelines

Spaces are not allowed in the system name.

Examples

```
-> system name OmniSwitch-2260
```

Release History

Release 5.1; 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.
show system	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 2260, 2360

Usage Guidelines

N/A

Examples

```
-> system location "NMS Test Lab"
-> system location TestLab
```

Release History

Release 5.1; 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.
show system	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 2260, 2360

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 28-8.

Examples

```
-> system date 08/08/2010
-> system date
08/08/2010
```

Release History

Release 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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.

Examples

```
-> system timezone mst
```

Release History

Release 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command introduced.

Related Commands

reload from	Reloads both CMMs from the specified directory.

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 2260, 2360

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/CPLD_V11.vme
-> update fpga-cpld cmm all file fpga_kit_4960
```

Release History

Release 5.1; command introduced.5.1

Related Commands

reload from	Reloads both CMMs from the specified directory.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

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 2260, 2360

Usage Guidelines

N/A

Examples

```
-> show system
System:
  Description:  Alcatel-Lucent Enterprise OS2260-24 5.1.80.R01 GA, July 09, 2021.,
  Object ID:    1.3.6.1.4.1.6486.803.1.1.2.1.1.1.3,
  Up Time:      1 days 13 hours 58 minutes and 50 seconds,
  Contact:      Alcatel-Lucent Enterprise, https://www.al-enterprise.com,
  Name:         OS2260,
  Location:     Unknown,
  Services:     78,
  Date & Time:  WED JUL 14 2021 02:45:11 (UTC)
Flash Space:
    Primary CMM:
      Available (bytes):  233091072,
      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 5.1; 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 2260, 2360

Usage Guidelines

N/A

Examples

```
-> show hardware-info
Chassis 1
CPU Manufacturer                  : Realtek
CPU Model                         : MIPS
Flash Manufacturer                : KIOXIA
Flash size                        : 461062144 bytes
RAM Manufacturer                  : Winbond
RAM size                          : 497664kB
FPGA version                      : 0.5
U-Boot Version                    : 5.1.4.R01
Power Supplies Present            : 1
NIs Present                       : 1,-"
```

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 5.1; 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 2260, 2360

Usage Guidelines

N/A

Examples

```
-> show chassis
Local Chassis ID 1 (Master)
  Model Name:                   OS2260-24,
  Module Type:                  0x80062101,
  Description:                  Chassis,
  Part Number:                  7-90,
  Hardware Revision:            002,
  Serial Number:                WKC20380012P,
  Manufacture Date:             Sep 24 2020,
  Admin Status:                 POWER ON,
  Operational Status:           UP,
  Number Of Resets:             1720,
  MAC Address:                  00:e0:b1:c7:f4:31"
```

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 5.1; 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 2260, 2360

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:                     OS2260-24,
  Module Type:                    0x80062101,
  Description:                    24G 4SFP,
  Part Number:                    7-90,
  Hardware Revision:              002,
  Serial Number:                  WKC20380012P,
  Manufacture Date:               Sep 24 2020,
  FPGA - Physical 1:              0.5,
  Admin Status:                   POWER ON,
  Operational Status:             UP,
  Max Power:                      0,
  CPU Model Type:                 RTL 9300,
  MAC Address:                    00:e0:b1:c7:f4:31,
```

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 5.1; 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.

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 2260, 2360

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
Module in chassis 1 slot 1
  Model Name:                   OS2260-24,
  Module Type:                  0x80062101,
  Description:                  24G 4SFP,
  Part Number:                  7-90,
  Hardware Revision:            002,
  Serial Number:                WKC20380012P,
  Manufacture Date:             Sep 24 2020,
  FPGA - Physical 1:            0.5,
  Admin Status:                 POWER ON,
  Operational Status:           UP,
  Max Power:                    0,
  CPU Model Type:               RTL 9300,
  MAC Address:                  00:e0:b1:c7:e4:24,
  UBOOT Version:                5.1.4.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 - Physical 1	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.
Max Power	The current power consumption for the module.
CPU Model Type	The CPU model type.
MAC Address	The MAC address assigned to the NI.
UBOOT Version	UBOOT version of the NI.

Release History

Release 5.1; command introduced.

Related Commands

show module	Displays the basic information for either a specified module or all modules installed in the chassis.
show module 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 2260, 2360

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 5.1; 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 2260, 2360

Usage Guidelines

N/A

Examples

```
->  show module long 1
Module in chassis 1 slot 1
  Model Name:                   OS2260-24,
  Module Type:                  0x80062101,
  Description:                  24G 4SFP,
  Part Number:                  7-90,
  Hardware Revision:            002,
  Serial Number:                WKC20380012P,
  Manufacture Date:             Sep 24 2020,
  FPGA - Physical 1:            0.5,
  Admin Status:                 POWER ON,
  Operational Status:           UP,
  Max Power:                    0,
  CPU Model Type:               RTL 9300,
  MAC Address:                  00:e0:b1:c7:e4:24,
  UBOOT Version:                5.1.4.R01,
```

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 - Physical 1	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.
UBOOT Version	UBOOT version of the module.

Release History

Release 5.1; 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 2260, 2360

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
Chassis/Slot      Status       Admin-Status        MAC
--------------+-------------+------------+------------------
 1/CMM-A         UP              POWER ON      00:e0:b1:c7:f4:31
 1/SLOT-1        UP              POWER ON      00:e0:b1:c7:e4:24
```

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 28-19 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 5.1; 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.

