Release Notes

OmniSwitch 6900/10K

Release 7.3.4.R02

These release notes accompany release 7.3.4.R02 software which is supported on the OmniSwitch 6900 and OmniSwitch 10K platforms. These release notes provide important information on individual software features and hardware modules. Since much of the information in these release notes is not included in the hardware and software user manuals, it is important that you read all sections of this document before installing new hardware or loading new software.

[IMPORTANT] *MUST READ* - This release includes changes to default AOS behavior as well as deprecating some feature support. It is required that the PREREQUISITE section be read and UNDERSTOOD prior to upgrading to AOS Release 7.3.4.R02. If, after reading the PREREQUISITE section, you still have questions, please contact Service & Support for further clarification.

Contents

Related Documentation

These release notes should be used in conjunction with OmniSwitch AOS Release 7 User Guides. The following are the titles and descriptions of the user manuals that apply to this release. User manuals can be downloaded at: http://enterprise.alcatel-lucent.com/?dept=UserGuides&page=Portal

OmniSwitch 6900 Series Hardware User Guide

Complete technical specifications and procedures for all OmniSwitch Series chassis, power supplies, and fans.

OmniSwitch 10K Hardware User Guide

Complete technical specifications and procedures for all OmniSwitch Series chassis, power supplies, and fans.

OmniSwitch AOS Release 7 CLI Reference Guide

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

OmniSwitch AOS Release 7 Network Configuration Guide

Includes network configuration procedures and descriptive information on all the major software features and protocols included in the base software package. Chapters cover Layer 2 information (Ethernet and VLAN configuration), Layer 3 information (routing protocols), security options (Authenticated Switch Access), Quality of Service (QoS), and link aggregation.

OmniSwitch AOS Release 7 Switch Management Guide

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

OmniSwitch AOS Release 7 Advanced Routing Configuration Guide

Includes network configuration procedures and descriptive information on all the software features and protocols included in the advanced routing software package. Chapters cover multicast routing (DVMRP and PIM), BGP, OSPF, OSPFv3, and IS-IS.

OmniSwitch AOS Release 7 Data Center Switching Guide

Includes and introduction to the OmniSwitch data center switching architecture as well as network configuration procedures and descriptive information on all the software features and protocols that support this architecture. Chapters cover Shortest Path Bridging MAC (SPBM), Data Center Bridging (DCB) protocols, Virtual Network Profile (vNP), and the Edge Virtual Bridging (EVB) protocol.

OmniSwitch AOS Release 7 Transceivers Guide

Includes SFP, SFP+, and QSFP transceiver specifications and product compatibility information.

Technical Tips, Field Notices

Contracted customers can visit our customer service website at: service.esd.alcatel-lucent.com.

System Requirements

Memory Requirements

The following are the standard shipped memory configurations. Configuration files and the compressed software images—including web management software (WebView) images—are stored in the flash memory.

Platform	SDRAM	Flash
OS6900-X Models	2GB	2GB
OS6900-T Models	4GB	2GB
OS6900-Q32	8GB	2GB
OS6900-X72	8GB	4GB
OS10K	4GB	2GB

UBoot and FPGA Requirements

The software versions listed below are the MINIMUM required, except where otherwise noted. Switches running the minimum versions, as listed below, do not require any UBoot or FPGA upgrades. Use the '**show hardware-info**' command to determine the current versions.

Switches not running the minimum version required should upgrade to the latest UBoot or FPGA that is available with the 7.3.4.R02 AOS software available from Service & Support.

- A separate file containing the Uboot and FPGA upgrade files is available from Service & Support.
- Please refer to the Upgrade Instructions section at the end of these Release Notes for step-by-step instructions on upgrading your switch to support 7.3.4.R02.

OmniSwitch 6900-X20/X40 - AOS Release 7.3.4.204.R02(GA)

Hardware	Minimum UBoot Release	Minimum FPGA Release
CMM (if XNI-U12E support is not needed)	7.2.1.266.R02	1.3.0/1.2.0
CMM (if XNI-U12E support is needed)	7.2.1.266.R02	1.3.0/2.2.0[1]
All Expansion Modules	N/A	N/A

1. FPGA 1.3.0/2.2.0 is required to support the XNI-U12E (Introduced in 7.3.3.R01)

OmniSwitch 6900-T20/T40 - AOS Release 7.3.4.204.R02(GA)

Hardware	Minimum UBoot Release	Minimum FPGA Release
CMM (if XNI-U12E support is not needed)	7.3.2.134.R01	1.4.0/0.0.0
CMM (if XNI-U12E support is needed)	7.3.2.134.R01	1.6.0/0.0.0[1]
All Expansion Modules	N/A	N/A

1. FPGA 1.6.0 is required to support the XNI-U12E (Introduced in 7.3.3.R01)

OmniSwitch 6900-Q32 - AOS Release 7.3.4.204.R02(GA)

Hardware	Minimum UBoot Release	Minimum FPGA Release
CMM	7.3.4.277.R01[1]	0.1.8[1]
All Expansion Modules	N/A	N/A

[1] Shipped from factory with correct version, no upgrade is available or required.

OmniSwitch 6900-X72 - AOS Release 7.3.4.204.R02(GA)[1]

Hardware	Uboot	FPGA
CMM	7.3.4.31.R02[2]	0.1.10[2]
All Expansion Modules	N/A	N/A

[1] AOS 7.3.4.R02 is the minimum version supported. The OS6900-X72 cannot be downgraded.

[2] Shipped from factory with correct version, no upgrade is available or required.

OmniSwitch 10K - Release 7.3.4.204.R02 (GA)

Module	Uboot	FPGA
CMM	7.2.1.266.R02	2.0
GNI-C48/U48	7.2.1.266.R02	0.7
GNI-U48 Daughter Card	7.2.1.266.R02	1.4
XNI-U32S	7.2.1.266.R02	2.12
XNI-U16L	7.3.1.325.R01	0.3
XNI-U16E	7.3.1.325.R01	0.3
XNI-U32E	7.3.1.325.R01	0.3
QNI-U4E	7.3.1.325.R01	0.3
QNI-U8E	7.3.1.325.R01	0.3

[IMPORTANT] *MUST READ*: AOS Release 7.3.4.R02 Prerequisites and Deployment Information

Please note the following important release specific information prior to upgrading or deploying this release. The information below covers important upgrade requirements, changes in AOS default behavior, and the deprecation of features.

- Prior to upgrading to AOS Release 7.3.4.R02 please refer to Appendix A for important best practices, prerequisites, and step-by-step instructions.
- All switches that ship from the factory with AOS Release 7.3.4.R02 will default to VC mode and attempt to run the automatic VC, automatic remote configuration, and automatic fabric protocols.
- The Multi-Chassis Link Aggregation CLI and functionality has been deprecated in AOS Release 7.3.4.R02. If Multi-Chassis Link Aggregation support is required DO NOT upgrade to AOS Release 7.3.4.R02.
- If upgrading from AOS Release 7.3.1 note the following:

- VRF functionality was updated to use the new profiles capability in 7.3.2.R01. These new profiles are not compatible with earlier versions of AOS. It's strongly recommened to create a backup of the 7.3.1 configuration prior to upgrading to prevent the VRF configuration having to be rebuilt if a switch should need to be downgraded.
- A new predefined DCB profile 11 was introduced in 7.3.2.R01, this will overwrite any existing custom profile 11.

- The NTP, SNMP, and SFLOW commands for specifying a source IP address were deprecated beginning with release 7.3.4.R01 and replaced with the IP Managed Services feature. If the following commands were configured, please use the **ip service source-ip** command after upgrading to 7.3.4.R02 to reconfigure the source IP address.

```
-> ntp src-ip preferred
-> snmp source-ip-preferred
-> sflow agent ip
```

- When using the **gateway** parameter with the 'ip static-route [ipv4Addr | ipv4Addr/prefixLen] gateway ipv4Addr' command, for example:

```
-> 'ip static-route 10.255.0.0/16  gateway 127.0.0.1'
```

If the gateway is a local IP interface, the command will not be accepted after upgrading to 7.3.4.R02. Use the interface parameter in place of the gateway parameter, for example:

```
-> 'ip static-route 10.255.0.0/16  interface Loopback
```

Demo License Operation

Beginning in 7.3.4.R01 and continuing in 7.3.4.R02 a 45-day Demo Advanced license is available. This license may or may not be automatically activated depending on the switch configuration. See the table below for an explanation of the switch behavior with the Demo Advanced license.

	Standalone/VC-1	VC-2 or more	Comments
Demo Advanced License Installation	**Demo Advanced License** Automatically activated upon boot up if no Advanced license is already installed and no vcboot.cfg and boot.cfg file exists in the Certified directory or they are both zero byte files.	**Demo Advanced License** Automatically activated upon boot up if no Advanced license is already installed and no vcboot.cfg and boot.cfg file exists in the Certified directory or they are zero byte files.	
Reboot Behavior After Demo License Expiration	If no Advanced features were ever enabled. – **Switch will not reboot.**	If no Advanced features were ever enabled. – **Switch will reboot.**	VC-1 or standalone does not require the Advanced license in 7.3.4.R02. VC-2 or more requires Advanced license.
	If Advanced features were enabled (even if the configurations were cleared or disabled before 45-day demo period). **- Switch will reboot.**	If Advanced features were enabled (even if the configurations were cleared/disabled before 45 days demo period). – **Switch will reboot**	
	If permanent license is installed before the expiration of demo license. – **Switch will not reboot.**	If permanent license is installed before the expiration of demo license. **- Switch will not reboot**	

<u>New Hardware Support</u>

OS6900-X72

The OS6900-X72 is a 10/40-Gigabit Ethernet fixed configuration chassis in a 1U form factor with forty-eight (48) 1/10-Gigabit SFP+ ports and six (6) 40-Gigabit QSFP+ ports, redundant AC or DC power and front to back cooling. The switch includes:

- 1 - Console Port (RJ-45 Form Factor - RS-232)
- 1 - USB Port (For use with Alcatel-Lucent OS-USB-FLASHDR USB flash drive)
- 1 - EMP Port
- 48 – SFP+ Ports
- 6 –QSFP+ Ports (1G not supported on these ports)
- 1 Slot – Fan Tray
- 2 Slots – Power Supplies (AC or DC)

Port groups 49-54 support 4X10G splitter cables which allows for up to seventy-two (72) 10-Gigabit ports on an OS6900-X72. When a splitter cable is used the port numbering scheme changes to accommodate the 4 10-Gig ports by using letters a, b, c, d to refer to the 10-Gig sub-ports. When referring to a single sub-port the port letter should be used to differentiate between all the sub-ports. If no letter is given the command assumes port 'a', for example.

```
    -> show interfaces 1/1/49 – refers to interface 1/1/49a

    -> show interfaces 1/1/49a – refers to interface 1/1/49a

    -> show interfaces 1/1/49d – refers to interface 1/1/49d
```

When referring to a range of ports the lettered sub-ports are implied, for example:

```
    -> show interfaces 1/1/49-50 – refers to interfaces 1/1/49a, 49b, 49c, 49d and 1/1/50a, 50b, 50c,
50d

    -> show interfaces 1/1/49a-49c – refers to interfaces 1/1/49a, 49b, 49c

    -> show interfaces 1/1/49-50a – refers to interfaces 1/1/49a, 49b, 49c, 49d, and 1/1/50a.
```

New Software Features and Enhancements

The following software features are being introduced with the 7.3.4.R02 release, subject to the feature exceptions and problem reports described later in these release notes:

Features listed as ‘Base’ are included as part of the base software and do not require any license installation. Features listed as ‘Advanced’ or “Data Center” require the installation of a license.

7.3.4.R02 New Feature/Enhancements Summary

Feature	Platform	License
Data Center Feature Support		
- RFP on SPB UNI Port	OS6900/10K	Data Center
Layer 3 Feature Support		
- Increase OSPFv2 Limits	OS10K	Base
Management Feature Support		
- Beacon LED	OS6900-Q32/X72	Base
Virtual Chassis Feature Support		
- Virtual Chassis Split Protection (VCSP)	OS6900/10K	Advanced

Data Center Feature Descriptions

RFP on SPB UNI Port

Prior to this feature when a link on one side of a media converter failed, the other side would continue to transmit packets waiting for a response. LFPT (Link Fault Pass Through) is a troubleshooting feature that ensures if a link on one side of the media converter fails the media converter will force the link down on its link partner notifying the other side that the link is down. As an alternative to LFPT, Remote Fault Propagation (RFP) on SPB UNI ports can be used. RFP will ensure that when one SAP interface link is down the other end will be brought down by software.

The method used to detect/trigger the failed condition and propagate the fault is an OAM based messaging solution which uses CCM packet as the information carrier medium to carry port and ISID information.

Layer 3 Feature Descriptions

Increase OSPFv2 Limits

This feature enhancement increases the maximum number of supported OSPFv2 limits to the following on an OmniSwitch 10K:

- Areas – 20 per switch
- Interfaces – 350 per area / 350 per switch
- Neighbors – 350 per area / 350 per switch

An OSPF router with 350 interfaces in one OSPF area will originate a Router-LSA as large as 4,600 bytes. This is well over the default IP interface MTU of 1500 bytes. To ensure that all OSPF routers in the domain have the same view of the link topology, it is strongly recommended that all OSPF interfaces in the domain support larger MTU sizes. This can be achieved by increasing the MTU-IP value of the VLAN configured with the OSPF interface. For example, the following will change the MTU size to 5000 bytes:

```
-> vlan 20 mtu-ip 5000
```

Management Feature Descriptions

Beacon LED Feature

The beacon LED feature provides a mechanism to allow an administrator to configure the color and the mode of an SFP+ and QSFP+ port LED. This can useful in the following scenarios:

- Port identification: Can help to identify a particular port(s) needing attention or where a cable may need to be swapped. Manually changing the color or mode of the port LED can help to guide a technician to a particular port. This can also be helpful in a highly dense mesh of cabling.
- Power Savings: Large Data Centers are looking for ways to reduce power consumption. One way could be to power off every LED on every node if operating properly and only use the LEDs for indicating ports that need attention.
- Tracking link activity: Servers are often configured in clusters for certain functions or applications. Ports could be color coded to differentiate between clusters.

LED Color and Mode Settings:

- LED Color – The color of the LED can be changed to yellow, white, red, magenta, green, blue, aqua, or off.
- Activity Mode – The LED will blink normally based on the port activity but the color of the LED can be changed.

- Solid Mode – The LED will not blink based on the port activity, it will always be solid. The color of the LED can be changed.

Note: The Beacon LED feature is not supported on sub-ports 'b', 'c', or 'd' when an interface is operating in 4X10G mode. Additionally, only Solid mode is supported on sub-port 'a' for 4X10G interfaces.

Virtual Chassis Feature Descriptions

Virtual Chassis Split Protection (VCSP)

In the case of a virtual chassis splitting into disjointed sub-VCs due to the failure of one or more VLFs both of the resulting VCs could end up having the same system MAC and IP addresses. Since there is no communication between these individual VCs due to the VFL failure they end up communicating with the rest of the network devices using the same MAC and IP addresses. This VC split scenario is disruptive to the network as the conflicting MAC and IP addresses can lead to layer 2 loops and layer 3 traffic disruption.

VCSP provides the following benefits:

- Avoid network disruptions by preventing duplicate MAC and IP addresses on the network.
- The sub-VC that forms out of the VC split is able to detect that a split has occurred by use of a helper switch.
- Once the VC split condition has been determined, the sub-VC will put its front-panel ports into an operationally down state preventing traffic forwarding and avoiding loops and possible traffic disruption. The VCSP link aggregate ports will remain up.
- A trap can be sent by the active-VC indicating the VC split state. The trap indicates that the split has occured and which elements are in the operationally down sub-VC.
- The entire VC will automatically recover when the sub-VC rejoins the VC.

This feature can also be leveraged for detecting a VC split in a remote VC topology where the VC may consist of elements located in different physical locations.

Note: A redundant VFL cable should be used for best traffic convergence in the event of failure.

Unsupported Software Features

The following CLI commands and Web Management options may be available in the switch software for the following features. These features are not supported but may be available as Early Availability features:

Feature	Platform	License
Dual-Home Link Aggregation	OS6900/OS10K	Base
NetSec	OS6900/OS10K	Base

Unsupported CLI Commands

The following CLI commands may be available in the switch software for the following features. These commands are not supported but may be available as Early Availability features:

Software Feature	Unsupported CLI Commands
Chassis	reload slot
SLB	server-cluster port all

Open Problem Reports and Feature Exceptions

The problems listed here include problems known at the time of the product's release. Any problems not discussed in this section should be brought to the attention of the Alcatel-Lucent Technical Support organization as soon as possible. Please contact customer support for updates on problem reports (PRs) where no known workaround was available at the time of release.

Layer 2

PR	Description	Workaround
204470	PVST+ status may be displayed as OFF when interoperating between an OmniSwitch and a Cisco switch using link aggregation with PVST+ compatibility enabled.	This is a display issue only, there is no functional impact.

Hardware

PR	Description	Workaround
203474	After removing both CMMs from an OS10K chassis, it could take up to 120 seconds for the NIs to power down.	There is no known workaround at this time.
206543	On an OS6900-X72, when auto-negotiation is disabled and the remote device has auto-negotiation enabled, the link will come up with the speed according to the type of transceiver present in the port (i.e. SFP+ 10G, SFP 1G). This behavior is different than other OS6900-X20/X40 models on which the link will not come UP until auto-negotiation on the remote-end is also disabled.	Configure auto-negotiation to be the same on both ends.
206579	In a Q32/X72, when a port capable of 40G/10G (splitter) is configured as 4x10G and if a 40G DAC/fiber cable is inserted instead of a splitter, the port is still functional as a 10G port.	Insert the correct splitter cable.
209535	Unable to configure dual-speed SFP to 1G on an 6900-X72. Displays message "ERROR: port speed setting is not supported on OS6900-X72".	There is no known workaround at this time.

Layer 3

PR	Description	Workaround
204588	ICMP ping to server cluster ip failed when static arp enabled on switch. Impact only when ping to server cluster ip from switch. This is an impact to customer for troubleshooting. But, No impact on traffic forwarding addressing to server cluster ip.No issue when HAVLAN	Ping to server cluster IP works fine with dynamic arp.

	disabled.	
207150	On an IP over SPB configuration, when a frame is received on a SAP port with a destination address as a router MAC (local router or vrrp) on the switch, the frame’s VLAN tag is removed causing the frame to not be handled properly for the SPB domain.	Enable VLAN translation to preserve the VLAN header in cases where an ingress frame is using the local router or VRRP MAC address of the switch.

Virtual Chassis

PR	Description	Workaround
209311	When performing an ISSU upgrade from 7.3.4.R01 to 7.3.4.R02 on a VC of 3 OS6900s with auto-VFL, when the second Slave chassis reboots it does not re-establish the auto-VFL with the first Slave chassis that has already rebooted with the new code. When the Master reboots the VC is split and all the chassis reboot again before recovering. This issue is only seen with a VC of 3 OS6900s using auto-VFL.	There is no known woarkaround at this time.
207463	On an OS10K port mirroring does not work when mirrored traffic has to go over an Auto-VFL.	1. Put both the source and destination mirror ports on the same chassis when using port mirroring on a 10K VC with auto-VFL. 2. Change from Auto-VFL to Static-VFL.

System

PR	Description	Workaround
128503	Oversize frames counter in CLI command 'show interfaces slot/port' is not incrementing when the switch is transmitting/receiving oversize frames.	Use the 'show interfaces slot/port accounting' command and refer to the 'Oversize' parameter.
206546	The MTU of the interface is set with an additional 4-bytes than the configured MTU value. As a result the frame size that can be successfully forwarded is 9220 for a physical port with default value of 9216 (range: 1518 to 9216).	While setting the maximum frame size on interfaces, 4 bytes should be deducted from the actual size.

Hot Swap/Redundancy Feature Guidelines

Hot Swap Feature Guidelines

Refer to the table below for hot swap/insertion compatibility. If the modules are not compatible a reboot of the chassis is required after inserting the new module.

- For the OS6900-X40 wait for first module to become operational before adding the second module.
- All module extractions must have a 30 second interval before initiating another hot swap activity.
- All module insertions must have a 5 minute interval AND the OK2 LED blinking green before initiating another hot swap activity.

Existing Expansion Slot	Hot-swap/Hot-insert compatibility
Empty	OS-XNI-U12, OS-XNI-U4
OS-XNI-U4	OS-XNI-U12, OS-XNI-U4
OS-XNI-U12	OS-XNI-U12, OS-XNI-U4
OS-HNI-U6	OS-HNI-U6
OS-QNI-U3	OS-QNI-U3
OS-XNI-T8	OS-XNI-T8
OS-XNI-U12E	OS-XNI-U12E

OS6900 Hot Swap/Insertion Compatibility

Existing Slot	Hot-swap/Hot-insert compatibility
Empty	All modules can be inserted
OS10K-GNI-C48E	OS10K-GNI-C48E
OS10K-GNI-U48E	OS10K-GNI-U48E
OS10K-XNI-U32S	OS10K-XNI-U32S
OS10K-XNI-U16L	OS10K-XNI-U16L
OS10K-XNI-U16E	OS10K-XNI-U16E
OS10K-XNI-U32E	OS10K-XNI-U32E
OS10K-QNI-U4E	OS10K-QNI-U4E
OS10K-QNI-U8E	OS10K-QNI-U8E

OS10K Hot Swap/Insertion Compatibility

Hot Swap Procedure

The following steps must be followed when hot-swapping expansion modules.

1. Disconnect all cables from transceivers on module to be hot-swapped.
2. Extract all transceivers from module to be hot-swapped.
3. Extract the module from the chassis and wait approximately 30 seconds before inserting a replacement.
4. Insert replacement module of same type.
5. Wait for a message similar to the following to display on the console or issue the command **-> show module status** and wait for operational status to show '**UP**':

   ChassisSupervisor niMgr info message:

   +++ Expansion module 2 ready!
6. Re-insert all transceivers into the new module.
7. Re-connect all cables to transceivers.

Technical Support

Alcatel-Lucent technical support is committed to resolving our customer's technical issues in a timely manner. Customers with inquiries should contact us at:

Region	Phone Number
North America	800-995-2696
Latin America	877-919-9526
European Union	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484

Email: esd.support@alcatel-lucent.com

Internet: Customers with Alcatel-Lucent service agreements may open cases 24 hours a day via Alcatel-Lucent's support web page at: service.esd.alcatel-lucent.com.

Upon opening a case, customers will receive a case number and may review, update, or escalate support cases on-line. Please specify the severity level of the issue per the definitions below. For fastest resolution, please have telnet or dial-in access, hardware configuration—module type and revision by slot, software revision, and configuration file available for each switch.

Severity 1 Production network is down resulting in critical impact on business—no workaround available.

Severity 2 Segment or Ring is down or intermittent loss of connectivity across network.

Severity 3 Network performance is slow or impaired—no loss of connectivity or data.

Severity 4 Information or assistance on product feature, functionality, configuration, or installation.

Third Party Licenses and Notices

Legal Notices applicable to any software distributed alone or in connection with the product to which this document pertains, are contained in files within the software itself located at: **/flash/foss**.

Appendix A: General Upgrade Requirements and Best Practices

This section is to assist with upgrading an OmniSwitch. The goal is to provide a clear understanding of the steps required and to answer any questions about the upgrade process prior to upgrading. Depending upon the AOS version, model, and configuration of the OmniSwitch various upgrade procedures are supported.

Standard Upgrade - The standard upgrade of a standalone chassis or virtual chassis (VC) is nearly identical. All that's required is to upload the new image files to the *Running* directory and reload the switch. In the case of a VC, prior to rebooting the Master will copy the new image files to the Slave(s) and once the VC is back up the entire VC will be synchronized and running with the upgraded code.

ISSU - The In Service Software Upgrade (ISSU) is used to upgrade the software on a VC or modular chassis with minimal network disruption. Each element of the VC is upgraded individually allowing hosts and switches which are dual-homed to the VC to maintain connectivity to the network. The actual downtime experienced by a host on the network should be minimal but can vary depending upon the overall network design and VC configuration. Having a redundant configuration is suggested and will help to minimize recovery times.

Virtual Chassis - The VC will first verify that it is in a state that will allow a successful ISSU upgrade. It will then copy the image and configuration files of the ISSU specified directory to all of the Slave chassis and reload each Slave chassis from the ISSU directory in order from lowest to highest chassis-id. For example, assuming chassid-id 1 is the Master, the Slave with chassis-id 2 will reload with the new image files. When Slave chassis-id 2 has rebooted and rejoined the VC, the Slave with chassis -id 3 will reboot and rejoin the VC. Once the Slaves are complete they are now using the new image files. The Master chassis is now rebooted which causes the Slave chassis to become the new Master chassis. When the original Master chassis reloads it comes back as a Slave chassis. To restore the role of Master to the original Master chassis the current Master can be rebooted and the original Master will takeover, re-assuming the Master role.

Modular Chassis - The chassis will first verify that it is in a state that will allow a successful ISSU upgrade. It will then copy the image and configuration files of the ISSU specified directory to the secondary CMM and reload the secondary CMM which becomes the new primary CMM. The old primary CMM becomes the secondary CMM and reloads using the upgraded code. As a result of this process both CMMs are now running with the upgraded code and the primary and secondary CMMs will have changed roles (i.e., primary will act as secondary and the secondary as primary). The individual NIs can be reset either manually or automatically (based on the NI reset timer).

Staggered Upgrade - A staggered upgrade is similar to ISSU but is designed for those situations that do not completely support ISSU. A staggered upgrade may be required when upgrading between different AOS release trees (i.e. 7.3.2 to 7.3.4) due to underlying code variations between the two releases which may not allow CMMs or Master/Slave chassis to communicate after one is upgraded to the newer version of code.

A staggered upgrade requires a script file to be run prior to the upgrade. The script will copy the required configuration and image files to the CMMs or chassis to be upgraded. It also provides a mechanism to allow the Primary CMM or Master chassis to know the upgrade has been completed successfully on the redundant CMM or Slave chassis before rebooting. This allows for an upgrade between different AOS release trees with minimal network disruption.

Supported Upgrade Paths and Procedures

	Upgrading From 7.3.4.R01	Upgrading From 7.3.3	Upgrading From 7.3.2	Upgrading From 7.3.1
OS6900 – VC	ISSU – Supported Staggered Upgrade – N/S Standard Upgrade - Supported	ISSU – Supported Staggered Upgrade –N/S Standard Upgrade - Supported	ISSU – N/S Staggered Upgrade – Supported Standard Upgrade - Supported	ISSU – N/S Staggered Upgrade – N/S Standard Upgrade - Supported
OS6900 – Standalone	ISSU – N/A Staggered Upgrade – N/S Standard Upgrade - Supported	ISSU – N/A Staggered Upgrade – N/A Standard Upgrade - Supported	ISSU – N/A Staggered Upgrade – N/A Standard Upgrade - Supported	ISSU – N/A Staggered Upgrade – N/A Standard Upgrade - Supported
OS10K – VC	ISSU – Supported Staggered Upgrade – N/S Standard Upgrade - Supported	N/A	ISSU – N/S Staggered Upgrade – Supported Standard Upgrade - Supported	ISSU – N/S Staggered Upgrade – N/S Standard Upgrade - Supported
OS10K – Standalone (Dual-CMM)	ISSU – Supported Staggered Upgrade – N/S Standard Upgrade - Supported	N/A	ISSU – N/S Staggered Upgrade – N/S Standard Upgrade - Supported	ISSU – N/S Staggered Upgrade – N/S Standard Upgrade - Supported
OS10K – Standalone (Single-CMM)	ISSU – N/A Staggered Upgrade – N/A Standard Upgrade - Supported	N/A	ISSU – N/A Staggered Upgrade – N/A Standard Upgrade - Supported	ISSU – N/A Staggered Upgrade – N/A Standard Upgrade - Supported

- If upgrading a standalone chassis or VC using a standard upgrade procedure please refer to Appendix B for specific steps to follow.
- If upgrading a VC using ISSU please refer to Appendix C for specific steps to follow.
- If upgrading a VC using a staggered upgrade please refer to Appendix D for specific steps to follow to help minimize any network disruption.

Prerequisites

These upgrade instructions require that the following conditions exist, or are performed, before upgrading. The person performing the upgrade must:

- Be the responsible party for maintaining the switch's configuration.
- Be aware of any issues that may arise from a network outage caused by improperly loading this code.
- Understand that the switch must be rebooted and network access may be affected by following this procedure.
- Have a working knowledge of the switch to configure it to accept an FTP connection through the EMP or Network Interface (NI) Ethernet port.
- Read the GA Release Notes prior to performing any upgrade for information specific to this release.
- Ensure there is a current certified configuration on the switch so that the upgrade can be rolled-back if required.
- Verify the current versions of UBoot and FPGA. If they meet the minimum requirements, (i.e. they were already upgraded during a previous AOS upgrade) then only an upgrade of the AOS images is required.
- Depending on whether a standalone chassis or VC is being upgraded, upgrading can take from 5 to 20 minutes. Additional time will be needed for the network to re-converge.

- The examples below use various models and directories to demonstrate the upgrade procedure. However any user-defined directory can be used for the upgrade.
- If possible, have EMP or serial console access to all chassis during the upgrade. This will allow you to access and monitor the VC during the ISSU process and before the virtual chassis has been re-established.
- Knowledge of various aspects of AOS directory structure, operation and CLI commands can be found in the Alcatel-Lucent OmniSwitch User Guides. Recommended reading includes:
    - Release Notes - for the version of software you're planning to upgrade to.
    - The AOS Switch Management Guide
        - Chapter – Getting Started
        - Chapter - Logging Into the Switch
        - Chapter - Managing System Files
        - Chapter - Managing CMM Directory Content
        - Chapter - Using the CLI
        - Chapter - Working With Configuration Files
        - Chapter - Configuring Virtual Chassis

Do not proceed until all the above prerequisites have been met. Any deviation from these upgrade procedures could result in the malfunctioning of the switch. All steps in these procedures should be reviewed before beginning.

Switch Maintenance

It's recommended to perform switch maintenance prior to performing any upgrade. This can help with preparing for the upgrade and removing unnecessary files. The following steps can be performed at any time prior to a software upgrade. These procedures can be done using Telnet and FTP, however using SSH and SFTP/SCP are recommended as a security best-practice since Telnet and FTP are not secure.

1. Use the command '**show system**' to verify current date, time, AOS and model of the switch.

```
6900-> show system
System:
  Description:  Alcatel-Lucent OS6900-X20 7.3.2.568.R01 Service Release, September 05, 2014.,
  Object ID:    1.3.6.1.4.1.6486.801.1.1.2.1.10.1.1,
  Up Time:      0 days 0 hours 1 minutes and 44 seconds,
  Contact:      Alcatel-Lucent, http://alcatel-lucent.com/wps/portal/enterprise,
  Name:         6900,
  Location:     Unknown,
  Services:     78,
  Date & Time:  FRI OCT 31 2014 06:55:43 (UTC)
Flash Space:
    Primary CMM:
      Available (bytes):  1111470080,
      Comments         :  None
```

2. Remove any old tech_support.log files, tech_support_eng.tar files:

```
6900-> rm *.log
6900-> rm *.tar
```

3. Verify that the **/flash/pmd** and **/flash/pmd/work** directories are empty. If they have files in them check the date on the files. If they are recently created files (<10 days), contact Alcatel-Lucent Service & Support. If not, they can be deleted.

4. Use the '**show running-directory**' command to determine what directory the switch is running from and that the configuration is certified and synchronized:

```
6900-> show running-directory

CONFIGURATION STATUS
  Running CMM              : MASTER-PRIMARY,
  CMM Mode                 : VIRTUAL-CHASSIS MONO CMM,
  Current CMM Slot         : CHASSIS-1 A,
  Running configuration    : vc_dir,
  Certify/Restore Status   : CERTIFIED
SYNCHRONIZATION STATUS
  Running Configuration    : SYNCHRONIZED
```

If the configuration is not certified and synchronized, issue the command '**write memory flash-synchro**':

```
6900-> write memory flash-synchro
```

6. If you do not already have established baselines to determine the health of the switch you are upgrading, now would be a good time to collect them. Using the show tech-support series of commands is an excellent way to collect data on the state of the switch. The show tech support commands automatically create log files of useful show commands in the **/flash** directory. You can create the tech-support log files with the following commands:

```
6900-> show tech-support
6900-> show tech-support layer2
6900-> show tech-support layer3
```

It is a good idea to offload these files and review them to determine what additional data you might want to collect to establish meaningful baselines for a successful upgrade.

Appendix B: Standard Upgrade - OmniSwitch 6900/10K Standalone/Virtual Chassis

These instructions document how to upgrade an OS6900 or OS10K standalone or virtual chassis to 7.3.4.R02 using the standard upgrade procedure. Upgrading to 7.3.4.R02 using the standard upgrade procedure consists of the following steps. The steps should be performed in order:

1. Download the Upgrade Files

Go the to Alcatel-Lucent Service and Support website and download and unzip the 7.3.4.R02 upgrade files for the appropriate model. The archives contain the following:

- OS6900 Image Files **-** Tos.img
- OS10K Image Files – Ros.img, Reni.img

2. FTP the Upgrade Files to the Switch

FTP the image files to the *Running* directory of the switch you are upgrading. The image files and directory will differ depending on your switch and configuration.

3. Upgrade the image file

Follow the steps below to upgrade the image files by reloading the switch from the *Running* directory.

```
OS6900-> reload from working no rollback-timeout
Confirm Activate (Y/N) : y
This operation will verify and copy images before reloading.
It may take several minutes to complete....
```

If upgrading a VC the new image file will be copied to all the Slave chassis and the entire VC will reboot. After approximately 5-20 minutes the VC will become operational.

4. Verify the Software Upgrade

Log in to the switch to confirm it is running on the new software. This can be determined from the login banner or the **show microcode** commmand**.**

```
OS6900-> show microcode
   /flash/working
   Package         Release              Size     Description
----------------+------------------------+--------+----------------------------------
Tos.img         7.3.4.204.R02           210697424 Alcatel-Lucent OS
```

```

-> show running-directory


CONFIGURATION STATUS
  Running CMM              : MASTER-PRIMARY,
  CMM Mode                 : VIRTUAL-CHASSIS MONO CMM,
  Current CMM Slot         : CHASSIS-1 A,
  Running configuration    : WORKING,
  Certify/Restore Status   : CERTIFY NEEDED
SYNCHRONIZATION STATUS
  Running Configuration    : SYNCHRONIZED
```

Note: If there are any issues after upgrading the switch can be rolled back to the previous certified version by issuing the **reload from certified no rollback-timeout** command.