Defaults

N/A

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

N/A

Examples

```
-> show powersupply
             Total     PS
Chassis/PS   Power     Type     Status   Location
-----------+---------+--------+--------+-----------
 1/1         550       AC       UP       Internal

-> show powersupply 1
Module in slot PS-1
  Model Name:                    (APD)NW-550B01-AAAF,
  Module Type:                   0x0,
  Description:                   ALE Internal,
  Part Number:                   ,
  Hardware Revision:             ,
  Serial Number:                 ,
  Manufacture Date:              Thu Jan  1 00:00:00 1970,
  Operational Status:            UP,
  Power Provision:               550W
```

Release History

Release 5.1; 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 2260, 2360

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 5.1; command introduced.

Related Commands

show temperature	Displays the internal operating temperature of the chassis, as well as current temperature threshold settings.

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 2260, 2360

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 5.1; 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 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

Not supported in this release.

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 5.1; command not supported.

Related Commands

N/A

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 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 2260, 2360

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 5.1; command introduced.

Related Commands

show chassis	Displays the basic configuration and status information for the switch chassis.

MIB Objects

N/A

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 2260, 2360

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 5.1; command introduced.

Related Commands

show chassis	Displays the basic configuration and status information for the switch chassis.

MIB Objects

N/A

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 2260, 2360

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 5.1; command introduced.

Related Commands

show chassis	Displays the basic configuration and status information for the switch chassis.

MIB Objects

```
chasMacAddressRangeTable
   chasMacRangeIndex
   chasGlobalLocal
   chasMacAddressStart
   chasMacAddressCount
   chasMacRowStatus
```

BLANK PAGE

29 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

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 2260, 2360

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 5.1; command was introduced.

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 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 2260, 2360

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 5.1; command was introduced.

Related Commands

ntp server	Specifies an NTP server from which the switch will receive updates.

MIB Objects

```
alaNtpEnable
```

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command was introduced.

Related Commands

show ntp status	Displays the information about the current NTP status.

MIB Objects

```
alaNtpAuthenticate
```

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command was introduced.

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

Usage Guidelines

N/A

Examples

```
-> ntp vrf-name vrf1
```

Release History

Release 5.1; 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 2260, 2360

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.

Maximum Associations Allowed	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 5.1; command introduced.

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 max-associations	Configures the maximum number of associations on the 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command was introduced.

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command was introduced.

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command was introduced.

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 2260, 2360

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 5.1; 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
```

30 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 2260, 2360

Usage Guidelines

N/A

Examples

```
-> session login-attempt 5
```

Release History

Release 5.1; 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 2260, 2360

Usage Guidelines

N/A

Examples

```
-> session login-timeout 30
```

Release History

Release 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

Usage Guidelines

N/A

Examples

```
-> user profile reset
```

Release History

Release 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

Usage Guidelines

N/A

Examples

```
-> exit
```

Release History

Release 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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.

telnet {port [**default** | *service_port*] | **admin-state** [**enable** | **disable**] | *ip_address*}

Syntax Definitions

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 2260, 2360

Usage Guidelines

The default directory for Telnet is **/flash**.

Examples

```
-> telnet port 20999
-> telnet admin-state disable
-> telnet 172.17.6.228
```

Release History

Release 5.1; 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.

ssh {port [**default** | *service_port*] | **admin-state** [**enable** | **disable**] | *ip_address*}

Syntax Definitions

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 2260, 2360

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:
```

Release History

Release 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

Usage Guidelines

N/A

Examples

```
-> ssh enforce-pubkey-auth enable
```

Release History

Release 5.1; 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 2260, 2360

Usage Guidelines

N/A

Examples

```
-> ssh strong-ciphers enable
-> ssh strong-ciphers disable
```

Release History

Release 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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.

Examples

```
-> installsshkey new_ssh_user /flash/system/new_ssh_user_rsa.pub
```

Release History

Release 5.1; 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 2260, 2360

Usage Guidelines

N/A

Examples

```
-> revokesshkey new_ssh_user remote_ssh_user@192.168.10.1
```

Release History

Release 5.1; 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 30-16.

show command-log

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 2260, 2360

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 19-52.
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 5.1; 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 2260, 2360

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 5.1; 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.

show telnet

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

N/A

Examples

```
show telnet
Telnet Admin-State = Enabled
Telnet Port = 23
```

Release History

Release 5.1; 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.

show ssh

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

N/A

Examples

```
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 5.1; command was introduced.

Related Commands

command-log	Enables or disables command logging on the switch.

MIB Objects

```
alaIpSshConfig
   alaIpSshAdminStatus
   alaIpSshPort
   alaIpSshPubKeyEnforceAdminStatus
   alaIpSshStrongCiphersAdminStatus
   alaIpSshStrongHmacsAdminStatus
   alaIpSshLoginGraceTime
```

BLANK PAGE

31 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 2260, 2360

Usage Guidelines

Separate the multiple directory names that are part of the path with a slash (/).

Examples

```
-> cd
-> cd /flash/certified
```

Release History

Release 5.1; 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 2260, 2360

Usage Guidelines

The **pwd** command can also be used on the secondary CMM.

Examples

```
-> pwd
/flash
```

Release History

Release 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

Examples

```
-> freespace /flash
/flash 3143680 bytes free

-> freespace
/flash 3143680 bytes free
```

Release History

Release 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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***}**

ftp admin-state [enable | disable]

Syntax Definitions

default	Sets the port back to the default of 21.
service_port	The TCP service port number. Must be 21 or 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 2260, 2360

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
```

Release History

Release 5.1; command 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

```
systemServices
   systemServicesArg1
   systemServicesAction
```

```
alaIpFtpAdminStatus
```

show ftp

Displays the current FTP server settings like the port used for FTP, the FTP server's status.

show ftp

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

N/A

Examples

```
-> show ftp
Ftp Admin-State = Enabled
Ftp Port = 21
```

Release History

Release 5.1; command introduced.

Related Commands

ftp	Starts an FTP session.

MIB Objects

```
alaIpFtpAdminStatus
alaIpFtpPort
```

BLANK PAGE

32 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.

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 2260, 2360

Usage Guidelines

If the WebView Server is disabled, WebView Access is automatically disabled.

Examples

```
-> webview server enable
-> webview server disable
```

Release History

Release 5.1; command was introduced.

Related Commands

webview access	Enables/disables webview access on the switch.
show webview	Displays web management configuration information.

MIB Objects

```
alaIND1WebMgtConfigMIBGroup
   alaInd1WebMgtServerStatus
```

webview access

Enables or disables web management access on the switch.

webview access {enable | disable}

Syntax Definitions

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 2260, 2360

Usage Guidelines

If Web Access is enabled, the WebView Server is automatically enabled.

Examples

```
-> webview access enable
-> webview access disable
```

Release History

Release 5.1; command was introduced.

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command was introduced.

Related Commands

webview access	Enables/disables webview access on the switch.
show webview	Displays web management configuration information.

MIB Objects

```
alaIND1WebMgtConfigMIBGroup
   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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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.

show webview

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 2260, 2360

Usage Guidelines

N/A

Examples

```
-> 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 5.1; command was introduced.

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
```

33 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 2260, 2360

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 19-56.

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

Usage Guidelines

- A timer session can be scheduled using the **configuration apply** command. For more information, refer to page 33-2.
- 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 5.1; 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 2260, 2360

Usage Guidelines

N/A

Examples

```
-> configuration cancel
```

Release History

Release 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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
```

BLANK PAGE

34 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**

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 2260, 2360

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 5.1; command was introduced.

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 2260, 2360

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 5.1; command was introduced.

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

Usage Guidelines

- Refer to the command on page 34-16 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 5.1; command was introduced.

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

Usage Guidelines

- Use the **show snmp station** command on page page 34-6 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 5.1; command was introduced.

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 2260, 2360

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 5.1; command was introduced.

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 2260, 2360

Usage Guidelines

N/A

Examples

```
-> snmp authentication-trap enable
-> snmp authentication-trap disable
```

Release History

Release 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

Usage Guidelines

N/A

Examples

```
-> show snmp authentication-trap
snmp authentication trap = disable
```

Release History

Release 5.1; 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 2260, 2360

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 5.1; 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
```

BLANK PAGE

35 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
cloud-agent discovery-interval
cloud-agent remove-inconsistent-certificate
show cloud-agent status
show cloud-agent vpn status

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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; command introduced.

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 2260, 2360

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 5.1; 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
```

36 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1; 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 2260, 2360

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 5.1.R2; command 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 2260, 2360

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 5.1; 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 2260, 2360

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
```

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.

Release History

Release 5.1; 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.
ip domain-name	Sets or deletes the default domain name for DNS lookups.

MIB Objects