5. Certify the Software Upgrade

After verifying the software and that the network is stable, use the following commands to certify the new software by copying the *Running* directory to the Certified directory.

```
OS6900-> copy running certified
Please wait…………………………………….

-> show running-directory


CONFIGURATION STATUS
  Running CMM              : MASTER-PRIMARY,
  CMM Mode                 : VIRTUAL-CHASSIS MONO CMM,
  Current CMM Slot         : CHASSIS-1 A,
  Running configuration    : WORKING,
  Certify/Restore Status   : CERTIFIED
SYNCHRONIZATION STATUS
  Running Configuration    : SYNCHRONIZED
```

Appendix C: ISSU – OmniSwitch 6900/10K Virtual Chassis

These instructions document how to upgrade an OS6900 or OS10K virtual chassis to AOS release 7.3.4.R02 using ISSU. Upgrading a VC to 7.3.4.R02 consists of the following steps. The steps should be performed in order:

1. Download the Upgrade Files

Go the to Alcatel-Lucent Service and Support Website and download and unzip the 7.3.4.R02 ISSU upgrade files for the appropriate platform. The archive contains the following:

- OS6900 Image Files **-** Tos.img
- OS10K Image Files **-** Ros.img, Reni.img
- ISSU Version File – issu_version

2. Create the new directory on the Master for the ISSU upgrade:

```
OS6900-> mkdir /flash/issu_dir
```

3. Clean up existing ISSU directories

It is important to connect to the Slave chassis and verify that there is no existing directory with the path **/flash/issu_dir** on the Slave chassis. ISSU relies upon the switch to handle all of the file copying and directory creation on the Slave chassis. For this reason, having a pre-existing directory with the same name on the Slave chassis can have an adverse affect on the process. To verify that the Slave chassis does not have an existing directory of the same name as the ISSU directory on your Master chassis, use the internal VF-link IP address to connect to the Slave. In a multi-chassis VC, the internal IP addresses on the Virtual Fabric Link (VFL) always use the same IP addresses: 127.10.1.65 for Chassis 1,127.10.2.65 for Chassis 2, etc. These addresses can be found by issuing the debug command '**debug show virtual-chassis connection**' as shown below:

```
OS6900-> debug show virtual-chassis connection
                          Address         Address
 Chas  MAC-Address        Local IP        Remote IP       Status
-----+------------------+---------------------+-------------------+-------------
 1     e8:e7:32:b9:19:0b  127.10.2.65     127.10.1.65     Connected
```

4. SSH to the Slave chassis via the internal virtual-chassis IP address using the password 'switch':

```
OS6900-> ssh 127.10.2.65

Password:switch
```

5. Use the **ls** command to look for the directory name being used for the ISSU upgrade. In this example, we're using **/flash/issu_dir** so if that directory exists on the Slave chassis it should be deleted as shown below. Repeat this step for all Slave chassis:

```
6900-> rm –r /flash/issu_dir
```

6. Log out of the Slave chassis:

```
6900-> exit
logout
Connection to 127.10.2.65 closed.
```

7. On the Master chassis copy the current *Running* configuration files to the ISSU directory:

```
OS6900-> cp /flash/working/*.cfg /flash/issu_dir
```

8. FTP the new image files to the ISSU directory. Once complete verify that the ISSU directory contains only the required files for the upgrade:

```
6900-> ls /flash/issu_dir
Tos.img       issu_version  vcboot.cfg    vcsetup.cfg
```

9. Upgrade the image files using ISSU:

```
OS6900-> issu from issu_dir
Are you sure you want an In Service System Upgrade? (Y/N) : y
```

During ISSU '**show issu status**' gives the respective status(pending,complete,etc)

```
OS6900-> show issu status
Issu pending
```

This indicates that the ISSU is completed

```
OS6900-> show issu status
Issu not active
```

Allow the upgrade to complete. DO NOT modify the configuration files during the software upgrade. It normally takes between 5 and 20 minutes to complete the ISSU upgrade.

10. Verify the Software Upgrade

Log in to the switch to confirm it is running on the new software. This can be determined from the login banner or the **show microcode** commmand**.**

```
OS6900-> show microcode
   /flash/working
   Package         Release              Size     Description
-----------------+------------------------+--------+----------------------------------
Tos.img          7.3.4.204.R02            210697424 Alcatel-Lucent OS
```

```
OS6900-> copy running certified
Please wait.........................................

-> show running-directory


CONFIGURATION STATUS
  Running CMM              : MASTER-PRIMARY,
  CMM Mode                 : VIRTUAL-CHASSIS MONO CMM,
  Current CMM Slot         : CHASSIS-1 A,
  Running configuration    : issu_dir,
  Certify/Restore Status   : CERTIFY NEEDED
SYNCHRONIZATION STATUS
  Flash Between CMMs       : SYNCHRONIZED
  Running Configuration    : SYNCHRONIZED
```

11. Certify the Software Upgrade

After verifying the software and that the network is stable, use the following commands to certify the new software by copying the *Running* directory to the Certified directory:

```
OS6900-> copy running certified
Please wait........................................

-> show running-directory


CONFIGURATION STATUS
  Running CMM              : MASTER-PRIMARY,
  CMM Mode                 : VIRTUAL-CHASSIS MONO CMM,
  Current CMM Slot         : CHASSIS-1 A,
  Running configuration    : issu_dir,
  Certify/Restore Status   : CERTIFIED
SYNCHRONIZATION STATUS
  Flash Between CMMs       : SYNCHRONIZED
  Running Configuration    : SYNCHRONIZED
```

Appendix D: Staggered Upgrade - OmniSwitch OS10K/OS6900

These instructions document how to upgrade an OS10K or OS6900 VC to 7.3.4.R02 using a staggered upgrade process. Upgrading an OmniSwitch to 7.3.4.R02 using a staggered upgrade procedure consists of the following steps. The steps should be performed in order.

1. Download the Upgrade Files

Go the to Alcatel-Lucent Service and Support Website and download and unzip the 7.3.4.R02 upgrade files for the appropriate model. The archives contain the following:

- OS6900 Image Files – Tos.img
- OS10K Image Files **-** Ros.img, Reni.img
- Upgrade Script – vcof2-upgrade

2. Create a directory to hold the upgrade files on the Master chassis

```
OS10K-> mkdir /flash/issu_dir
```

3. FTP the upgrade files to the directories below on the Master chassis:

- Ros.img and Reni.img - /flash/issu_dir
- vcof2-upgrade - /flash

4. Execute the script on the Master chassis:

```
OS10K-> chmod a+x /flash/vcof2-upgrade
OS10K-> /flash/vcof2-upgrade  issu_dir
```

The above commands perform the following:

4a. Copies the **vcboot.cfg** and **vcsetup.cfg** from the current *Running* directory to **/flash/issu_dir** directory. It also copies the image files and configuration files to the secondary and Slave CMMs. It then creates the special upgrade helper file "**vcupgrade.cfg**" and copies it to the Slave. It then initiates a reload on the Slave with the new software to begin the upgrade process. This process can take approximately 3-5 minutes.

4b. The Slave chassis reboots with the new code and detects the "**vcupgrade.cfg**" file. The Slave chassis shuts down all ports except the VFL ports to the old Master with the old code. This process can take approximately 6-8 minutes and may result in minimal sub-second traffic loss.

4c. When the Slave chassis with the new code is ready it reloads the old Master, takes over the Master role with the new code and brings up all ports that were previously shut down. Depending on the network protocols, routes, links, and switch configuration it can take approximately 10-60 seconds to stabilize.

4d. The old Master comes up as the Slave chassis with the new code and joins the VC. This process can take approximately 6-8 minutes and may result in minimal sub-second traffic loss.

5. Verify the Software Upgrade

To verify that the software was successfully upgraded to 7.3.4.R02, use the **show microcode** command as shown below:

```
OS10K-> show microcode
/flash/working

Package       Release          Size       Description
-------------+-----------------+-----------+------------------
Ros.img      7.3.4.204.R02    106031376    Alcatel-Lucent OS
Reni.img     7.3.4.204.R02    106031376    Alcatel-Lucent OS
```

6. Certify the Software Upgrade

After verifying the software and that the network is stable, use the following commands to certify the new software by copying the *Running* directory to the Certified directory:

```
OS6900-> copy running certified
Please wait…………………………………….

-> show running-directory


CONFIGURATION STATUS
  Running CMM              : MASTER-PRIMARY,
  CMM Mode                 : VIRTUAL-CHASSIS MONO CMM,
  Current CMM Slot         : CHASSIS-1 A,
  Running configuration    : issu_dir,
  Certify/Restore Status   : CERTIFIED
SYNCHRONIZATION STATUS
  Flash Between CMMs       : SYNCHRONIZED
  Running Configuration    : SYNCHRONIZED
```

Appendix E: Previous Release Feature Summary

Existing Hardware/Software Feature Summary - AOS 7.3.4.R01

Feature	Platform	License
Hardware Feature Support		
OS6900-Q32		
SFP-10G-ZR Transceiver		
QSFP-4X10G-SR Transceiver		
QSFP-4X10G-C Transceiver		
Data Center Feature Support		
- VXLAN	6900-Q32	Data Center
- VM/VXLAN Snooping	6900/10K	Data Center
DHCP		
- Internal DHCPv4 and DHCPv6 Server	6900/10K	Base
- IPv6 DHCP Relay Agent	6900/10K	Base
- DHCP Snooping	6900/10K	Base
Layer 3 Feature Support		
- BGP 4-Octet ASN	6900/10K	Advanced
- BGP AS Path Filtering for IPv6	6900/10K	Advanced
- BGP Password Support for IPv6	6900/10K	Advanced
- BGP Route Reflector for IPv6	6900/10K	Advanced
- Distributed ARP	6900	Base
- Increase OSPFv2 Interfaces	6900/10K	Advanced
- ISIS for IPv6	6900/10K	Advanced
- M-ISIS	6900/10K	Advanced
- Static Routing to an IP Interface Name	6900/10K	Base
- IP Routed Port	6900/10K	Base
Automatic Management Feature Support		
- Automatic Virtual Chassis	6900/10K	Advanced
- Automatic Remote Configuration	6900/10K	Base

Feature	Platform	License
- Automatic Fabric	6900/10K	Base
- Automatic IP Protocols	6900/10K	Base
Management Feature Support		
- Embedded Pyton Scripting / Event Manager Support	6900/10K	Base
- IP Managed Services	6900/10K	Base
- OpenFlow Support for Standalone and Virtual Chassis	6900/10K	Base
Security		
- 802.1x for VLANs, SPBM, and VXLAN Services	6900/10K	Base

Existing Hardware/Software Feature Summary – AOS 7.3.3

Feature	Platform	License
Hardware Support		
- OS-XNI-U12E	OS6900	Base
- SFP-FC-SR Transceiver	OS6900	Base
Data Center Feature Support		
- FCoE/FC Gateway	6900	Data Center
- CEE DCBX Version 1.01	6900	Data Center
Layer 3 Feature Support		
- ISIS – IPv4/IPv6	6900	Advanced
- BGP 4-Octet ASN	6900	Advanced
Management		
- Virtual Chassis mesh of 6 chassis with ISSU support	6900	Advanced
Early Availability Feature Support		

Feature	Platform	License
- OpenFlow Agent versions 1.3.1 and 1.0 (Normal and Hybrid modes)	6900	Base
- Internal IPv4/IPv6 DHCP Server	6900	Base
- OmniSwitch Networking Plug-in for OpenStack	6900	Base
- M-ISIS	6900	Advanced

Existing Hardware/Software Feature Summary - AOS 7.3.2.R01

Feature	Platform	License
Hardware Feature Support		
- OmniSwitch 6900-T20		
- OmniSwitch 6900-T40		
- OS-XNI-T8		
Data Center Feature Support		
- FIP Snooping	OS10K/6900	Data Center
- Virtual Maching Performance Monitoring	OS10K/6900	Data Center
Layer 2 Feature Support		
- Dynamic Auto Fabric	OS10K/6900	Base
Layer 3 Feature Support		
- IPv4 over SPBM	OS10K/6900	Advanced
- Interop between PIM & DVMRP	OS10K/6900	Base
- Non-Contiguous Mask and IPv6 Gateway Support	OS10K/6900	Base
- Increase VRF Instances	OS10K/6900	Base
Management/Additional Feature Support		
- Command Abbreviation	OS10K/6900	Base
- Web Services & CLI Scripting	OS10K/6900	Base
- Enhanced Server & Session Limits	OS10K/6900	Base
Additional Feature Support		
- Application Fingerprinting	OS10K/6900	Base
- Fault Propagation and Link Flapping - Wait to Shutdown	OS10K/6900	Base

Existing Hardware/Software Feature Summary - AOS 7.3.1.R01

Feature	Platform	License
Hardware Feature Support		
OS10K-XNI-U16L OS10K-XNI-U16E OS10K-XNI-U32E OS10K-QNI-U4E OS10K-QNI-U8E QSFP-40G-LR Transceiver SFP-10G-24DWDM80 Transceiver SFP-10G-GIG-SR Transceiver		
Data Center Feature Support		
Shortest Path Bridging (SPB)	OS10K/6900	Advanced
Data Center Bridging • DCBX • ETS • PFC	OS10K/6900 OS10K/6900 OS10K/6900	Data Center Data Center Data Center
Edge Virtual Briding (EVB)	OS10K/6900	Data Center
Virtual Network Profiles • SAP/SPB-M Services • Customer Domains (Multi-tenancy) • Dynamic SAP • UNP over MC-LAG on OS10K	OS10K/6900 OS10K/6900 OS10K/6900 OS10K/6900	Base Base Base Base
Layer 2 Feature Support		
Ethernet Ring Protection v2 (ERPv2)	OS10K/6900	Base
Layer 3 Feature Support		
VRF Management	OS10K/6900	Base
VRF Route Leak	OS10K/6900	Base
Management Feature Support		
Virtual Chassis	OS10K/6900	Advanced

Feature	Platform	License
SFP+ Line Diags & Enhanced Port Performance (EPP)	OS10K/6900	Base
License Management	OS10K/6900	Base
Ethernet OAM • ITU Y1731 and 802.1ag	OS10K/6900 OS10K/6900	Base
Service Assurance Agent	OS10K/6900	Base

Note: The SAP/SPB-M Services, Customer Domains, Dynamic SAP, and Virtual Chassis features were introduced in AOS Release 7.3.1.632.R01. The remaining features in this section were introduced in AOS Release 7.3.1.519.R01.

Existing Hardware/Software Feature Summary - AOS 7.2.1.R02

Feature	Platform	License
Hardware Feature Support		
OmniSwitch 6900 Rear-to-Front Cooling OS-QNI-U3 Module OS-HNI-U6 Module QSFP-40G-SR Transceiver QSFP-40G-C Transceiver OS6900-BP-R (YM-2451F) Power Supply OS6900-BPD-R (YM-2451P) Power Supply OS6900-FT-R FanTray		
Layer 2 Feature Support		
High Availability VLAN • Added support for OS10K • HA-VLAN with MCLAG	OS10K OS10K/6900	Base Base
Multi-Chassis Link Aggregation • Configurable Chassis Group ID (Multiple MC-LAG Domains) • Standalone Port in VIP VLAN • SLB Over MC-LAG	OS10K/6900 OS10K/6900 OS10K/6900	Base Base Base
MVRP • Added support for OS10K	OS10K	Base
Universal Network Profiles • UNP with Dynamic Profiles • UNP with Link-Aggregation • UNP with MC-LAG • UNP with Learned Port Security	OS6900 OS6900 OS6900 OS6900	Base Base Base Base
Layer 3 Feature Support		
16 ECMP routes for IPv6	OS10K/6900	Base
Qos		
VFC/VoQ Profiles • Added support for profiles 2-4 • Added support for WRED	OS10K/6900 OS6900	Base Base

Feature	Platform	License
Security		
Learned Port Security Enhancements	OS10K/6900	Base

Existing Hardware/Software Feature Summary - AOS 7.2.1.R01

Feature	Platform	License
Hardware Feature Support		
OmniSwitch 6900-X20 OmniSwitch 6900-X40 OS-XNI-U4 OS-XNI-U12 OS6900-BP-F (YM-2451C) Power Supply OS6900-BPD-F (YM-2451D) Power Supply OS6900-FT-F FanTray		
Manageability Feature Support		
CLI	OS6900	Base
Ethernet Interfaces	OS6900	Base
License Management	OS6900	Base
Multiple VRF Routing and Forwarding	OS6900	Advanced
Network Time Protocol (NTP)	OS6900	Base
Pause Control(RX) /Flow Control	OS6900	Base
Remote Access FTP SCP SSH/SFTP Telnet TFTP	OS6900	Base
Resiliency Features Hot Swap Expansion Modules Power Supply Redundancy Fan Redundancy	OS6900	Base
SNMP	OS6900	Base
Software Rollback – Multi-Image/Multi-Config	OS6900	Base
Storm Control	OS6900	Base
Text File Configuration	OS6900	Base
UDLD	OS6900	Base
USB Support	OS6900	Base
Web-Based Management (WebView)	OS6900	Base

Feature	Platform	License
Layer 2 Feature Support		
802.1AB with MED Extensions	OS6900	Base
802.1Q	OS6900	Base
Configurable Hash Mode	OS6900	Base
HA-VLAN	OS6900	Base
Link Aggregation –Static and LACP (802.3ad)	OS6900	Base
Multi-Chassis Link Aggregation	OS6900	Base
MVRP	OS6900	Base
Source Learning	OS6900	Base
Spanning Tree • 802.1d and 802.1w • Multiple Spanning Tree Protocol • PVST+ • Root Guard	OS6900	Base
Universal Network Profiles (UNP)	OS6900	Base
VLANs	OS6900	Base
IPv4 Feature Support		
Bi-Directional Forwarding Detection (BFD)	OS6900	Base
DHCP / UDP DHCP Relay/Option-82 Per-VLAN UDP Relay	OS6900	Base
BGP4 with Graceful Restart	OS6900	Advanced
DNS Client	OS6900	Base
GRE	OS6900	Base
IP Multicast Routing	OS6900	Advanced
IP Multicast Switching (IGMP)	OS6900	Base
IP Multicast Switching (Proxying)	OS6900	Base
IP Multinetting	OS6900	Base
IP Route Map Redistribution	OS6900	Base