```
systemDNS
   systemDNSEnableDnsResolver
   systemDNSDomainName
   systemDNSNsAddr1
   systemDNSNsAddr2
   systemDNSNsAddr3
```

A Software License and Copyright Statements

This appendix contains Alcatel-Lucent and third-party software vendor license and copyright statements.

Alcatel-Lucent 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 Alcatel-Lucent Alcatel-Lucent 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 Alcatel-Lucent 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 Alcatel-Lucent 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 Alcatel-Lucent 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.** Alcatel-Lucent considers the Licensed Files to contain valuable trade secrets of Alcatel-Lucent, the unauthorized disclosure of which could cause irreparable harm to Alcatel-Lucent. 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 Alcatel-Lucent harmless from any claim, lawsuit, legal proceeding, settlement or judgment (including without limitation Alcatel-Lucent'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.** Alcatel-Lucent 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. Alcatel-Lucent 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 Alcatel-Lucent for either replacement or, if so elected by Alcatel-Lucent, 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.** Alcatel-Lucent'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 Alcatel-Lucent 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 Alcatel-Lucent and Licensee, if any, Alcatel-Lucent is under no obligation to maintain or support the copies of the Licensed Files made and distributed hereunder and Alcatel-Lucent 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 Alcatel-Lucent and certifying to Alcatel-Lucent 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. Alcatel-Lucent may terminate this License Agreement upon the breach by Licensee of any term hereof. Upon such termination by

Alcatel-Lucent, Licensee agrees to return to ALE USA, Inc.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 (e.g., Wind River and their licensors with respect to the Run-Time Module) 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 A-4 for the third party license and notice terms.

Third Party Licenses and Notices

The licenses and notices related only to such third party software are set forth below:

A. Booting and Debugging Non-Proprietary Software

A small, separate software portion aggregated with the core software in this product and primarily used for initial booting and debugging constitutes non-proprietary software, some of which may be obtained in source code format from ALE USA, Inc. for a limited period of time. ALE USA, Inc. will provide a machine-readable copy of the applicable non-proprietary software to any requester for a cost of copying, shipping and handling. This offer will expire 3 years from the date of the first shipment of this product.

B. The OpenLDAP Public License: Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1 Redistributions of source code must retain copyright statements and notices.

2 Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

3 Redistributions must contain a verbatim copy of this document.

4 The names and trademarks of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission.

5 Due credit should be given to the OpenLDAP Project.

6 The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use the Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND CONTRIBUTORS "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATIO OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

OpenLDAP is a trademark of the OpenLDAP Foundation.

C. Linux

Linux is written and distributed under the GNU General Public License which means that its source code is freely-distributed and available to the general public.

D. GNU GENERAL PUBLIC LICENSE: Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 675 Mass Ave, Cambridge, MA 02139, USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0 This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either

verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term “modification”.) Each licensee is addressed as “you”.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1 You may copy and distribute verbatim copies of the Program’s source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2 You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3 You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4 You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5 You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6 Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7 If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on

consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8 If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9 The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10 If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11 BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12 IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS.

Appendix: How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

> <one line to give the program's name and a brief idea of what it does.> Copyright (C) 19yy <name of author>
>
> This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.
>
> This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.
>
> You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

> Gnomovision version 69, Copyright (C) 19yy name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'. This is free software, and you are welcome to redistribute it under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than 'show w' and 'show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

> Yoyodyne, Inc., hereby disclaims all copyright interest in the program 'Gnomovision' (which makes passes at compilers) written by James Hacker.
>
> <signature of Ty Coon>, 1 April 1989
> Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

> URLWatch:
>
> For notice when this page changes, fill in your email address.

Maintained by: Webmaster, Linux Online Inc.
Last modified: 09-Aug-2000 02:03AM.
Views since 16-Aug-2000: 177203.

Material copyright Linux Online Inc.
Design and compilation copyright (c)1994-2002 Linux Online Inc.
Linux is a registered trademark of Linus Torvalds
Tux the Penguin, featured in our logo, was created by Larry Ewing
Consult our privacy statement

URLWatch provided by URLWatch Services.
All rights reserved.

E. University of California

Provided with this product is certain TCP input and Telnet client software developed by the University of California, Berkeley.

Copyright (C) 1987. The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

F. Carnegie-Mellon University

Provided with this product is certain BOOTP Relay software developed by Carnegie-Mellon University.

G. Random.c

PR 30872 B Kesner created May 5 2000
PR 30872 B Kesner June 16 2000 moved batch_entropy_process to own task iWhirlpool to make code more efficient

random.c -- A strong random number generator

Version 1.89, last modified 19-Sep-99

Copyright Theodore Ts’o, 1994, 1995, 1996, 1997, 1998, 1999. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, and the entire permission notice in its entirety, including the disclaimer of warranties.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission. ALTERNATIVELY, this product may be distributed under the terms of the GNU Public License, in which case the provisions of the GPL are required INSTEAD OF the

above restrictions. (This clause is necessary due to a potential bad interaction between the GPL and the restrictions contained in a BSD-style copyright.)

THIS SOFTWARE IS PROVIDED “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ALL OF WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF NOT ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

H. Apptitude, Inc.

Provided with this product is certain network monitoring software (“MeterWorks/RMON”) licensed from Apptitude, Inc., whose copyright notice is as follows: Copyright (C) 1997-1999 by Apptitude, Inc. All Rights Reserved. Licensee is notified that Apptitude, Inc. (formerly, Technically Elite, Inc.), a California corporation with principal offices at 6330 San Ignacio Avenue, San Jose, California, is a third party beneficiary to the Software License Agreement. The provisions of the Software License Agreement as applied to MeterWorks/RMON are made expressly for the benefit of Apptitude, Inc., and are enforceable by Apptitude, Inc. in addition to ALE USA, Inc.. IN NO EVENT SHALL APPTITUDE, INC. OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES, INCLUDING COSTS OF PROCUREMENT OF SUBSTITUTE PRODUCTS OR SERVICES, LOST PROFITS, OR ANY SPECIAL, INDIRECT, CONSEQUENTIAL OR INCIDENTAL DAMAGES, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, ARISING IN ANY WAY OUT OF THIS AGREEMENT.

I. Agranat

Provided with this product is certain web server software (“EMWEB PRODUCT”) licensed from Agranat Systems, Inc. (“Agranat”). Agranat has granted to ALE USA, Inc. certain warranties of performance, which warranties [or portion thereof] ALE USA, Inc. now extends to Licensee. IN NO EVENT, HOWEVER, SHALL AGRANAT BE LIABLE TO LICENSEE FOR ANY INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES OF LICENSEE OR A THIRD PARTY AGAINST LICENSEE ARISING OUT OF, OR IN CONNECTION WITH, THIS DISTRIBUTION OF EMWEB PRODUCT TO LICENSEE. In case of any termination of the Software License Agreement between ALE USA, Inc. and Licensee, Licensee shall immediately return the EMWEB Product and any back-up copy to ALE USA, Inc., and will certify to ALE USA, Inc. in writing that all EMWEB Product components and any copies of the software have been returned or erased by the memory of Licensee’s computer or made non-readable.

J. RSA Security Inc.

Provided with this product is certain security software (“RSA Software”) licensed from RSA Security Inc. RSA SECURITY INC. PROVIDES RSA SOFTWARE “AS IS” WITHOUT ANY WARRANTY WHATSOEVER. RSA SECURITY INC. DISCLAIMS ALL WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO ANY MATTER WHATSOEVER INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS.

K. Sun Microsystems, Inc.

This product contains Coronado ASIC, which includes a component derived from designs licensed from Sun Microsystems, Inc.

L. Wind River Systems, Inc.

Provided with this product is certain software ("Run-Time Module") licensed from Wind River Systems, Inc. Licensee is prohibited from: (i) copying the Run-Time Module, except for archive purposes consistent with Licensee's archive procedures; (ii) transferring the Run-Time Module to a third party apart from the product; (iii) modifying, decompiling, disassembling, reverse engineering or otherwise attempting to derive the source code of the Run-Time Module; (iv) exporting the Run-Time Module or underlying technology in contravention of applicable U.S. and foreign export laws and regulations; and (v) using the Run-Time Module other than in connection with operation of the product. In addition, please be advised that: (i) the Run-Time Module is licensed, not sold and that ALE USA, Inc. and its licensors retain ownership of all copies of the Run-Time Module; (ii) WIND RIVER DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, (iii) The SOFTWARE LICENSE AGREEMENT EXCLUDES LIABILITY FOR ANY SPECIAL, INDIRECT, PUNITIVE, INCIDENTAL AND CONSEQUENTIAL DAMAGES; and (iv) any further distribution of the Run-Time Module shall be subject to the same restrictions set forth herein. With respect to the Run-Time Module, Wind River and its licensors are third party beneficiaries of the License Agreement and the provisions related to the Run-Time Module are made expressly for the benefit of, and are enforceable by, Wind River and its licensors.

M.Network Time Protocol Version 4

The following copyright notice applies to all files collectively called the Network Time Protocol Version 4 Distribution. Unless specifically declared otherwise in an individual file, this notice applies as if the text was explicitly included in the file.