Feature	Platform	License
IP-IP Tunneling	OS6900	Base
OSPFv2	OS6900	Advanced
RIPv1/v2	OS6900	Base
Routing Protocol Preference	OS6900	Base
Server Load Balancing	OS6900	Base
VRRPv2	OS6900	Advanced
IPv6 Feature Support		
BGP4 BGP IPv6 Extensions	OS6900	Advanced
IPSec IPv6 OSPFv3 RIPng	OS6900	Advanced
IPv6 Client and/or Server Support	OS6900	Base
IPv6 Multicast Routing	OS6900	Advanced
IPv6 Multicast Switching (MLD v1/v2)	OS6900	Base
IPv6 Routing	OS6900	Advanced
IPv6 Scoped Multicast Addresses	OS6900	Base
IPv6 Neighbor Discovery Support	OS6900	Base
OSPFv3	OS6900	Advanced
RIPng	OS6900	Advanced
VRRPv3	OS6900	Advanced
QoS Feature Support		
Auto-Qos Prioritization of NMS Traffic	OS6900	Base
Ingress and egress bandwith shaping	OS6900	Base
Policy Based Routing	OS6900	Advanced
Tri-Color Marking	OS6900	Base
Multicast Feature Support		
DVMRP	OS6900	Advanced
IGMP Multicast Group Configuration Limit	OS6900	Base

Feature	Platform	License
IGMP Relay	OS6900	Base
IPv4/IPv6 Multicast Switching (IPMS)	OS6900	Base
L2 Static Multicast Address	OS6900	Base
PIM / PIM-SSM (Source-Specific Multicast)	OS6900	Advanced
Monitoring/Troubleshooting Feature Support		
DDM - Digital Diagnostic Monitoring	OS6900	Base
Health Statistics	OS6900	Base
Ping and Traceroute	OS6900	Base
Policy Based Mirroring	OS6900	Base
Port Mirroring	OS6900	Base
Port Monitoring	OS6900	Base
Remote Port Mirroring	OS6900	Base
Rmon	OS6900	Base
sFlow	OS6900	Base
Switch Logging and Syslog	OS6900	Base
Metro Ethernet Feature Support		
ERP G.8032 – Shared VLAN	OS6900	Base
Ethernet Services	OS6900	Base
L2 Control Protocol Tunneling (L2CP)	OS6900	Base
Security Feature Support		
Access Control Lists (ACLs) for IPv4/IPv6	OS6900	Base
Account & Password Policies	OS6900	Base
Admin User Remote Access Restriction Control	OS6900	Base
ARP Defense Optimization	OS6900	Base
ARP Poisoning Detect	OS6900	Base
Authenticated Switch Access	OS6900	Base

Feature	Platform	License
IP DoS Filtering	OS6900	Base
Learned Port Security (LPS)	OS6900	Base
Policy Server Management	OS6900	Base

Existing Hardware/Software Feature Summary - AOS 7.1.1. R01

Feature	Platform	Software Package
Hardware Feature Support		
OmniSwitch 10K Chassis OS10K-CMM OS10K-CFM OS10K-GNI-C48E OS10K-GNI-U48E OS10K-XNI-U32S OS10K-PS-25A OS10K-PS-24D OS10K-Fan-Tray		
Manageability Feature Support		
CLI	OS10K	Base
Ethernet Interfaces	OS10K	Base
ISSU	OS10K	Base
Multiple VRF Routing and Forwarding	OS10K	Base
Network Time Protocol (NTP)	OS10K	Base
Pause Control/Flow Control	OS10K	Base
Remote Access FTP SCP SSH/SFTP Telnet TFTP	OS10K	Base
Smart Continuous Switching Hot Swap Management Module Failover Power Monitoring Redundancy	OS10K	Base
SNMP	OS10K	Base
Software Rollback – Multi-Image/Multi-Config	OS10K	Base
Storm Control	OS10K	Base
Text File Configuration	OS10K	Base

Feature	Platform	Software Package
UDLD	OS10K	Base
USB Support	OS10K	Base
Web-Based Management (WebView)	OS10K	Base
Layer 2 Feature Support		
802.1AB with MED Extensions	OS10K	Base
802.1Q	OS10K	Base
Configurable Hash Mode	OS10K	Base
Link Aggregation –Static and LACP (802.3ad)	OS10K	Base
Multi-Chassis Link Aggregation	OS10K	Base
Source Learning	OS10K	Base
Spanning Tree • 802.1d and 802.1w • Multiple Spanning Tree Protocol • PVST+ • Root Guard	OS10K	Base
VLANs	OS10K	Base
IPv4 Feature Support		
Bi-Directional Forwarding Detection (BFD)	OS10K	Base
DHCP / UDP DHCP Relay/Option-82 Per-VLAN UDP Relay	OS10K	Base
BGP4 with Graceful Restart	OS10K	Base
DNS Client	OS10K	Base
GRE	OS10K	Base
IP Multicast Routing	OS10K	Base
IP Multicast Switching (IGMP)	OS10K	Base
IP Multicast Switching (Proxying)	OS10K	Base
IP Multinetting	OS10K	Base

Feature	Platform	Software Package
IP Route Map Redistribution	OS10K	Base
IP-IP Tunneling	OS10K	Base
OSPFv2	OS10K	Base
RIPv1/v2	OS10K	Base
Routing Protocol Preference	OS10K	Base
Server Load Balancing	OS10K	Base
VRRPv2	OS10K	Base
IPv6 Feature Support		
BGP4 BGP IPv6 Extensions	OS10K	Base
IPSec IPv6 OSPFv3 RIPng	OS10K	Base
IPv6 Client and/or Server Support	OS10K	Base
IPv6 Multicast Routing	OS10K	Base
IPv6 Multicast Switching (MLD v1/v2)	OS10K	Base
IPv6 Routing	OS10K	Base
IPv6 Scoped Multicast Addresses	OS10K	Base
IPv6 Neighbor Discovery Support	OS10K	Base
OSPFv3	OS10K	Base
RIPng	OS10K	Base
VRRPv3	OS10K	Base
QoS Feature Support		
Auto-Qos Prioritization of NMS Traffic	OS10K	Base
Ingress and egress bandwith shaping	OS10K	Base
Policy Based Routing	OS10K	Base
Tri-Color Marking	OS10K	Base
Multicast Feature Support		
DVMRP	OS10K	Base

Feature	Platform	Software Package
IGMP Multicast Group Configuration Limit	OS10K	Base
IGMP Relay	OS10K	Base
IPv4/IPv6 Multicast Switching (IPMS)	OS10K	Base
L2 Static Multicast Address	OS10K	Base
PIM / PIM-SSM (Source-Specific Multicast)	OS10K	Base
Monitoring/Troubleshooting Feature Support		
DDM - Digital Diagnostic Monitoring	OS10K	Base
Health Statistics	OS10K	Base
Ping and Traceroute	OS10K	Base
Policy Based Mirroring	OS10K	Base
Port Mirroring	OS10K	Base
Port Monitoring	OS10K	Base
Remote Port Mirroring	OS10K	Base
Rmon	OS10K	Base
sFlow	OS10K	Base
Switch Logging and Syslog	OS10K	Base
Metro Ethernet Feature Support		
ERP G.8032 – Shared VLAN	OS10K	Base
Ethernet Services	OS10K	Base
L2 Control Protocol Tunneling (L2CP)	OS10K	Base
Security Feature Support		
Access Control Lists (ACLs) for IPv4/IPv6	OS10K	Base
Account & Password Policies	OS10K	Base
Admin User Remote Access Restriction Control	OS10K	Base
ARP Defense Optimization	OS10K	Base
ARP Poisoning Detect	OS10K	Base

Feature	Platform	Software Package
Authenticated Switch Access	OS10K	Base
IP DoS Filtering	OS10K	Base
Learned Port Security (LPS)	OS10K	Base
Policy Server Management	OS10K	Base

Appendix F: Release Specifications

This appendix is derived from the OmniSwitch AOS user guides. It contains all the specification tables at the beginning of each chapter in each of the user guides of the corresponding release. It is designed to be a single resource to help verify the specifications being documented for AOS releases. The information contained here is duplicated in the Specifications Tables in each user guide.

Swith Management Guide Specifications

Getting Started Specifications

Platforms Supported	OmniSwitch 10K, 6900
Standalone Configuration Files	boot.cfg
Virtual Chassis Configuration Files	vcboot.cfg vcsetup.cfg
Demo License	45-day Demo Advanced license
Image Files	Ros.img (OS10K) Reni.img (OS10K) Tos.img (OS6900)
Validation File	issu_version
ISSU Directory	Any user-defined directory to store the image files
NI Reset Timer	120 minutes
Control LED	Blinks amber during ISSU upgrade

Login Specifications

Platforms Supported	OmniSwitch 10K, 6900
Login Methods	Telnet, SSH, HTTP, SNMP
Number of concurrent Telnet sessions	6
Number of concurrent SSH sessions	8
Number of concurrent HTTP (WebView) sessions	4
Secure Shell public key authentication	Password DSA/RSA Public Key
RFCs Supported for SSHv2	RFC 4253 - SSH Transport Layer Protocol RFC 4418 - UMAC: Message Authentication Code using Universal Hashing

File Management Specifications

Platforms Supported	OmniSwitch 10K, 6900

File Transfer Methods	FTP (v4/v6), SFTP (v4/v6), SCP (v4/v6), TFTP
Client/Server Support	FTP - Client (IPv4 Only) or Server SFTP - Client or Server SCP - Client or Server TFTP – Client
Number of concurrent FTP/ SFTP sessions	4
Configuration Recovery	The **flash/certified** directory holds configurations that are certified as the default start-up files for the switch. They will be used in the event of a non-specified reload.
Default Switch Directory - /**flash**	Contains the **certified, working, switch, network,** and user-defined directories.
File/Directory Name Metrics	255 character maximum. File and directory names are case sensitive.
File/Directory Name Characters	Any valid ASCII character except '/'.
Sub-Directories	Additional user-defined directories created in the /**flash** directory.
Text Editing	Standard Vi standard editor.
System Clock	Set local date, time and time zone, Universal Time Coordinate (UTC), Daylight Savings (DST or summertime).

Managing CMM Directory Content

CMM Specifications

Platforms Supported	**OmniSwitch 10K, 6900**
Size of Flash Memory	2 GB OS6900-X72 – 4 GB
Maximum Length of File Names	255 Characters
Maximum Length of Directory Names	255 Characters
Maximum Length of System Name	32 Characters
Default Boot Directory	Certified

USB Flash Drive Specifications

Platforms Supported	OmniSwitch 10K, 6900
USB Flash Drive Support	Alcatel-Lucent Certified USB Flash Drive
Automatic Software Upgrade	Supported
Disaster Recovery	Supported OS10K - **Rrescue.img** file required

	OS6900 - **Trescue.img** file required

Note: The format of the Alcatel-Lucent certfied USB Flash Drive must be FAT32. To avoid file corruption issues the USB Drive should be stopped before removing from a PC. Directory names are case sensitive and must be lower case.

CLI Specifications

Platforms Supported	OmniSwitch 10K, 6900
Configuration Methods	• Online configuration via real-time sessions using CLI commands. • Offline configuration using text file holding CLI commands.
Command Capture Feature	Snapshot feature captures switch configurations in a text file.
User Service Features	• Command Line Editing • Command Prefix Recognition • CLI Prompt Option • Command Help • Keyword Completion • Keyword Abbreviation • Command History • Command Logging • Syntax Error Display • More Command

Configuration File Specifications

Platforms Supported	OmniSwitch 10K, 6900
Creation Methods for Configuration Files	• Create a text file on a word processor and upload it to the switch. • Invoke the switch’s snapshot feature to create a text file. • Create a text file using the switch’s text editor.
Timer Functions	Files can be applied immediately or by setting a timer on the switch.
Command Capture Feature	Snapshot feature captures switch configurations in a text file.
Error Reporting	Snapshot feature includes error reporting in the text file.
Text Editing on the Switch	Vi standard editor.
Default Error File Limit	1

User Database Specifications

Platforms Supported	OmniSwitch 10K, 6900
Maximum number of alphanumeric characters in a username	63
Maximum number of alphanumeric characters in a user password	30
Maximum number of local user accounts	50

SNMP Specifications

Platforms Supported	OmniSwitch 10K, 6900
RFCs Supported for SNMPv2	1902 through 1907 - SNMPv2c Management Framework 1908 - Coexistence and transitions relating to SNMPv1 and SNMPv2c
RFCs Supported for SNMPv3	2570 – Version 3 of the Internet Standard Network Management Framework 2571 – Architecture for Describing SNMP Management Frameworks 2572 – Message Processing and Dispatching for SNMP 2573 – SNMPv3 Applications 2574 – User-based Security Model (USM) for version 3 SNMP 2575 – View-based Access Control Model (VACM) for SNMP 2576 – Coexistence between SNMP versions
Platforms Supported	OmniSwitch 10K, 6900
SNMPv1, SNMPv2, SNMPv3	The SNMPv3 protocol is ascending compatible with SNMPv1 and v2 and supports all the SNMPv1 and SNMPv2 PDUs
SNMPv1 and SNMPv2 Authentication	Community Strings
SNMPv1, SNMPv2 Encryption	None
SNMPv1 and SNMPv2 Security requests accepted by the switch	Sets and Gets
SNMPv3 Authentication	SHA, MD5
SNMPv3 Encryption	DES
SNMPv3 Security requests accepted by the switch.	Non-authenticated Sets, Non-authenticated Gets and Get-Nexts, Authenticated Sets, Authenticated Gets and Get-Nexts, Encrypted Sets, Encrypted Gets and Get-Nexts

Web Services, CLI Scripting, OpenFlow Specifications

Platforms Supported	OmniSwitch 10K, 6900
Configuration Methods	HTTP/HTTPS Python API
Response Formats	Extensible Markup language (XML) JavaScript Object Notation (JSON)
Maximum Web Services Session	4
Alcatel-Lucent Python Library	consumer.py (Python version 2.X/3.X compatible) Note: This file is available on the Service & Support Website. It is being provided as an example application to help with Web Services familiarization but is not an officially supported part of the Web Services solution.
Internal Python in AOS/Event based CLI Scripting	Python 3
Default Script Run Time Limit 60 Seconds.	60 Seconds

OpenFlow Specifications

Platforms Supported	OmniSwitch 10K, 6900 **Note**: Not supported on OS10K-XNI-U32S module.
Modes Supported	Normal Hybrid (API)
Version Supported	1.0 1.3.1
Maximum Number of logical switches	3
Maximum number of controllers per logical switch	3
Maximum number of logical switches in Hybrid mode	1
Support for Virtual Chassis	Supported
OpenFlow 1.0/1.3.1 TCP port	6633

Virtual Chassis Specifications

Platforms Supported	OmniSwitch 10K, 6900
Maximum number of physical switches in a Virtual Chassis	OS10K - 2 OS6900 - 6

Note: OS10Ks and OS6900s cannot be mixed in a Virtual Chassis Note: Different OS6900 models can be mixed in a Virtual Chassis.	
Valid chassis identifier	OS10K - 1 or 2 OS6900 – 1 through 6
Valid chassis group identifier	0–255
Valid chassis priority	0–255
Maximum number of Virtual Fabric Links	OS10K – 1 OS6900 - 5
Valid Virtual Fabric Link identifier	OS10K – 0 OS6900 – 0 through 4
VFL Supported Port Types	10G or 40G Fiber
Valid control VLAN	2-4094
Valid Virtual Chassis protocol hello interval	1-65535
Maximum number of member ports per Virtual Fabric Link	16
Licenses Required	Advanced or Demo Advanced **Note**: A VC of 1 chassis does not require a license
OS6900 OK LED	Blinking Green = Master Solid Green = Slave

Note: Distributed MAC Learning Mode is not supported on a Virtual Chassis

Automatic Remote Configuration Specifications

Platforms Supported	OmniSwitch 10K, 6900
DHCP Specifications	DHCP Server required DHCP Client on OmniSwitch - VLAN 1 - Tagged VLAN 127 (all ports) - LLDP Management VLAN - Automatic LACP (tagged VLAN 127, untagged VLAN 1)
File Servers	TFTP FTP/SFTP
Clients supported	TFTP FTP/SFTP
Instruction file	Maximum length of: • Pathname: 255 characters • Filename: 63 characters

Maximum length of username for FTP/SFTP file server.	15 characters
Maximum DHCP lease tries	6
Unsupported Features	ISSU and IPv6 are not supported. Upgrade of uboot, miniboot, or FPGA files is not supported.
OK LED	Flashing amber during Automatic Remote Configuration process

Automatic Fabric Specifications

Platforms Supported	OmniSwitch 10K, 6900
OmniSwitch Software License	Advanced (free 45-day demo license activated when the switch comes up)
Modes Supported	Standalone or Virtual Chassis
Ports Supported	Any port that is not configured for use by another feature (for example, 802.1q tag, UNP, or Ethernet Services).
IP Protocols Supported for Automatic IP Configuration	OSPFv2, OSPFv3, IS-IS IPv4, IS-IS IPv6

NTP Specifications

Platforms Supported	OmniSwitch 10K, 6900
RFCs supported	1305–Network Time Protocol
NTP Key File Location	**/flash/network**
Platforms Supported	OmniSwitch 10K, 6900
Maximum number of NTP servers	12

Network Configuration Guide Specifications

Ethernet Specifications

IEEE Standards Supported	802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD) 802.3u (100BaseTX) 802.3ab (1000BaseT) 802.3z (1000Base-X) 802.3ae (10GBase-X) 802.3ba (40GBase-X) 802.3z (Energy Efficient Ethernet)

Platforms Supported	OmniSwitch 10K, 6900
Ports Supported	Ethernet (10 Mbps) Fast Ethernet (100 Mbps) Gigabit Ethernet (1 Gbps) 10 Gigabit Ethernet (10 Gbps) 40 Gigabit Ethernet (40 Gbps)
Auto Negotiation	Supported
Port Mirroring / Monitoring	Supported
802.1Q Hardware Tagging	Supported
Jumbo Frame Configuration	Supported on 1/10/40 Gigabit Ethernet ports
Maximum Frame Size	1553 bytes (10/100 Mbps) 9216 bytes (1/10/40 Gbps)
Enhanced Port Performance (EPP)	Supported on OS6900 with 10-Gigabit transceivers

UDLD Specifications

Platforms Supported	OmniSwitch 10K, 6900
Maximum number of UDLD ports per system	Up to maximum physical ports per system

Source Learning Specifications

Platforms Supported	OmniSwitch 10K, 6900
RFCs supported	2674—Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions
Maximum number of learned MAC addresses when centralized MAC source learning mode is enabled	OS10K - 32K Module / 32K Chassis OS6900-X20/X40/T20/T40 - 128K OS6900-Q32/X72 – 228K
Maximum number of learned MAC addresses when distributed MAC source learning mode is enabled.	OS10K - 32K Module (C48E/U48E/U32S) OS10K – 128K Module (U32E/U16E(L)/U4E/U8E) OS10K – 256K (Chassis) OS6900 - Not Supported

VLAN Specifications

Platforms Supported	OmniSwitch 10K, 6900
RFCs Supported	2674 - Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions
IEEE Standards Supported	802.1Q - Virtual Bridged Local Area Networks 802.1D - Media Access Control Bridges

Maximum VLANs per switch	4094
Maximum Tagged VLANs per Port	4093
Maximum Untagged VLANs per Port	One untagged VLAN (default VLAN) per port.
Maximum VLAN Port Associations (VPA) per switch (Recommended)	OS10K - 20000 OS6900 - 10000
Maximum Spanning Tree VLANs per switch	252 (1x1 mode)

High Availability VLANs Specifications

Platforms Supported	OmniSwitch 10K, 6900
Maximum high availability VLANs per switch	16
Switch ports eligible for high availability VLAN assignment.	Fixed ports on second-generation Network Interface (NI) modules.
Switch port not eligible for high availability VLAN assignment.	Mirroring ports.