```
***********************************************************************
*                                                                     *
* Copyright (c) David L. Mills 1992-2003                              *
*                                                                     *
* Permission to use, copy, modify, and distribute this software and   *
* its documentation for any purpose and without fee is hereby         *
* granted, provided that the above copyright notice appears in all    *
* copies and that both the copyright notice and this permission       *
* notice appear in supporting documentation, and that the name        *
* University of Delaware not be used in advertising or publicity      *
* pertaining to distribution of the software without specific,        *
* written prior permission. The University of Delaware makes no       *
* representations about the suitability this software for any         *
* purpose. It is provided "as is" without express or implied          *
* warranty.                                                           *
*                                                                     *
***********************************************************************
```

N. Remote-ni

Provided with this product is a file (part of GDB), the GNU debugger and is licensed from Free Software Foundation, Inc., whose copyright notice is as follows: Copyright (C) 1989, 1991, 1992 by Free Software Foundation, Inc. Licensee can redistribute this software and modify it under the terms of General Public License as published by Free Software Foundation Inc.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

O. GNU Zip

GNU Zip -- A compression utility which compresses the files with zip algorithm.

Copyright (C) 1992-1993 Jean-loup Gailly.

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

P. FREESCALE SEMICONDUCTOR SOFTWARE LICENSE AGREEMENT

Provided with this product is a software also known as DINK32 (Dynamic Interactive Nano Kernel for 32-bit processors) solely in conjunction with the development and marketing of your products which use and incorporate microprocessors which implement the PowerPC (TM) architecture manufactured by Motorola. The licensee comply with all of the following restrictions:

1. This entire notice is retained without alteration in any modified and/or redistributed versions.

2. The modified versions are clearly identified as such. No licenses are granted by implication, estoppel or otherwise under any patents or trademarks of Motorola, Inc.

The SOFTWARE is provided on an "AS IS" basis and without warranty. To the maximum extent permitted by applicable law, MOTOROLA DISCLAIMS ALL WARRANTIES WHETHER EXPRESS OR IMPLIED, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY AGAINST INFRINGEMENT WITH REGARD TO THE SOFTWARE (INCLUDING ANY MODIFIED VERSIONS THEREOF) AND ANY ACCOMPANYING WRITTEN MATERIALS.To the maximum extent permitted by applicable law, IN NO EVENT SHALL MOTOROLA BE LIABLE FOR ANY DAMAGES WHATSOEVER.

Copyright (C) Motorola, Inc. 1989-2001 All rights reserved.

Version 13.1

Q. Boost C++ Libraries

Provided with this product is free peer-reviewed portable C++ source libraries.

Version 1.33.1

R. U-Boot

Provided with this product is a software licensed from Free Software Foundation Inc. This is used as OS Bootloader; and located in on-board flash. This product is standalone and not linked (statically or dynamically) to any other software.

Version 1.1.0

S. Solaris

Provided with this product is free software; Licensee can redistribute it and/or modify it under the terms of the GNU General Public License.

T. Internet Protocol Version 6

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE. FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL. DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS. OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION). HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT. LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The copyright of the products such as crypto, dhcp, net, netinet, netinet6, netley, netwrs, libinet6 are same as that of the internet protocol version 6.

U. CURSES

Copyright (C) 1987. The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

V. ZModem

Provided with this product is a program or code that can be used without any restriction.

Copyright (C) 1986 Gary S. Brown. All rights reserved.

W.Boost Software License

Provided with this product is reference implementation, so that the Boost libraries are suitable for eventual standardization. Boost works on any modern operating system, including UNIX and Windows variants.

Version 1.0

Copyright (C) Gennadiy Rozental 2005. All rights reserved.

X. OpenLDAP

Provided with this software is an open source implementation of the Lightweight Directory Access Protocol (LDAP).

Version 3

Copyright (C) 1990, 1998, 1999, Regents of the University of Michigan, A. Hartgers, Juan C. Gomez. All rights reserved.

This software is not subject to any license of Eindhoven University of Technology.Redistribution and use in source and binary forms are permitted only as authorized by the OpenLDAP Public License.

This software is not subject to any license of Silicon Graphics Inc.or Purdue University. Redistribution and use in source and binary forms are permitted without restriction or fee of any kind as long as this notice is preserved.

Y. BITMAP.C

Provided with this product is a program for personal and non-profit use.

Copyright (C) Allen I. Holub, All rights reserved.

Z. University of Toronto

Provided with this product is a code that is modified specifically for use with the STEVIE editor. Permission is granted to anyone to use this software for any purpose on any computer system, and to redistribute it freely, subject to the following restrictions:

1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from defects in it.

2.The origin of this software must not be misrepresented, either by explicit claim or by omission.

3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software.

Version 1.5

Copyright (C) 1986 by University of Toronto and written by Henry Spencer.

AA.Free/OpenBSD

Copyright (c) 1982, 1986, 1990, 1991, 1993 The Regents of University of California. All Rights Reserved.

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*]} 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*]} 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*]} eee {enable | disable}
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 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 port chassis/slot/port tdr enable
show interfaces [slot *chassis/slot* | port *chassis/slot/port*[-*port2*]] tdr-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*} 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 slot {*chassis/slot* | *all}* update-from *filename*
lanpower {slot *chassis/slot}* fpoe {enable | disable}
lanpower {slot *chassis/slot}* ppoe {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 } 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 {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 {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
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 aging-time
show mac-learning learning-state [vlan *vlan*[*-vlan2*] | port *chassis/slot/port* | linkagg *agg_id*]

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*]]

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]

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 [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 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

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*] 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
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*]]

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 {auto}
[no] virtual-chassis auto-vf-link-port chassis/slot/port
vc-takeover
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

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

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 *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 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 route-pref static *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]
ip directed-broadcast {enable | disable}
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*}]
no ip directed-broadcast trusted source-ip *ip_address* {*ip_address/mask* | *ip_address* mask *subnet_mask*}
ip directed-broadcast clear [trusted-source-ip {*ip_address/mask* | *ip_address* mask *subnet_mask*}]
show ip directed-broadcast [trusted-source-ip {*ip_address/mask* | *ip_address* mask *subnet_mask*}] details
ip service {all | *service_name* | port *service_port*} admin-state {enable | disable}
ip service {*service_name*} port {default | *service_port}*
ip service source-ip {Loopback0 | interface_name} [tftp] [telnet] [tacacs] [swlog] [ssh] [snmp] [sflow] [radius] [ntp] [ldap] [ftp] [dns] [all]
no ip service source-ip {Loopback0 | interface_name} [tftp] [telnet] [tacacs] [swlog] [ssh] [snmp] [sflow] [radius] [ntp] [ldap] [ftp] [dns] [all]
arp *ip_address mac_address* [alias] [arp-name *name*] [interface interface_name] [port chassis/slot/port] [linkagg agg_id]
no arp *ip_address* [alias]
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

show ip route-pref
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 service
show ip service source-ip
show ip dos arp-poison
show arp [*ip_address* | *mac_address*]
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

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
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]

IP Multicast Switching Commands

ip multicast [vlan *vlan_id*[-*vlan_id2*]] admin-state [enable | disable]
no ip multicast [vlan *vlan_id*[-*vlan_id2*]] admin-state
ip multicast [vlan *vlan_id*[-*vlan_id2*]] flood-unknown [enable | disable]
no ip multicast [vlan *vlan_id*[-*vlan_id2*]] flood-unknown
ip multicast [vlan *vlan_id*[-*vlan_id2*]] version [*version*]
no ip multicast [vlan *vlan_id*[-*vlan_id2*]] version
ip multicast port *chassis/slot/port* **max-group** [*num*] [**action** {**none** | **drop** | **replace**}]
ip multicast [vlan *vlan_id*[-*vlan_id2*]] max-group [num] [action {none | drop | replace}]
ip multicast static-neighbor vlan *vlan_id* {port *chassis/slot/port* | *linkagg agg_id}*
no ip multicast static-neighbor vlan *vlan_id* {port *chassis/slot/port* | linkagg *agg_id*}
ip multicast static-querier vlan *vlan_id* {port *chassis/slot/port* | linkagg *agg_id*}
no ip multicast static-querier vlan *vlan_id* {port *chassis/slot/port* | linkagg *agg_id*}
ip multicast static-group *ip_address* vlan *vlan_id* {port *chassis/slot/port* | linkagg *agg_id*}
no ip multicast static-group *ip_address* vlan *vlan_id* {port *chassis/slot/port* | linkagg *agg_id*}
ip multicast [vlan *vlan_id*[-*vlan_id2*]] query-interval [*seconds*]
no ip multicast [vlan *vlan_id*[-*vlan_id2*]] query-interval
ip multicast [vlan *vlan_id*[-*vlan_id2*]] last-member-query-interval [tenths_of_seconds]
no ip multicast [vlan *vlan_id*[-*vlan_id2*]] last-member-query-interval
ip multicast [vlan *vlan_id*[-*vlan_id2*]] query-response-interval [tenths_of_seconds]
no ip multicast [vlan *vlan_id*[-*vlan_id2*]] query-response-interval
ip multicast [vlan *vlan_id*[-*vlan_id2*]] unsolicited-report-interval [*seconds*]
no ip multicast [vlan *vlan_id*[-*vlan_id2*]] unsolicited-report-interval
ip multicast [vlan *vlan_id*[-*vlan_id2*]] router-timeout [*seconds*]
no ip multicast [vlan *vlan_id*[-*vlan_id2*]] router-timeout
ip multicast [vlan *vlan_id*[-*vlan_id2*]] source-timeout [*seconds*]
no ip multicast [vlan *vlan_id*[-*vlan_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*]] robustness [*robustness*]
no ip multicast [vlan *vlan_id*[-*vlan_id2*]] robustness
ip multicast [vlan *vlan_id*[-*vlan_id2*]] spoofing {enable | disable}
no ip multicast [vlan *vlan_id*[-*vlan_id2*]] spoofing
ip multicast [vlan *vlan_id*[-*vlan_id2*]] spoofing static-source-ip *ip_address*
no ip multicast [vlan *vlan_id*[-*vlan_id2*]] spoofing static-source-ip
ip multicast [vlan *vlan_id*[-*vlan_id2*] zapping [{enable | disable}]
no ip multicast [vlan *vlan_id*[-*vlan_id2*]] zapping