Spanning Tree Specifications

Platforms Supported	OmniSwitch 10K, 6900
IEEE Standards supported	802.1d—Media Access Control (MAC) Bridges 802.1s—Multiple Spanning Trees 802.1w—Rapid Spanning Tree Protocol
Spanning Tree operating modes supported	Flat mode—one spanning tree instance per switch Per-VLAN mode—one spanning tree instance per VLAN
Spanning Tree port eligibility	Fixed ports 802.1Q tagged ports Link aggregate of ports
Maximum VLAN Spanning Tree instances per switch.	252 (per-VLAN mode)
Maximum flat mode Multiple Spanning Tree Instances (MSTI) per switch	16 MSTI, in addition to the Common and Internal Spanning Tree instance (also referred to as MSTI 0).

Loopback Detection Specifications

Platforms Supported	OmniSwitch 10K, 6900
Ports Supported	There is no restriction on the type of ports on which the LBD can be enabled. But it is recommended LBD should be enabled on the edge ports.
Transmisson Timer	Range from 5 to 600 seconds.
Auto-recovery Timer	Range from 30 to 86400 seconds.

Static Link Aggregation Specifications

Platforms Supported	OmniSwitch 10K, 6900
Maximum number of link aggregation groups	OS10K – 128 OS6900 - 256
Maximum number of links per group supported	OS10K – 8 OS6900 - 16

Dynamic Link Aggregation Specifications

Platforms Supported	OmniSwitch 10K, 6900
IEEE Specifications Supported	802.3ad — Aggregation of Multiple Link Segments
Maximum number of link aggregation groups	OS10K – 128 OS6900 - 256
Maximum number of ports per link aggregate	OS10K – 8 OS6900 - 16

ERP Specifications

ITU-T G.8032 03/2010	Ethernet Ring Protection version 2 (Multi Rings and Ladder networks supported) (Hold off timer, Lockout , Signal degrade SD, RPL Replacement, Forced Switch, Manual Switch, Clear for Manual/Forced Switch, Dual end blocking not supported)
ITU-T Y.1731/IEEE 802.1ag	ERP packet compliant with OAM PDU format for CCM
Supported Platforms	OmniSwitch 10K, 6900
Maximum number of rings per node	64
Maximum number of nodes per ring	16 (recommended)
Maximum number of VLANs per port.	4094
Range for ring ID	1 - 2147483647
Range for remote MEPID	1 - 8191
Range for wait-to-restore timer	1 - 12 minutes
Range for guard timer	1 - 200 centi-seconds

MVRP Specifications

IEEE Standards Supported	IEEE 802.1ak-2007 Amendment 7: Multiple Registration Protocol IEEE 802.1Q-2005 Corrigendum 2008
Platforms Supported	OmniSwitch 10K, 6900
Maximum MVRP VLANs	4094

802.1AB Specifications

Platforms Supported	OmniSwitch 10K, 6900
IEEE Specification	IEEE 802.1AB-2005 Station and Media Access Control Connectivity Discovery
Maximum number of network policies that can be associated with a port	8
Maximum number of network policies that can be configured on the switch	32

IP Specifications

Platforms Supported	OmniSwitch 10K, 6900
RFCs Supported	791–Internet Protocol 792–Internet Control Message Protocol 826–An Ethernet Address Resolution Protocol 2784–Generic Routing Encapsulation (GRE) 2890–Key and Sequence Number Extensions to GRE (extensions defined are not supported) 1701–Generic Routing Encapsulation (GRE) 1702–Generic Routing Encapsulation over IPV4 Networks 2003-IP Encapsulation within IP
Maximum router interfaces per system	4094 IPv4
Maximum router interfaces per VLAN	16
Maximum HW routes	OS10K (C48/U48)- 16K OS10K (U32E) – 16K OS10K (U32S) – 12K OS6900-X20/X40/T20/T40 - 16K OS6900-Q32/X72 – 12K
Maximum SW routes per switch	OS10K – 256K OS6900 – 128K
Maximum HW ARP entries per	OS10K (XNI-U32S) – 8K

module/standalone chassis	OS10K (All other modules) - 16K OS6900 (X20/X40) - 8K OS6900 (T20/T40) – 16K OS6900-Q32/X72 – 48K (Note: Mixing an XNI-U32S with other modules in the same chassis reduces the maximum ARP entries to 8K for all modules.)
Maximum HW ARP entries in VC of OS6900 (Distributed ARP not enabled)	Equal to capacity of module with lowest number of supported ARPs.
Maximum HW ARP entries in VC of OS6900 (Distributed ARP enabled)	VC of at least 4 (Q32 and X72) – 192K Please see the Distributed ARP section in the IP chapter of the Network Configuration Guide for configuration examples.
Maximum number of GRE tunnel interfaces per switch	127
Maximum number of IPIP tunnel interfaces per switch	127
Routing protocols supported over the tunnel interfaces	RIP, OSPF, BGP
Maximum next hops per ECMP entry	16

VRF Specifications

Platforms Supported	OS10K, 6900
OmniSwitch License Requirements	Advanced License required on OmniSwitch 6900 only.
Routing Protocols Supported	Static, IPv4, RIPv2, OSPFv2,BGP4, IS-IS
Maximum number of max profile VRF instances per switch (no low profiles)	64
Maximum number of low profile VRF instances per switch (no max profiles)	300 (OmniSwitch 10K) 128 (OmniSwitch 6900)
Maximum VRF instances per VLAN	1
Maximum OSPF VRF routing instances per switch	16
Maximum RIPv2 VRF routing instances per switch	16
Maximum BGP VRF routing instances per switch	32
SNMP version required for management	SNMPv3

IPv6 Specifications

Platforms Supported	OmniSwitch 10K, 6900
OmniSwitch License Requirements	Advanced License required on OmniSwitch 6900 only for IPv6 static routing and RIPng
RFCs Supported	1981 Path MTU Discovery for IP version 6 2375 IPv6 Multicast Address Assignments 2460 Internet Protocol, Version 6 (IPv6) Specification 2464 Transmission of IPv6 Packets over Ethernet Networks 2465 Management Information Base for IP Version 6: Textual Conventions and General Group 2466 Management Information Base for IP Version 6: ICMPv6 Group 2711 IPv6 Router Alert Option 3056 Connection of IPv6 Domains via IPv4 Clouds 3484 Default Address Selection for Internet Protocol version 6 (IPv6) 3493 Basic Socket Interface Extensions for IPv6 3542 Advanced Sockets Application Program Interface (API) for IPv6 3587 IPv6 Global Unicast Address Format 3595 Textual Conventions for IPv6 Flow Label 3596 DNS Extensions to Support IP Version 6 4007 IPv6 Scoped Address Architecture 4022 Management Information Base for the Transmission Control Protocol (TCP) 4113 Management Information Base for the User Datagram Protocol (UDP) 4193 Unique Local IPv6 Unicast Addresses 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers 4291 IP Version 6 Addressing Architecture 4294 IPv6 Node Requirements 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification 4861 Neighbor Discovery for IP version 6 (IPv6) 4862 IPv6 Stateless Address Autoconfiguration 5095 Deprecation of Type 0 Routing Headers in IPv6 5453 Reserved IPv6 Interface Identifiers 5722 Handling of Overlapping IPv6 Fragments
Maximum IPv6 interfaces	VLANs- 4096 Configured Tunnels - 255 6to4 Tunnels - 1
Maximum IPv6 global unicast or anycast addressess	10K
Maximum IPv6 global unicast addresses per IPv6 interface	50
Maximum IPv6 addresses assigned via VRRP configuration	1K

Maximum IPv6 hardware routes when there are no IPv4 routes present (includes dynamic and static routes)	OS10K / OS6900 – 256 (prefix >= 65) OS10K (U48/C48) – 8K (prefix <= 64) OS10K (U32S) – 6K (prefix <= 64) OS10K (U32E) – 8K (prefix <= 64) OS6900-X/T – 8K (prefix <= 64) OS6900-Q32/X72 – 6K (prefix <= 64) (Note: Exceeding these limits, or having IPv4 routes will result in some traffic being routed in software)
Maximum Number of RIPng Peers	10
Maximum Number of RIPng Interfaces	10
Maximum Number of RIPng Routes	5K
Maximum next hops per ECMP entry	16

IPsec Specifications

Platforms Supported	OmniSwitch 10K, 6900
IP Version Supported	IPv6
RFCs Supported	4301 - Security Architecture for the Internet Protocol 4302 - IP Authentication Header (AH) 4303 - IP Encapsulating Security Payload (ESP) 4305 - Cryptographic Algorithm Implementation Requirements for ESP and AH 4308 - Cryptographic Suites for IPsec
Encryption Algorithms Supported for ESP	NULL, 3DES-CBC, and AES-CBC
Key lengths supported for Encryption Algorithms	3DES-CBC - 192 bits AES-CBC - 128, 192, or 256 bits
Authentication Algorithms Supported for AH	HMAC-SHA1-96, HMAC-MD5-96, and AES- XCBC-MAC-96
Key lengths supported for Authentication Algorithms	HMAC-MD5 - 128 bits HMAC-SHA1 - 160 bits AES-XCBC-MAC - 128 bits
Master Security Key formats	Hexadecimal (16 bytes) or String (16 characters)
Priority value range for IPsec Policy	1 - 1000
Index value range for IPsec Policy Rule	1 - 10
SPI Range	256 - 999999999
Modes Supported	Transport

RIP Specifications

Platforms Supported	OmniSwitch 10K, 6900
RFCs Supported	RFC 1058–RIP v1 RFC 2453–RIP v2 RFC 1722–RIP v2 Protocol Applicability Statement RFC 1724–RIP v2 MIB Extension
Maximum Number of Interfaces	10
Maximum Number of Peers	100
Maximum Number of Routes	10K
Maximum next hops per ECMP entry	16

BFD Specifications

RFCs Supported	5880—Bidirectional Forwarding Detection 5881—Bidirectional Forwarding Detection for IPv4 and IPv6 (Single Hop) 5882—Generic Application of Bidirectional Forwarding Detection
Platforms Supported	OmniSwitch 10K, 6900
Maximum Number of BFD Sessions	OS6900 (per chassis) - 32 OS6900 (Virtual Chassis) - 100 OS10K (per NI) - 64 OS10K (Chassis/ Virtual Chassis) - 512
Protocols Supported	BGP, OSPF, VRRP Remote Address Tracking only, and Static Routes. IPv6 protocols not supported.
Modes Supported	Asynchronous Echo (Demand Mode not supported)
Transmit/Receive Timer	100-199 ms

DHCP Relay Specifications

Platforms Supported	OmniSwitch 10K, 6900
RFCs Supported	0951–Bootstrap Protocol 1534–Interoperation between DHCP and BOOTP 1541–Dynamic Host Configuration Protocol 1542–Clarifications and Extensions for the Bootstrap Protocol 2132–DHCP Options and BOOTP Vendor Extensions 3046–DHCP Relay Agent Information Option, 2001

DHCP Relay Implementation	Global DHCP Per-VLAN DHCP
DHCP Relay Service	BOOTP/DHCP (Bootstrap Protocol/Dynamic Host Configuration Protocol)
UDP Port Numbers	67 for Request 68 for Response
IP addresses supported for each Relay Service	Maximum of 256 IP addresses for each Relay Service.
IP addresses supported for the Per-VLAN service	Maximum of 256 VLAN relay services.
Maximum number of UDP relay services allowed per switch	10
Maximum number of VLANs to which forwarded UDP service port traffic is allowed	256

DHCP Server Specifications

Platforms Supported	OmniSwitch 10K, 6900
RFCs Supported	RFC 2131 - Dynamic Host Configuration Protocol RFC 3315 - Dynamic Host Configuration Protocol for IPv6 RFC 950 - Internet Standard Subnetting Procedure RFC 868 - Time Protocol RFC 1035 - Domain Implementation and Specification RFC 1191- Path MTU Discovery
DHCP Server Implementation	BOOTP/DHCP
UDP Port Numbers	67 for Request and Response (IPv4) 547 for Request (IPv6) 546 for Response (IPv6)
IP address lease allocation mechanisms:	**Static BootP:** IP address is allocated using the BootP configuration when the MAC address of the client is defined. **Static DHCP:** The network administrator assigns an IP address to the client. DHCP conveys the address assigned by the

	DHCP server to the client. **Dynamic DHCP:** The DHCP server assigns an IP address to a client for a limited period of time or until the client explicitly releases the address.
OmniSwitch IPv4 Configuration Files	dhcpd.conf dhcpd.pcy dhcpsrv.db
OmniSwitch IPv6 Configuration Files	dhcpdv6.conf dhcpdv6.pcy dhcpv6srv.db
Maximum number of leases	8000
Maximum lease information file size	375 KB

VRRP Specifications

Platforms Supported	OmniSwitch 10K, 6900
RFCs Supported	RFC 3768–Virtual Router Redundancy Protocol RFC 2787–Definitions of Managed Objects for the Virtual Router Redundancy Protocol
Compatible with HSRP	No
Maximum number of VRRPv2 and VRRPv3 virtual routers	255
Maximum number of IP addresses per instance	16

Server Load Balancing Specifications

Platforms Supported	OmniSwitch 10K, 6900
Maximum number of clusters	32
Maximum number of physical servers per cluster	32
Layer-3 classification	Destination IP address QoS policy condition
Layer-2 classification	QoS policy condition
Server health checking	Ping, link checks
High availability support	Hardware-based failover, VRRP, Chassis

	Management Module (CMM) redundancy
Networking protocols supported	Virtual IP (VIP) addresses
Maximum number of probes on a switch	40

IPMS Specifications

Platforms Supported	OmniSwitch 10K, 6900
RFCs Supported	RFC 1112 — Host Extensions for IP Multicasting RFC 2236 — Internet Group Management Protocol, Version 2 RFC 2710 -- Multicast Listener Discovery (MLD) for IPv6 RFC 2933 — Internet Group Management Protocol MIB RFC 3019 -- IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol RFC 3376 -- Internet Group Management Protocol, Version 3 RFC 3810 — Multicast Listener Discovery Version 2 (MLDv2) for IPv6 RFC 4541 — Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches RFC 4604 — Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast
IGMP Versions Supported	IGMPv1, IGMPv2, IGMPv3
Maximum number of IPv4 multicast flows	OS10K - 4K OS10K – 2K (XNI-U32S) OS6900 (X20/X40) - 2K OS6900 (T20/T40) – 2K OS6900-Q32/X72 – 20K (Note: Mixing an XNI-U32S with other modules in the same chassis reduces the maximum entries to 2K)

IPMSv6 Specifications

RFCs Supported	RFC 2710 — Multicast Listener Discovery for IPv6 RFC 3019 — IPv6 MIB for Multicast Listener Discovery Protocol 3306—Unicast-Prefix-based IPv6 Multicast Addresses RFC 3810 — Multicast Listener Discovery Version 2 for IPv6 RFC 4541 - Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener

	Discovery (MLD) Snooping Switches RFC 4604 - Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicas
Platforms Supported	OmniSwitch 10K, 6900
MLD Versions Supported	MLDv1, MLDv2
MLD Query Interval	1 to 65535 in seconds
MLD Router Timeout	1 to 65535 in seconds
MLD Source Timeout	1 to 65535 in seconds
MLD Query Response Interval	1 to 65535 in milliseconds
MLD Last Member Query Interval	1 to 65535 in milliseconds
Maximum number of IPv6 multicast flows	OS10K - 4K OS10K – 2K (XNI-U32S) OS6900 (X20/X40) - 2K OS6900 (T20/T40) – 2K OS6900-Q32/X72 – 20K (Note: Mixing an XNI-U32S with other modules in the same chassis reduces the maximum entries to 2K)

QoS Specifications

Maximum number of policy rules	8192
Maximum number of policy conditions	8192
Maximum number of policy actions	8192
Maximum number of policy rules per slot	1024 – OS10K-XNI-U32E, OS6900 1280 – OS10K-XNI-U32S 2560 OS6900-Q32/X72 5120 OS10K-GNI-C48E, OS10K-GNI-U48E)
Maximum number of bandwidth policy rules	2560 (OmniSwitch 10K) 512 (OmniSwitch 6900)
Maximum number of validity periods	64
Maximum number of policy services	256
Maximum number of groups (network, MAC, service, port)	2048
Maximum number of group entries	1024 per group (512 per service group)
Maximum number of Class of Service (CoS) queues per port.	8

Queue Set Profiles (QSP)	4
Weighted Random Early Detection profiles (WRP)	1 (OmniSwitch 6900) Not supported on the OmniSwitch 10K
Maximum number of QoS policy lists per switch	32 (includes the default list)
Maximum number of QoS policy lists per Universal Network Profile (UNP)	1

Policy Server Specifications

Platforms Supported	OmniSwitch 10K, 6900
LDAP Policy Servers RFCs Supported	RFC 2251–Lightweight Directory Access Protocol (v3) RFC 3060–Policy Core Information Model—Version 1 Specification
Maximum number of policy servers (supported on the switch)	5
Maximum number of policy servers (supported by PolicyView)	1

UNP Specifications

Platforms Supported	OmniSwitch 6900, 10K
Number of UNPs per switch	4K (Includes static and dynamic profiles)
Number of UNPs users per switch	2K
Authentication Type	MAC and 802.1x
Profile type	VLAN, SPB service, or VXLAN service
UNP port type	Bridge (VLAN-based classification) or access (service-based classification)
UNP classification rules	MAC address, MAC-range, IP address, and VLAN tag
Number of QoS policy lists per switch	32 (includes the default list)
Number of QoS policy lists per User Network Profile	1

Application Fingerprinting Specifications

Platforms Supported	OmniSwitch 10K, 6900
OmniSwitch Software License	N/A
Supported Packet Types	IP (IPv4 and IPv6)
Application signature type	REGEX
AOS provided signatures	Chatting Program, Mail, Networking or IETF Proposal Standard, P2P, Remote Access, VOIP

Authentication Server Specifications

Platforms Supported	OmniSwitch 10K, 6900
RADIUS RFCs Supported	RFC 2865–Remote Authentication Dial In User Service (RADIUS) RFC 2866–RADIUS Accounting RFC 2867–RADIUS Accounting Modifications for Tunnel Protocol Support RFC 2868–RADIUS Attributes for Tunnel Protocol Support RFC 2809–Implementation of L2TP Compulsory Tunneling through RADIUS RFC 2869–RADIUS Extensions RFC 2548–Microsoft Vendor-specific RADIUS Attributes RFC 2882–Network Access Servers Requirements: Extended RADIUS Practices
TACACS+ RFCs Supported	RFC 1492–An Access Control Protocol
LDAP RFCs Supported	RFC 1789–Connectionless Lightweight X.5000 Directory Access Protocol RFC 2247–Using Domains in LDAP/X.500 Distinguished Names RFC 2251–Lightweight Directory Access Protocol (v3) RFC 2252–Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions RFC 2253–Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names RFC 2254–The String Representation of LDAP Search Filters RFC 2256–A Summary of the X.500(96) User Schema for Use with LDAPv3
Other RFCs	RFC 2574–User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) RFC 2924–Accounting Attributes and Record Formats RFC 2975–Introduction to Accounting Management RFC 2989–Criteria for Evaluating AAA Protocols for Network Access
Maximum number of authentication servers in single authority mode	8
Maximum number of authentication servers in multiple authority mode	8
Maximum number of servers per Authenticated Switch Access type	8

Port Mapping Specifications

Platforms Supported	OmniSwitch 10K, 6900
Ports Supported	Ethernet (10 Mbps) Fast Ethernet (100 Mbps) Gigabit Ethernet (1 Gbps) 10 Gigabit Ethernet (10 Gbps) 40 Gigabit Ethernet (40 Gbps)
Port Mapping Sessions	8

Learned Port Security Specifications

Platforms Supported	OmniSwitch 10K, 6900
Ports eligible for Learned Port Security	Fixed and 802.1Q tagged
Ports not eligible for Learned Port Security	Link aggregate ports. 802.1Q (trunked) link aggregate ports.
Minimum number of learned MAC addresses allowed per LPS port	1
Maximum number of learned MAC addresses allowed per LPS port	1000
Maximum number of filtered MAC addresses allowed per LPS port	100
Maximum number of configurable MAC address ranges per LPS port	1

Diagnosing Switch Problems Specifications

Port Mirroring Specifications

Platforms Supported	OmniSwitch 10K, 6900
Ports Supported	Ethernet (10 Mbps) Fast Ethernet (100 Mbps) Gigabit Ethernet (1 Gbps) 10 Gigabit Ethernet (10 Gbps) 40 Gigabit Ethernet (40 Gbps)
Mirroring Sessions Supported	OmniSwitch 10K - 2 (OS10-XNI-U32 supports 1 session) OmniSwitch 6900 - 2
Combined Mirroring/Monitoring Sessions per Chassis	OmniSwitch 10K – 3 OmniSwitch 6900 - 2
N-to-1 Mirroring Supported	128 to 1
Number of RPMIR VLANs per session	1

Port Monitoring Specifications

Platforms Supported	OmniSwitch 10K, 6900
Ports Supported	Ethernet (10 Mbps) Fast Ethernet (100 Mbps) Gigabit Ethernet (1 Gbps) 10 Gigabit Ethernet (10 Gbps) 40 Gigabit Ethernet (40 Gbps)
Monitoring Sessions Supported	OmniSwitch 10K – 1 OmniSwitch 6900 - 1
Combined Mirroring/Monitoring Sessions per Chassis	OmniSwitch 10K - 3 OmniSwitch 6900 - 2
File Type Supported	ENC file format (Network General Sniffer Network Analyzer Format)

sFlow Specifications

RFCs Supported	3176 - sFlow Management Information Base
Platforms Supported	OmniSwitch 10K, 6900
Receiver/Sampler/Polling Instances	2
Sampling	length of packet type of frame source and destination MACs source and destination VLANs source and destination priorities source and destination IP addressessource and destination ports tcp flags and tos
Polling	In octets Out octets Number of Rx Unicast packets Number of Tx Unicast packets Number of Rx Multicast packets Number of Tx Multicast packets Number of Rx Broadcast packets Number of Tx Broadcast packets In Errors Out Errors

RMON Specifications

RFCs Supported	2819 - Remote Network Monitoring Management

	Information Base
Platforms Supported	OmniSwitch 10K, 6900
RMON Functionality Supported	Basic RMON 4 group implementation –Ethernet Statistics group –History (Control and Statistics) group –Alarms group –Events group
RMON Functionality Not Supported	RMON 10 group* RMON2* –Host group –HostTopN group –Matrix group –Filter group –Packet Capture group (*An external RMON probe that includes RMON 10 group and RMON2 be used where full RMON probe functionality is required.)
Flavor (Probe Type)	Ethernet/History/Alarm
Status	Active/Creating/Inactive
History Control Interval (seconds)	1 to 3600
History Sample Index Range	1 to 65535
Alarm Interval (seconds)	1 to 2147483647
Alarm Startup Alarm	Rising Alarm/Falling Alarm/ RisingOrFalling Alarm
Alarm Sample Type	Delta Value/Absolute
RMON Traps Supported	RisingAlarm/FallingAlarm These traps are generated whenever an Alarm entry crosses either its Rising Threshold or its Falling Threshold and generates an event configured for sending SNMP traps.

Switch Health Specifications

Platforms Supported	OmniSwitch 10K, 6900

Health Functionality Supported	– Switch level CPU Utilization Statistics (percentage);
	– Switch/module/port level Input Utilization Statistics (percentage);
	– Switch/module/port level Input/Output Utilization Statistics (percentage);
	– Switch level Memory Utilization Statistics (percentage);

	– Device level (e.g., Chassis/CMM) Temperature Statistics (Celsius).
Monitored Resource Utilization Levels	–Most recent utilization level; –Average utilization level during last minute; –Average utilization level during last hour; –Maximum utilization level during last hour.
Resource Utilization Raw Sample Values	Saved for previous 60 seconds.
Resource Utilization Current Sample Values	Stored.
Resource Utilization Maximum Utilization Value	Calculated for previous 60 seconds and stored.
Utilization Value = 0	Indicates that none of the resources were measured for the period.
Utilization Value = 1	Indicates that a non-zero amount of the resource (less than 2%) was measured for the period.
Percentage Utilization Values	Calculated based on Resource Measured During Period/Total Capacity.
Resource Threshold Levels	Apply automatically across all levels of switch (switch/module/port).
Rising Threshold Crossing	A Resource Threshold was exceeded by its corresponding utilization value in the current cycle.
Falling Threshold Crossing	A Resource Threshold was exceeded by its corresponding utilization value in the previous cycle, but is not exceeded in the current cycle.
Threshold Crossing Traps Supported	Device, module, port-level threshold crossings.

VLAN Stacking Specifications

Platforms Supported	OmniSwitch 10K, 6900
IEEE Standards Supported	IEEE 802.1Q, 2003 Edition, IEEE Standards for Local and metropolitan area networks—Virtual Bridged Local Area Networks P802.1ad/D6.0 (C/LM) Standard for Local and Metropolitan Area Networks - Virtual Bridged Local Area Networks - Amendment 4: Provider Bridges
Maximum number of Services	4K
Maximum number of SVLANs	4K
Maximum number of SAPs	8K
Maximum number of SAP Profiles	8K (1K if profiles assign priority or bandwidth)
Maximum number of SAP profile VLAN translation or double tagging VPAs	8K (4K on OS10K XNI-U32 module)

Maximum number of customer VLANs (CVLANs) associated with a SAP	4K

Switch Logging Specifications

Platforms Supported	OmniSwitch 10K, 6900
Functionality Supported	High-level event logging mechanism that forwards requests from applications to enabled logging devices.
Functionality Not Supported	Not intended for debugging individual hardware applications.
Number of Syslog Servers Supported	12
Logging Devices	Flash Memory/Console/IP Address
Application ID Levels Supported	IDLE (255), DIAG (0), IPC-DIAG (1), QDRIVER (2), QDISPATCHER (3), IPC-LINK (4), NI- SUPERVISION (5), INTERFACE (6), 802.1Q (7), VLAN (8), GM (9), BRIDGE (10), STP (11), LINKAGG (12), QOS (13), RSVP (14), IP (15), IPMS (17), AMAP (18), GMAP (19), SLB(25), AAA (20), IPC-MON (21), IP-HELPER (22), PMM (23), MODULE (24), EIPC (26), CHASSIS (64), PORT-MGR (65), CONFIG (66), CLI (67), SNMP (68), WEB (69), MIPGW (70), SESSION (71), TRAP (72), POLICY (73), DRC (74), SYSTEM (75), HEALTH (76), NAN-DRIVER (78), RMON (79), TELENET (80), PSM (81), FTP (82), SNMI (83), DISTRIB (84), EPIL0GUE (85), LDAP (86), NOSNMP (87), SSL (88), DBGGW (89), LANPOWER (108)
Severity Levels/Types Supported	2 (Alarm - highest severity), 3 (Error), 4 (Alert), 5 (Warning) 6 (Info - default), 7 (Debug 1), 8 (Debug 2), 9 (Debug 3 - lowest severity)

Ethernet OAM Specifications

Platforms Supported	OmniSwitch 10K, 6900
Standards Supported	IEEE 802.1ag Version 8.1–Connectivity Fault Management IEEE 802.1D–Media Access Control (MAC) Bridges IEEE 802.1Q–Virtual Bridged Local Area Networks ITU-T Y.1731–OAM Functions and Mechanisms for Ethernet-Based Networks
Maximum Maintenance Domains (MD) per Bridge	8

Maximum Maintenance Associations (MA) per Bridge	128
Maximum Maintenance End Points (MEP) per Bridge	256
Maximum MEP CMM Database Size	1K
Minimum CCM interval	100ms

Service Assurance Specifications

Platforms Supported	OmniSwitch 10K, 6900
Standards Supported	N/A

Advanced Routing Guide Specifications

OSPF Specifications

Platforms supported	OmniSwitch 10K, 6900
RFCs supported	1370—Applicability Statement for OSPF 1850—OSPF Version 2 Management Information Base 2328—OSPF Version 2 2370—The OSPF Opaque LSA Option 3101—The OSPF Not-So-Stubby Area (NSSA) Option 3623—Graceful OSPF Restart
Maximum number of areas	10 (OmniSwitch 6900) 20 (OmniSwitch 10K)
Maximum number of interfaces per router	128 (OmniSwitch 6900) 350 (OmniSwitch 10K)
Maximum number of interfaces per area	100 (OmniSwitch 6900) 350 (OmniSwitch 10K)
Maximum number of Link State Database entries	100K
Maximum number of neighbors per router	254 (OmniSwitch 6900) 350 (OmniSwitch 10K)
Maximum number of neighbors per area	254 (OmniSwitch 6900) 350 (OmniSwitch 10K)
Maximum number of SW routes	OS10K - 64K OS6900 – 32K (Depending on the number of interfaces/ neighbors, this value may vary.)
License Requirements	Advanced License required on OmniSwitch 6900 only.

OSPFv3 Specifications

Platforms supported	OmniSwitch 10K, 6900
RFCs supported	RFC 1826—IP Authentication Header RFC 1827—IP Encapsulating Security Payload RFC 2553—Basic Socket Interface Extensions for IPv6 RFC 2373—IPv6 Addressing Architecture RFC 2374—An IPv6 Aggregatable Global Unicast Address Format RFC 2460—IPv6 base specification RFC 2470—OSPF for IPv6

Maximum number of areas	5
Maximum number of interfaces per router	20
Maximum number of interfaces per area	16
Maximum number of Link State Database entries per router	20K
Maximum number of neighbors per router	128
Maximum number of neighbors per area	16
Maximum number of routes per router	10K (Depending on the number of interfaces/neighbors, this value may vary.)
License Requirements	Advanced License required on OmniSwitch 6900 only.

ISIS Specifications

Platforms supported	OmniSwitch 10K, 6900
RFCs supported	1142-OSI IS-IS Intra-domain Routing Protocol 1195-OSI IS-IS for Routing in TCP/IP and Dual Environments 3373-Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies 3567-Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication 2966-Prefix Distribution with two-level IS-IS (Route Leaking) support 2763-Dynamic Host name exchange support 3719-Recommendations for Interoperable Networks using IS-IS 3787-Recommendations for Interoperable IP Networks using IS-IS draft-ietf-isis-igp-p2p-over-lan-05.txt-Point-to-point operation over LAN in link-state routing protocols 5308 - IS-IS support for IPv6 (Routing IPv6 with IS-IS)
Maximum number of areas (per router)	3
Maximum number of L1 adjacencies per interface (per router)	70
Maximum number of L2 adjacencies per interface (per router)	70
Maximum number of IS-IS interfaces (per router)	70

Maximum number of Link State Packet entries (per adjacency)	255
Maximum number of IS-IS routes	24000
Maximum number of IS-IS L1 routes	12000
Maximum number of IS-IS L2 routes	12000
License Requirements	Advanced License required on OmniSwitch 6900 only.

BGP Specifications

Platforms Supported	OmniSwitch 10K, 6900
RFCs Supported	1771/4271–A Border Gateway Protocol 4 (BGP-4) 2439–BGP Route Flap Damping 3392/5492–Capabilities Advertisement with BGP-4 2385–Protection of BGP Sessions via the TCP MD5 Signature Option 1997–BGP Communities Attribute 4456–BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP) 3065–Autonomous System Confederations for BGP 4273–Definitions of Managed Objects for BGP-4 4486–Subcodes for BGP Cease Notification 4760–Multiprotocol Extensions for BGP-4 2545–Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing 2918 - Route Refresh Capability for BGP-4 4724 - Graceful Restart Mechanism for BGP 6793 – BGP 4-Octet ASN 5668- 4-Octet AS Specific BGP Extended Community
BGP Attributes Supported	Origin, AS Path, Next Hop (IPv4), MED, Local Preference, Atomic Aggregate, Aggregator (IPv4), Community, Originator ID, Cluster List, Multiprotocol Reachable NLRI (IPv6), Multiprotocol Unreachable NLRI (IPv6), AS4 Path, AS4 Aggregator (IPv4), AS, Specific Extended Community.
Maximum number of peers	512
Maximum number of networks	4K
Maximum number of aggregation addresses	2K
Maximum number of routes	OS10K - 256K OS6900 – 128K
Maximum number of policies	1K
License Requirements	Advanced License required on OmniSwitch 6900 only.

Multicast Boundary Specifications

Platforms Supported	OmniSwitch 10K, 6900
RFCs Supported	2365—Administratively Scoped IP Multicast 5132 - IP Multicast MIB
Valid Scoped Address Range	239.0.0.0 to 239.255.255.255
License Requirements	Advanced License required on OmniSwitch 6900 only.

DVMRP Specifications

Platforms Supported	OmniSwitch 10K, 6900
RFCs supported	1075 - Distance Vector Multicast Routing Protocol, Version1 4087—IP Tunnel MIB draft-ietf-idmr-dvmrp-v3-09.txt - Distance Vector Multicast Routing Protocol, Version 3 2715—Interoperability Rules for Multicast Routing Protocols
DVMRP version supported	DVMRPv3.255
DVMRP attributes supported	Reverse Path Multicasting, Neighbor Discovery, Multicast Source Location, Route Report Messages, Distance metrics, Dependent Downstream Routers, Poison Reverse, Pruning, Grafting, DVMRP Tunnels
DVMRP timers supported	Flash update interval, Graft retransmissions, Neighbor probe interval, Neighbor timeout, Prune lifetime, Prune retransmission, Route report interval, Route hold-down, Route expiration timeout
Maximum number of interfaces	384 **Note**: Maximum 384 combined Multicast Interfaces between PIMv4, PIMv6 and DVMRP
Multicast protocols per interface	1 (PIM and DVMRP cannot be enabled on the same interface)
License Requirements	Advanced License required on OmniSwitch 6900 only.

PIM Specifications

Platforms supported	OmniSwitch 10K, 6900
RFCs supported	2365 - Administratively Scoped IP Multicast 4601—Protocol Independent Multicast-Sparse Mode (PIM-SM) Protocol Specification 4007 - IPv6 Scoped IP Multicast 5060 - Protocol Independent Multicast MIB 5132 —IP Multicast MIB

	3569—An Overview of Source-Specific Multicast (SSM) 3973—Protocol Independent Multicast-Dense Mode (PIM-DM) 5059 - Bootstrap Router (BSR) Mechanism for PIM 5240 - Protocol Independent Multicast (PIM) Bootstrap Router MIB 2715—Interoperability Rules for Multicast Routing Protocols
PIM-SM version supported	PIM-SMv2
PIM attributes supported	Shared trees (also referred to as RP trees), Designated Routers (DRs), Bootstrap Routers (BSRs), Candidate Bootstrap Routers (C-BSRs), Rendezvous Points (RPs) (applicable only for PIM-SM), Candidate Rendezvous Points (C-RPs)
PIM timers supported	C-RP expiry, C-RP holdtime, C-RP advertisement, Join/Prune, Probe, Register suppression, Hello, Expiry, Assert, Neighbor liveness
Maximum PIM interfaces	384 **Note**: Maximum 384 combined Multicast Interfaces between PIMv4, PIMv6 and DVMRP
Maximum Rendezvous Point (RP)	100
Maximum Bootstrap Routers (BSRs)	1
Multicast Protocols per Interface	1 (PIM and DVMRP cannot be enabled on the same IP interface)
Valid SSM IPv4 Address Ranges	232.0.0.0 to 232.255.255.255
Valid SSM IPv6 Address Ranges	FF3x::/32
License Requirements	Advanced License required on OmniSwitch 6900 only

Multicast Border Router Specifications

Platforms Supported	OmniSwitch 10K, 6900
RFCs Supported	4601—Protocol Independent Multicast-Sparse Mode (PIM-SM) Protocol Specification 3973—Protocol Independent Multicast-Dense Mode (PIM-DM) 2715—Interoperability Rules for Multicast Routing Protocols draft-ietf-idmr-dvmrp-v3-09.txt - Distance Vector Multicast Routing Protocol, Version 3
MBR Interoperability	DVMRP interoperability with IPv4 PIM (PIM-SM and PIM-DM only).
OmniSwitch License Requirements	Advanced License required on OmniSwitch 6900 only.

Data Center Switching Guide Specifications

DCB Specifications

Platforms Supported	OmniSwitch 6900 and the following OmniSwitch 10K modules: • OS10K-QNI-U8 (8 x 40G) • OS10K-QNI-U4 (4 x 40G) • OS10K-XNI-U32E (32 x 10G) • OS10K-XNI-U16E (16 x 10G) • OS10K-XNI-U16L (8 x 10G, 8 x 1G)
OmniSwitch Software License	Data Center
IEEE Standards supported	802.1Qbb—Priority-based Flow Control 802.1Qaz D2.5—Enhanced Transmission Selection 802.1Qaz D2.5—Data Center Bridging Exchange 802.1Q-REV/D1.5—Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks
Maximum number of DCB profiles	128 profiles: • Profiles 1–11 are predefined, with profile 8 serving as the default profile for all ports. • Profiles 12–128 are reserved for user-defined (custom) profiles.
Maximum number of lossless queues (priorities)	110 total per switch (OmniSwitch 6900) 8 per-port (OmniSwitch 10K)
DCB TLVs supported	ETS Configuration ETS Recommendation PFC Configuration (Application Priority TLV not supported)

Shortest Path Bridging Specifications

Platforms Supported	OmniSwitch 10K, 6900
OmniSwitch Software License	Advanced
IEEE Standards supported	802.1aq/D3.6: Draft February 10, 2011—Virtual Bridged Local Area Networks-Amendment 9: Shortest Path Bridging 802.1ah/D4.2: DRAFT March 26, 2008— Virtual Bridged

	Local Area Networks–Amendment 6: Provider Backbone Bridging
IETF Internet-Drafts Supported	draft-ietf-isis-ieee-aq-05.txt—ISIS Extensions Supporting IEEE 802.1aq Shortest Path Bridging IETF draft—IP/IPVPN services with IEEE 802.1aq SPBB networks IETF draft—IP/IPVPN services with IEEE 802.1aq SPB networks
SPB Mode Supported	SPB-M (MAC-in-MAC)
IP over SPB-M	IPv4 (VPN-Lite and L3 VPN) VRF-to-ISID mapping (one-to-one, many-to-one)
Maximum number of ISIS-SPB instances per switch.	1
Maximum number of BVLANs per switch	4
Number of equal cost tree (ECT) algorithms supported.	16
Maximum number of service instance identifiers (I-SIDs) per switch	OS6900-Q32 – 8K OS6900-X72 – 8K All other models - 1K
Maximum number of VLANs or SVLANs per I-SID	4K
Maximum number of SAPS	OS10K - 8K OS6900 –X20/X40 – 4K OS6900-T20/T40 - 8K OS600-Q32/X72 8K Note: In a VC with OS6900-X models the maximum is 4K.
Maximum Transmission Unit (MTU) size for SPB services.	9K (not configurable at this time)

FIP Snooping Specifications

Platforms Supported	OmniSwitch 10K, 6900
OmniSwitch Software License	Data Center
INCITS Standards Supported	T11—Fibre Channel Backbone - 5 (FC-BB-5) Rev 2.00 June 4, 2009 FC-BB-5 Annex C: Increasing FC-BB_E Robustness Using Access Control Lists T11—Switch Fabric - 5 (FC-SW-5) Rev 8.5 June 3,

	2009
Maximum number of FIP Snooping Sessions	128
Port types supported	10G or faster Ethernet with DCB profile and DCBx enabled with PFC/ETS active (ports and link aggregates)

FCoE Gateway Specifications

Platforms Supported	OmniSwitch 6900 (7.3.3)
OmniSwitch Software License	Data Center
INCITS Standards Supported	• FC-PI-4 Fibre Channel T11/08-138v1 • FC-PI-5 Fibre Channel T11 2118-D/Rev 6.10 • FC-BB-5 Backbone 5 T11/1871-D • FC-BB-6 Backbone 6 T11/2159-D (CNA switching only)
Fibre Channel functionality supported	• FCoE transit bridge - FCoE tunneling of encapsulated FC frames - FCoE initialization protocol (FIP) snooping • FCoE/FC gateway switch - N_Port proxy (NPIV) - F_Port proxy (Reverse-NPIV) - E_Port proxy (E2E-tunnel)
Supported Port types	• Fibre Channel for NPIV gateway—OS-XNI-U12E module with SFP-FC-SR transceiver • Ethernet for FCoE/FIP snooping—10G or faster with DCB profile, DCBx enabled with PFC/ETS active (ports and link aggregates)
OmniSwitch 64-bit World Wide Node Name (WWNN)	10:00:xx:xx:xx:xx:xx:xx (xx = switch MAC address)
OmniSwitch 64-bit World Wide Port Name (WWPN) for each Fibre Channel port	10:00:xx:xx:xx:xx:xx:xx (xx = port MAC address)
VSAN–FC port associations Multiple FC port assignments per VSAN allowed.	Only one VSAN assignment per FC port allowed.
VSAN–FCoE VLAN mapping	One-to-One
VSAN scalability per switch	Based on the number of FC ports (for example, if switch has 12 FC ports, then 12 VSANs; one for each FC port). Note that an FC port configured as an E2E tunnel endpoint does not use up a VSAN assignment.
Maximum number of VSANs per network	4094
E2E tunnel scalability	One tunnel termination per FC port up to the number

	of available FC ports on the switch or virtual chassis.
MTU size supported for SANs	2180
Load Balancing	NP_Port load balancing only: • Dynamic • Dynamic-reorder • ENode-based • Static

Virtual Machine Classification Specifications

UNP (vNP) Specifications

Platforms Supported	OmniSwitch 10K, 6900
Number of UNPs per switch	4K (includes static and dynamic profiles).
Number of UNP users per switch	2K
Authentication type	MAC-based authentication
Profile type	VLAN or Shortest Path Bridging (SPB)
UNP port type	Bridge (VLAN-based classification) or access (service-based classification)
UNP classification rules	MAC address, MAC-range, IP address, and VLAN tag
Number of QoS policy lists per switch	32 (includes the default list)
Number of QoS policy lists per UNP	1

EVB Specifications

Platforms Supported	OmniSwitch 10K, 6900
OmniSwitch Software License	Data Center
IEEE Standards Supported	P802.1Qbg Standard Draft, Revision D2.2. February 18, 2012—Virtual Bridged Local Area Networks–Amendment 21: Edge Virtual Bridging
EVB mode	Bridging (virtual machines request the required CVLAN ID tag)
Edge Relay (ER) support	Single ER per switch port. The ER can operate as a Virtual Ethernet Port Aggregator (VEPA) or as a Virtual Ethernet Bridge (VEB).

VXLAN Specifications

Platforms Supported	OmniSwitch 6900-Q32/X72
OmniSwitch Software License	Advanced
RFCs Supported	7348 —VXLAN: A Framework for Overlaying Layer 2 Virtualized Networks over Layer 3 Networks.
VXLAN segments (L2 overlay networks)	16 million
VXLAN service instances	8K
VXLAN Tunnel End Points in a VXLAN network.	500
VXLAN UDP destination ports	8 (default UDP port number is 4789).
VXLAN Service Access Points (SAP)	8K (per device or per Virtual Chassis)
VXLAN SAPs with a VLAN ID range	8 SAPs per service access port
Service access ports with SAPs that contain a VLAN ID range	255
VXLAN Network IDs (VNIs)	4K
Multicast Groups	500
Multicast protocol supported	Bidirectional PIM (BIDIR-PIM)

VXLAN Snooping Specifications

Platforms Supported	OmniSwitch 10K, 6900
OmniSwitch Software License	No software license required
RFCs Supported	7348—VXLAN: A Framework for Overlaying Layer 2 Virtualized Networks over Layer 3 Networks.
Packet Sampling Rate	1K packets-per-second on each module

Appendix G: Fixed Problem Reports

To improve the quality of the official AOS releases and the responsiveness of PR resolution, ALE is committed to reducing the number of parallel field releases requiring support. As a first step to encourage upgrades to 7.3.4 R02 a concerted effort of validation has been done on key field issues found in previous AOS releases and to incorporate their fixes into 7.3.4.R02. Please see the table below for the list of these important PRs that were addressed in 7.3.4.R02.

158712	10K debug stp bpdu-trace start all 4/48 does not capture BPDU
160665	show interfaces counters fields "InBits/s" and "OutBits/s" are not accurate
163249	The "swlog output flash-file-size" command is accepted, but doesn't work
165416	Vip-Vlan Name is not taken in account when creating a Vip-Vlan
166108	OS10K - Power reduced, 2400 available, 570 more needed, shutting down NIs
166729	10K dropping 9198 OSPF DD packet
166810	OS6900 sends STP frames on MCLAG
167084	HA vlan in L3 with igmp does not work / ARP entry not created
167101	BFP convergence delay with ERP in network
167148	AOS Switch does not responds to MS Windows 7 ARP with APIPA source IP.
167302	OS_6900 Vlan1 tag removed after a reboot
167979	Warning message to be displayed if an SNMP station is configured with a non-existent user
168242	OS_6900 not able to rebuild the MC streams once uplinks toggled.
168297	DST for AEST needs to be modified in 7.x.x codes
169584	10K 3rd static route BFD don't come up until IP interface is ping
169736	SNMP: OID slbServerFlows (.1.3.6.1.4.1.6486.801.1.2.1.20.1.1.3.1.1.10) is not implemented.
169773	10K VRRP unable to initialized after upgrade from 7.1.1.R01 to 7.2.1.R02
169994	ERROR: unknown object type failure while executing ?show ip bgp path neighbor-rcv n.n.n.n?
170680	10K: pmd analysis needed
171467	10K static mac or static multicast mac not loaded correctly on port or linkagg port
171534	OS10K crash when creating RMON probes alarm. Need pmd analysis and fix.
171535	ARP source IP shows as 0.0.0.0 with Windows 7 PC and UNP VLAN assignment issues
172693	Need crash analysis for 6900
173232	LLDP: lldp local-management-address is using other interface instead of Loopbacko
175013	An error message is displayed upon configuring more than one multi-chassis linkagg
175460	OSPF cost configuration requires the OSPF interface to be disabled: Want to apply config on fly
176339	OS6900 getting error: Out of TCAM processors on 1/1(0)
176553	Error in swlogs ChassisSupervisor niMgr alert(3) Incompatible expansion module and dump files genera
176659	Remote command-log shows disabled even after enabling it.
176903	Default route with subnet /24 accepted by switch for EMP network.
176941	inconsistent issues with qos policies in OS6900 and error is "Out of TCAM processors on 0/1(0)".
176980	ERP state in pending with blocked ports on non-RPL node.

177354	OS6900 Sflow not working with 7.3.1 code, works fine with 7.2.1.R02. Sflow UDP packet shows source p
177481	We are having the issue with NTP synchronization in OS10K
177565	Port configured in boot.cfg for a default vlan other than 1 is still a member of VLAN 1 after boot (
177623	unp classification does not work on unp access port
177631	BGP: OS6900 crash after disabling the aspath lists and do "ip bgp neighbor 194.44.88.251 clear soft
177661	MIBWALK on Q-BRIDGE-MIB::dot1qTpFdbPort.1 fails
177686	Reference to PR# 176980. Connectivity issue between MC-LAG peers for newly created VLANs.
177697	Unable to ping the ip interface configured on switch from directly connected client on same subnet.
177812	BGP aspath-list filters do not work
177815	Ni not powering up after a power failure/reboot
177953	ip-helper DHCP/UDP relay issue in a MC-LAG environment
177986	BPDUs from OS10K-VC are not tunneled across the PBB network
178215	OS6900 - SPB SAP not working properly over VC
178279	OS 6900 -X20 switch with 7.3.1.R01 the messgae linkAggCmm main info(5) mip_msg_queuing NO 1 error s
178288	OS10K - STP BLK linkagg does not transition from BLK/BACK to FWD/DESG state
178366	MCLAG/VFL link not passing traffic until primary link is admin down
178419	OS6900 switch running 7.3.1.645.R01, system name changing to default after a reboot.
179173	Customer informed there's a 10mins wait time before VC status is ready after switch upgrade.
179291	OS10K - VRRP issue over SPB network
179374	7.3.1.R01: wrong show command does not return error message
179652	In Webview of OS6900 showing type unknow (9) for unpQtag port on VLAN members.
180081	wants to see the traps On Console prompt
180086	VLANs still exists after deleting it from OS10K MC-LAG
180256	Device or resource busy and vpaType 4 mode 1 failed messages seen.
180262	[TYPE1] Unable to configure the NTP server using ntp's DNS Name
180376	Loopback0 Ip address not able to ping with OS 6900
180397	In OS6900 VC setup we are getting continuous error message in swlog
180667	Management ports such as Loopback, EMP, Management, etc, and routing interfaces report interface spe
180816	Telnet using DNS name thorws error message "This is not an authorized host"
180911	Switch crashed when smnp set with 40 characters
181043	Not all the LACP ports seen during MIB walk.
181083	ip6nid library(portmgrlibni) error(2) Message seen in logs
181188	MSTI configuration is not displayed on OS6900 VC setup
181197	redistributing of OSPF routes stopped after the crash
181297	Unable to issue "show configuration snapshot" and "write memory".
181297	Unable to issue "show configuration snapshot" and "write memory".
181423	ERROR: ESM: Slot/Port out of range <101041>
181453	switch getting healthModuleMemory1MinAvg