ip multicast [vlan *vlan_id*[-*vlan_id2*]] querier-forwarding [enable | disable]
no ip multicast [vlan *vlan_id*[-*vlan_id2*]] querier-forwarding
ip multicast [vlan *vlan_id*[-*vlan_id2*]] proxying [enable | disable]
no ip multicast [vlan *vlan_id*[-*vlan_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*]] zero-based-query [enable | disable]
no ip multicast [vlan *vlan_id*[-*vlan_id2*]] zero-based-query
ip multicast [vlan *vlan_id*[-*vlan_id2*]] forward-mode {asm | ssm | mac | auto}
no ip multicast [vlan *vlan_id*[-*vlan_id2*]] forward-mode
ip multicast [vlan *vlan_id*[-*vlan_id2*]] update-delay-interval *milliseconds*
no ip multicast [vlan *vlan_id*[-*vlan_id2*]] update-delay-interval
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*]] apply-profile *profile_name*
no ip multicast [vlan *vlan_id*[-*vlan_id2*]] appy-profile
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] admin-state [enable | disable]
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] admin-state
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] flood-unknown [enable | disable]
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] flood-unknown
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] version [*version*]
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] version
ipv6 multicast **port** *chassis/slot/port* max-group [*num*] [action {none | drop | replace}]

ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]**]** max-group [num] [action {none | drop | replace}]
ipv6 multicast static-neighbor vlan *vlan_id* {port *chassis/slot/port* | *linkagg* agg_id*}*
no ipv6 multicast static-neighbor vlan *vlan_id* {port *chassis/slot/port* | linkagg agg_id}
ipv6 multicast static-querier vlan *vlan_id* {port *chassis/slot/port* | *linkagg* agg_id*}*
no ipv6 multicast static-querier vlan *vlan_id* {port *chassis/slot/port* | linkagg agg_id}
ipv6 multicast static-group *ipv6_address* vlan *vlan_id* {port *chassis/slot/port* | *linkagg* agg_id*}*
no ipv6 multicast static-group *ipv6_address* vlan *vlan_id* {port *chassis/slot/port* | linkagg agg_id}
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] query-interval [*seconds*]
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] query-interval
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]**]** last-member-query-interval [*milliseconds*]
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]**]** last-member-query-interval
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] query-response-interval [*milliseconds*]
no ip multicast [vlan *vlan_id*[-*vlan_id2*]] query-response-interval
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] unsolicited-report-interval [*seconds*]
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] unsolicited-report-interval
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] router-timeout [*seconds*]
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] router-timeout
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] source-timeout [*seconds*]
no ip multicast [vlan *vlan_id*[-*vlan_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*]] robustness [*robustness*]
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] robustness
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] spoofing {enable | disable}
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] spoofing
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] spoofing static-source-ip *ipv6_address*
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] spoofing static-source-ip
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] zapping [enable | disable]
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] zapping
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] querier-forwarding [enable | disable]
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] querier-forwarding
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] proxying [enable | disable]
no ipv6 multicast [vlan *vlan_id*[-*vlan_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*]**]** zero-based-query [enable | disable]
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]**]** zero-based-query
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]**]** forward-mode {asm | ssm | mac | auto}
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]**]** forward-mode
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] update-delay-interval *milliseconds*
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] update-delay-interval
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*]] apply-profile *profile_name*
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] appy-profile
show ip multicast [vlan *vlan_id*]
show ip multicast {port [chassis/slot/port]}
show ip multicast forward [*ip_address*] [vlan **[***vlan_id*[-*vlan_id2*]] [all-vrf]
show ip multicast neighbor [vlan **[***vlan_id*[-*vlan_id2*]] [all-vrf]
show ip multicast querier [vlan **[***vlan_id*[-*vlan_id2*]] [all-vrf]
show ip multicast group [*ip_address*] [vlan [*vlan_id*[-*vlan_id2*]] [all-vrf]
show ip multicast source [*ip_address*] [**vlan [***vlan_id*[-*vlan_id2*]] [all-vrf]
show ip multicast tunnel [*ip_address*] [**vlan [***vlan_id*[-*vlan_id2*]] [all-vrf]
show ip multicast bridge [vlan [*vlan_id*[-*vlan_id2*] | *ip_address* | *mac_address*]] [all-vrf]
show ip multicast bridge-forward [vlan [*vlan_id*[-*vlan_id2*] | *ip_address* | *mac_address*]] [all-vrf]
show ip multicast profile [*profile_name***]**
show ipv6 multicast port [chassis/slot/port]
show ipv6 multicast forward [*ipv6_ddress*] [vlan [*vlan_id*[-*vlan_id2*]] [**all-vrf]**
show ipv6 multicast neighbor [vlan [*vlan_id*[-*vlan_id2*]] [all-vrf]
show ipv6 multicast querier [vlan [*vlan_id*[-*vlan_id2*]] [all-vrf]]
show ipv6 multicast group [*ipv6_ddress*] [vlan [*vlan_id*[-*vlan_id2*]] [all-vrf]
show ipv6 multicast source [*ipv6_ddress*] [vlan [*vlan_id*[-*vlan_id2*]] [all-vrf]
show ipv6 multicast tunnel [*ipv6_address*] [vlan [*vlan_id*[-*vlan_id2*]] [all-vrf]
show ipv6 multicast bridge [vlan *vlan_id*[-*vlan_id2*] | *ipv6_address* | *mac_address*]] [all-vrf]