181645	RADIUS Authentication issues with OS10K wu
181648	SPB issue: Devices are unable to access remote site if they have more than 2 SPB hops in between
181702	Two OS10K switches getting some error messages on the swlogs continuously
182068	OS6900-T40 switch error seen plGetIfIndexFromPortInfo@7686: Out of range chassis ID with 7.3.2.R01
182182	Illegal static routes allowed in OS6900 ip static-route 10.64.472.0/24 gateway 10.40.1.120
182249	IGMP packets receives on Omni switch port which is not a part of specific VLAN.
182258	After reload of OS6900 VC setup ldap configuration is missing
182291	LACP not establishing between AOS 7 and HP Proliant server.
182383	OS6900 - BPDU not properly tunneled through SAP ports; STP loop seen after ISSU upgrade to 7.3.1.730
182527	PMD is generated each time an IP interface is created
182528	MAC address collisions
182528	MAC address collisions
182566	ACL action "priority" modifies 802.1p field
182641	OS10K 40G ping lost through out the switch after upgrade from 7.2.1.354.R02 to 7.3.2.344.R01
182814	DNS is not working on OS6900
183158	OS6900 - Auto-Fabric feature: new switch out of box automatically generate a SPB configuration witho
183294	OS6900, Auto-fabric feature: one minute discovery logs flooding swlog.
183459	debug stp bpdu-stats show output is not consistent with stpni_printStats
183522	Unable to dispaly the VLAN in configuration.
183522	Unable to dispaly the VLAN in configuration.
183742	OS6900: Frame Loss on traffic across Virtual Fabric Link
183899	Swlogs filled with error message VlanMgrNi main error(2) and slave chassis filled with message bcmd
183903	During issu upgrade from 7.3.1.682 to 7.3.1.748 (Chassis-1 rebooting), Linkagg-103 which had only on
184043	Two OS6900-virtual chassis connected via static linkagg learing MAC-address in wrong ports running A
184070	System Timezone for South Africa or Disabling DST
184338	OS 10K fans working at 85 % after upgrade to 7.3.1.748
184338	OS 10K fans working at 85 % after upgrade to 7.3.1.748
184425	ARP Enhancement.
184523	[OS 10K]- HA VLAN not flooding packets correctly, if source and destination are on the same port, p
184659	Ethertype displayed in decimal
184680	OS6900 crashed after connecting to Nexus 5000 running NXOS v5
184703	Misleading output in "show qos qsi dcb dcbx status" in the "Error" column
184707	Logging for "fipsni" enables logging for all appids
184885	Mac-learning issue on OS10K
185102	OS10K VC setup getting messages in swlog. swlogd: ChassisSupervisor i2cMgrHwThread info(5) All swi
185277	Messages "ipni arp info(5) arp info overwritten" seen after upgrading OS6900 to 7.3.2.344.R01.
185453	Flood rate applied goes missing in show configuration snapshot
185771	With OS 6900 after the port monitoring command it is not responsive and not able to remove the port

185771	With OS 6900 after the port monitoring command it is not responsive and not able to remove the port
186260	lost OSPF neighbors and ERP issue after the upgrade.
186262	App-fingerprint not working with MC-LAG
186335	OS10K: Experience L3 Packet Lost if inject 8000 arp broadcast into Qtagg port
186545	Health monitor trap doesnt mentioned the chassis number in VC
186592	10K/6900 VC - log flooding console session after ISSU upgrade or vc-takeover
186715	OS10K - VC split
186715	OS10K - VC split
186988	OS6900: High CPU caused by port-monitoring pmmcmmd task.
187165	ChassisSupervisor fan & temp Mgr info(5) temperature 67 <= 74, lower fan_load to 55%
187237	10K-VC :: SLB VIP@ connectivity issue when launching ?vc-takeover?
187237	10K-VC :: SLB VIP@ connectivity issue when launching ?vc-takeover?
187267	OS6900 memory full and reboot.
187279	unit-0 port_cbl_cable entry 0 parity error.
187323	Switch crashed during stpNi initialization.
187330	OS6900 timezone and swlog time synchronization issue
187352	No matches for policy rules on VFL ports; VFL ports should not be allowed to be configured for sourc
187396	BUG: spinlock lockup on CPU#0 issue on OS6900 with VC
187413	cp: write error: No space left on device.
187413	cp: write error: No space left on device.
187461	10K-VC ISSU upgrade failed
187493	The OAM Loopback displays "100% packet loss" and Link trace displays "ERROR: LTR Entry does not exis
187493	The OAM Loopback displays "100% packet loss" and Link trace displays "ERROR: LTR Entry does not exis
187494	All the OSPF neighbor went "INIT" state when VC Master power off
187628	OS6900: snmpget of oid returns next entry in table instead of correct one.
187628	OS6900: snmpget of oid returns next entry in table instead of correct one.
187931	Need crash analysis on OS6900 in VC setup
187931	Need crash analysis on OS6900 in VC setup
188302	plGetPortInfoFromBasePort@7483: Out of range VC chassis ID 3 error message seen in logs
188302	plGetPortInfoFromBasePort@7483: Out of range VC chassis ID 3 error message seen in logs
188346	stpni_printStats table - code changes needed in order to to print the local port number.
188346	stpni_printStats table - code changes needed in order to to print the local port number.
188390	Port-Mirroring causing issues in the network.
188434	Ni7 interface counters show as zero when the interfaces are up and passing traffic on OS10K
188675	OS6900 switch getting rebooted very often and pmd generated.
188746	lldpCmm library(plApi) error(2) plGetIfIndexFromBasePort@1649: Get port info (basePort 40000055)
189003	SNMPWALK shows incorrect port number
189005	Unable to ping Loopback0 of OS6900 from OS6850

189017	EMP ip address is not reachable after changing the ip address.
189190	show license info is blank after reload of OS6900 VC-732.R01
189281	Parity errors in OS6900 running 732.413.R01 causing the switch not to learn mac-addresses properly.
189589	When CMM_A of the primary Virtual Chassis is removed, arp broadcast packets stopped forwarding out o
189672	OSPF -unplanned- graceful restart does not work as expected during VC Master chassis failure MD5 seq
189709	An error is thrown when copying files between VC members
189944	interface ingress-bandwidth and "interface flood-limit" deletation failed in AOS 7.
190182	DHCP relay is not working in OS6900
190436	vfcn error: [vfccQsHandleLinkEvents:276] VFCC : gport 12 LINK UP Invalid Speed 0 sts 1.
190509	On a VC of six OS6900, different behaviour seen for split detection between chassis.
190572	OS6900 errors seen frequntly: ipni arp info(5) arp info overwritten messages
190839	In a specific scenario eoamCmm task generates pmd.
190891	OS6900 Incorrectly ARPs for it's own VRRP address.
190901	show qos qsp detail doesn't give any output
190908	ERROR: CIR cannot be greater than PIR incorrect error message
190924	7.3.3 vmCmm crash due to VLAN description having 32 characters
191045	port goes up/down every one minute and network outage
191201	Remote Fault Propagation is not working on OS6900.
191308	In OS6900 running 7.3.2.439, the command vrrp delay is not taking effect.
191494	10K-VC : invalid IP state
191547	FP_METER_TABLE entry 1 parity error
191665	OS6900 ICMPv6 neighbor solicitation issue.
191741	[TYPE1] Issues with System daylight savings.
191748	AOS6900 (Virtual Chassis) rebooted automatically, analysis required.
191901	OS10k switch crashed with generating PMD file.
191995	AOS6900 rebooted automatically, analysis required.
192184	Ni 8 crashed with PMD files
192210	linkAggCmm main info(5) Wrong index number 1 message seen in swlogs
192308	OS6900: TCP port 179 display issue.
192432	bcmd rpcs alert message: +++ slnHwlrnCbkHandler:657 no buffer ALERT!! Error.
192493	OS6900 - Incorrect DDM display when port is admin down
192556	App-fingerprint issue with OS6900 chassis with UNP configuration.
192561	During ISSU upgrade 10K-VC LACP port remains up for few sec while switch starts rebooting, which is
192570	Mexican timezone cannot be configured correctly
192741	SMSyncUpdateCMMVer1: 4/0 oper status change from 4 to 0 messages are logging in swlogs.
192774	Specific VLAN config removed from OS6900 chassis using "diff" and "cp" commands.
192814	Incorrect route got stuck in hardware
192836	OS6900: ARP replies seen on ports which are not tagged for the vlan.

192874	Ref PR# 191901: Wrong socket structure makes infinite loop of flush events from stpNi to SlNi
192901	OS10k NI 1 parking issue due to core.bcmd dump in niX/pmd/work
192932	SPB counters are not correct for ingress traffic for local SPB port
193177	AOS 6900 crashes with PMD when AAA is configured.
193228	In 6900 ChassisSupervisor Power Mgr alert message: PS 1 reported down error
193263	BGP route-map goes into a loop on "show" command
193317	[TYPE1] Clearing a BGP neighbor changes the configuration status
193385	The switch logs IPv6 OSPF hello packets received on a passive interface as errors
193657	In 6900 VC to code 7.3.2.469.R01, we still see MAC address learned from port 2/1/10 having one link
193883	OS10k specific static routes not installed at Ni level
193908	In 6900SES CMD alarm(1) CLI log trigger for any configuration change via MIP_gateway in swlog events
194216	OS6900 Source address of syslog process is missing
194265	Tx Lost frames increasing on the VFL links of OS6900 VC after the reload of switches.
194274	OS10k - need to increase the maximum number of sessions allowed for NTP clients
194452	Unable to set SLB hashing to SRC-IP for SLB.
194460	show LACP port range seeing internal error
194737	Slave chassis in the VC reloaded, without generating any PMD file.
194902	VC reloaded when policy based port mirroring is configured.
195008	Chassis 2 of virtual chassis goes to "failure-shutdown" state once VFL came back on.
195020	IPRM NHS triggers are not sendin all of the existing routes to BGP (OSPF route wasn't sent)
195083	OpenSSL vulnerablity CVE-2014-0224 and CVE-2014-0160
195220	OS10K network instability issue.
195324	Links flaps seen on 10Gig BEB switches in SPB in environment
195579	no-cache cannot be configured with DSCP, TOS or L2-priority
195810	Unable to set lacp system priority > 255 while configuring it on the port.
195978	Dynamic routes learned via ospf missing after Issu upgrade
196007	OS6900 OSPF point-to-point neighboring issue.
196470	Port mirroring not working on master chassis after failover.
196817	vm_insert_page error inserting new egress buff
197093	Parsing error message when changing sFlow receiver port number
197118	The "show ip ospf lsdb" always shows full lsdb, even when specific parameters are used.
197201	The "^" character shifted incase of incorrect command
197323	OS6900 rebooted with generating the PMD for ipmsni and lldpNi and vlan stacking issue is seen after
197364	OS6900-T20: Virtual-Chassis not working on XNI-U12E VFL ports.
197515	sflow packets are duplicated in the sampled data path
197581	On releasing Sflow receiver, BCM port sampling rate is not reset
197661	OS6900: tx loss frames on SPB interface ports
197694	OS6900: *** buffer overflow detected ***: /bin/etherCmm terminated.

197698	Traffic is getting dropped during the VC takeover
197720	ChassisSupervisor memMgr alert Not Supported The top 20 memory hogs in Not Supported are ....
197844	SSH vulnerability/vulnerabilities for 10K
198108	MIB for retrieving the UNP information is not available to display in the unp information in VM mana
198469	OS6900 we get the error message in swlog ipcmmd library(plApi) error(2) plGetIfIndexFromGport@1617 f
198494	Need OID for ?healthModuleCpuLatest? in 7.X code for OV2500.
198549	Implement TRAP/ SWLOG notification upon failure to add MAC due to TABLE FULL/ BUCKET FULL conditions
198831	6900 LACP not loaded
198914	Disply error message while configuring Rtr interface
199019	QoS Port not functioning correctly in OS6900
199391	OS6900-VC rebooted on 09-Oct-2014 and after a week Slave unit crashed with USB task.
199396	portmgrcmm library(plApi) error(2)
199508	E_Port Proxy Mode not working on OS6900.
199559	VFL-link shows up on the master and down the on SLave with only CMM-B
200025	VC of 10Ks dropping traffic crossing the VFL when using IGMP mode
200088	UNp information not displayed due to the issue in "alaDaMacVlanUserTable" mib.
200188	OS6900 VC FP_COUNTER parity errors and mac-learning issue.
200356	10K-VC :: unable to configure port-monitoring on a port while this port is up
200399	ERP Ring convergence is not happening properly among 4 nodes
200504	10K-VC :: vcsetup.cfg is missing on both CMM from Chassis-2 after reboot
200511	ISSU upgrade failed with OS6900 X40 with OS-XNI-U12 VFL uplink
200541	10K-VC :: Master is unable to provide information about new inserted CMM on Slave
200589	10K-VC: After inserting new CMM-A in Slave chassis "CI1", Master chassis crashed and Traffic losses
200847	IPRM not advertising the OSPF ECMP changes correctly to BGP.
201018	PGM controls packets dropped by the switch
201048	Unable to authenticate SSH using the TACACs server and PAM: pam_open_session(): Have exhausted maxim
201111	debug $(pidof vrrp) call vrrpIgnoreVrid(0,70)" command to ignore unwanted VRRP packets not active
201113	Not possible to disable the command "debug $(pidof vrrp) call vrrpIgnoreVrid(0,70)" at runtime.
201235	IP Traffic routing/forwarding done even after configuring the "no forward" for an IP Interface.
201280	OS6900: "modify running-directory" clarification
201678	multicast mac-address mismatch is reporting the wrong port
201876	Connectivity issue between switches when VLANs are mapped to MSTI 1.
201881	NTP Vulnerability query - CVE-2014-9293 CVE-2014-9294 CVE-2014-9295 CVE-2014-9296 CVE-2013-5211
201934	Creation of tagged RTR-PORT does not delete the default VLAN 1
201945	OS6900-VC ISSU failed with crash files for QOS task.
202046	NTPD Vulnerability: ntpd version 4.2.7 and pervious versions allow attackers to overflow several bu
202371	DTLS Vulnerability query - CVE-2014-3571 CVE-2015-0206
202466	Chassis 2 detached away from VC of 6. RCA needed.

202556	6900 switch up time resets to 0 after up time of 497.1 days without reboot.
202574	Multicast routing packets with TTL=0 or 1 is being forwarded on the PIM enable interface.
202736	OS6900 linkflapping with network outage.
202815	OS6900 display issue in web view
202873	OS6900 switch crahed due to SaaCMM task
202896	OS6900 issue with qos policy for TCP traffic
202995	NTP configuration is not getting applied
203039	OS 10K NI 2 parity errors, rebooted. Crashed and not up.
203142	OS10K ISSU upgrade issue
203169	Switch Suddenly stopped sending out traps
203184	OSPF graceful restart not working properly during CMM Takeover
203275	OS10k Switch got crashed after mounting the USB in the OS10k switch.
203344	Issue while configuring speed as 100Mbps on OS-XNI-T8 module connected on OS6900VC.
203354	Getting vcboot.cfg.err file after the reboot when "usb enable" is configured.
203380	Logs appeared after re-set the uptime "ChassisSupervisor CS Main info(5) CSP_SetChassisMode mode 2 -
203384	Getting the error message "plGetChassisSlotPortFromIfIndex@1302"
203394	ChassisSupervisor SharedMem Sync info(5) messages continously logged in swlog of OS6900 VC
203404	interface information not updated in kernal if emp address is on the same subnet of vlan interface
203600	VC is not reachable via 0.0.0.0/0 route in case EMP is down
203666	OS6900 issues with FCOE E-tunnel mode. Reference PR# 199508
203735	+++ iprmIntfEnable: Failed to find IPv4 interface 4118EMP
203768	Master Switch reloaded of VC went to Shutdown mode
203835	IP interface DOWN and BFD session associated with this interface UP
203842	EMP routes down after removing an EMP interface
203849	VC takeover allowed before VC goes into L8
203980	Incorrect error message when setting autoneg on T8 NI
204114	The command "show ip bgp policy prefix-list" fails to display the output once in every 3 times.
204152	Default route is preferred instead for black hole ip static route
204189	OS6900 T model having issue in USB management.
204256	6900 VC-3;40G VFL;;6900X40+U6/6900X20+U3/6900T20+U3;; DUT3 crashed w/msg “Oops: Kernel access of bad area, sig: 11 [#1]” after vc-takeover between DUT1/DUT2.
204272	OS6900-VC: Master-Chassis-1 crashed with bcmd task.
204282	OS6900 VRRP Dual Master Issue.
204463	An out prefix list for BGP doesn't filter any prefixes
204531	ARP Poison not working in OS 10K
204583	OSPF adjacencies down after a VC takeover in case BFD is enabled
204685	Slave unit in a VC trying to establish TCP connection to the BGP neighbour
204786	Route leaking issue layer 3 VPN SPB.

204834	Impact analysis on our products with CVE-2015-0291 t1_lib.c in OpenSSL 1.0.2.
204883	STP for linkagg ports in blocking state in hardware after the ports are disconnected and reconnected
204937	OS10K: Issue with power slot.
205145	Daylight saving needs to be disabled for MKS (MOSCOW) time.
205211	linkQual:POOR error message seen in logs. however its difficult to interpret which port is having th
205295	show powersupply error in 10K VC.
205472	SES AAA error(2) ...while communicating with AAA at 127.2.65.1:21288
205498	4XOS6900: Chassis 2 in VC was crashed
205685	NTP client is not using the source IP address configured using IP Managed Services
205749	Need analysis for the NI crash on OS10K
205825	portmgrcmm library(plApi) error(2) Error messages on OS6900 after upgrade to 7.3.4.450R01
206683	Duplicate VLAN stacking entries in boot.cfg of OS6900 7.3.4.450.R01
206776	Switch crashed due to IPRM task
206903	OS6900-OS6900 NTP server status rejected and no update on status.
207117	OS6900 reboot - Demo license wrongly getting applied on OS6900/OS10K switches when upgraded to 7.3.4
207436	LACP frames are not traversing VFL in Ethernet-Services
207508	[6900 VC, NLB] Traffic to VIP comming from different VRF than default, is dropped by the VFL
208006	MIBWALK on ifStackStatus creates portmgrcmm library(plApi) error(2)
208300	stpCmm _TRPt debug1(6) TRAP:newRoot stp=0 upon inactive linkagg config