show ipv6 multicast bridge-forward [vlan *vlan_id*[-*vlan_id2*] | *ipv6_address* | *mac_address*]] [all-vrf]
show ipv6 multicast profile [*profile_name***]**

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 phones [priority *priority_value* | trusted]
qos no phones
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 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*] 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 qsi {port *chassis/slot/port*[-*port2*] | linkagg *agg_id*[-*agg_id2*] | vf-link *vfl_id*} qsp {*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 log
show qos config
show qos statistics
show qos qsp [*qsp_id* | *qsp_name*] [brief | detail [port *chassis/slot/port*[-*port2*]] | linkagg *agg_id*[-*agg_id2*]]]
show qos qsi [port *chassis/slot/port*[-*port2*] | linkagg *agg_id*[-*agg_id2*] | vf-link *vfl_id*] detail
show qos qsi [port *chassis/slot/port*[-*port2*] | linkagg *agg_id*[-*agg_id2*]] summary
show qos qsi {port chassis/slot/port[-port2] | linkagg *agg_id*[-*agg_id2*]} stats [bytes | rate [bytes]]
clear qos qsi {port *chassis/slot/port*[-*port2*] | linkagg *agg_id*[-*agg_id2*]} 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*
iec message-type *message* priority *string*
iec message-type *message* flush
iec show
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 {any | *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* app-mon-application-group *group_name*
policy condition *condition_name* no app-mon-application-group
policy condition *condition_name* app-mon-application-name *app_name*
policy condition *condition_name* no app-mon-application-name
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 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 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*
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*]
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}
show aaa switch-access ip-lockout-threshold
show aaa switch-access banned-ip
show aaa switch-access priv-mask
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}

Access Guardian Commands

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 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 802.1x-pass-through
no unp 802.1x-pass-through
unp ipv6-drop
no unp ipv6-drop
unp ap-mode {enable | disable}{secure [enable | disable]}
unp user flush [port *chassis/slot/port1*[-*port2*] | linkagg *agg_id*[-*agg_id2*]] [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* 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* 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* map vlan *vlan_id*
unp {port *chassis/slot/port1*[-*port2*] | linkagg *agg_id1*[-*agg_id2*]} port-type {bridge}
no unp {port *chassis/slot/port1*[-*port2*] | linkagg *agg_id1*[-*agg_id2*]}
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*]} 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*]} 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/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/port***[**-*port2***]** | **linkagg** *agg_id*[-*agg_id2*]} ap-mode {secure}
no unp {port *chassis/slot/port***[**-*port2***]** | **linkagg** *agg_id*[-*agg_id2*]} ap-mode {secure}
unp **port**-template {*template_name* | bridgeDefaultPortTemplate
no unp port-template *template_name* [802.1x-authentication | 802.1x authentication pass-alternate | mac-authentication | mac-authentication pass-alternate | ...]
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]
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}
show unp profile [*profile_name*]
show unp profile [*profile_name*] map {vlan}
show unp global configuration
show unp classification lldp-rule
show unp {port [*chassis*/*slot/port1*[-*port2*]] | linkagg [*agg_id*[-*agg_id2*]]} [type {bridge}]
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-template [*template_name*] [config | configured-vlans | profile]
show unp user [port *chassis/slot/port*[-*port2*] | linkagg *agg_id*[-*agg_id2*]] [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*] [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*]] [profile *profile_name*] [authentication-type {none | mac | 802.1x}] [mac-address *mac_address*]

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 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*]
show ip dynamic-proxy-arp

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*

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*}
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}

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 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]*
write memory [flash-synchro]
copy running certified [flash-synchro]
modify running-directory *image_dir*
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
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}*
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 temperature [fabric [*index*] | slot [*index*] | fantray [*index*] | cmm [*index* | *cmm_letter*] | chassis-id *chassis*]
show me
show tcam utilization [*chasiss*/*slot*] [*chasiss*/*slot/tcam*]
show tcam utilization [*chasiss*/*slot*] [*chasiss*/*slot/tcam*] detail
show tcam app-groups
show pmd-files
show tech-support [layer2 | layer3 | eng [complete]]
show mac-range [*index*]

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 client admin-state {enable | disable}
ntp broadcast-client {enable | disable}
ntp broadcast-delay *microseconds*
ntp key *key* [trusted | untrusted]
ntp key load
ntp authenticate {enable | disable}
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
telnet {port [default | service_port] | admin-state [enable | disable] | *ip_address***}**
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
show telnet
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}*
ftp admin-state [enable | disable]
show ftp

Web Management Commands

webview server {enable | disable}
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
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

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

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

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

L

M

N

P

Q

R

S

T

U

V

W