Release Notes – Rev. D

OmniSwitch 6465, 6560, 6860(E)/6865/6900/9900

Release 8.5R4

These release notes accompany release 8.5R4. 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.

Alcatel-Lucent Enterprise

Contents

Related Documentation

These release notes should be used in conjunction with OmniSwitch AOS Release 8 User Guides. The following are the titles of the user guides that apply to this release.

- OmniSwitch 6465 Hardware User Guide
- OmniSwitch 6900 Hardware User Guide
- OmniSwitch 6560 Hardware User Guide
- OmniSwitch 6860(E) Hardware User Guide
- OmniSwitch 6865 Hardware User Guide
- OmniSwitch 9900 Hardware User Guide
- OmniSwitch AOS Release 8 CLI Reference Guide
- OmniSwitch AOS Release 8 Network Configuration Guide
- OmniSwitch AOS Release 8 Switch Management Guide
- OmniSwitch AOS Release 8 Advanced Routing Configuration Guide
- OmniSwitch AOS Release 8 Data Center Switching Guide
- OmniSwitch AOS Release 8 Specifications Guide
- OmniSwitch AOS Release 8 Transceivers Guide

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
OS6465	1GB	1GB
OS6560	2GB	2GB
OS6560-24X4/P24X4	1GB	1GB
OS6860(E)	2GB	2GB
OS6865	2GB	2GB
OS6900-X Models	2GB	2GB
OS6900-T Models	4GB	2GB
OS6900-Q32	8GB	2GB
OS6900-X72	8GB	4GB
OS6900-V72/C32	16GB	16GB
OS9900	16GB	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 this AOS release software 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.

OmniSwitch 6465 – AOS Release 8.5.196.R04(GA)

Hardware	Minimum UBoot	Minimum FPGA
OS6465-P6	8.5.83.R01	0.10
OS6465-P12	8.5.83.R01	0.10
OS6465-P28	8.5.89.R02	0.5

OmniSwitch 6560 – AOS Release 8.5.196.R04(GA)

Hardware	Minimum Uboot	Minimum FPGA
OS6560-24Z24	8.5.22.R01	0.7
OS6560-P24Z24	8.4.1.23.R02	0.6 (Minimum) 0.7 (Current)*

Hardware	Minimum Uboot	Minimum FPGA
OS6560-24Z8	8.5.22.R01	0.7
OS6560-P24Z8	8.4.1.23.R02	0.6 (Minimum) 0.7 (Current)*
OS6560-24X4	8.5.89.R02	0.4
OS6560-P24X4	8.5.89.R02	0.4
OS6560-P48Z16 (903954-90)	8.4.1.23.R02	0.6 (Minimum) 0.7 (Current)*
OS6560-P48Z16 (904044-90)	8.5.97.R04	0.3
OS6560-48X4	8.5.97.R04	0.4
OS6560-P48X4	8.5.97.R04	0.4
OS6560-X10	8.5.97.R04	0.5
***Note**: FPGA version 0.7 is only required to address issue CRAOS8X-7207.		

OmniSwitch 6860(E) – AOS Release 8.5.196.R04(GA)

Hardware	Minimum Uboot	Minimum FPGA
OS6860/OS6860E (except U28)	8.1.1.70.R01	0.9 (0x9)
OS6860E-U28	8.1.1.70.R01	0.20 (0x14)
OS6860E-P24Z8	8.4.1.17.R01	0.5 (0x5)

OmniSwitch 6865 – AOS Release 8.5.196.R04(GA)

Hardware	Minimum Uboot	Minimum FPGA*
OS6865-P16X	8.3.1.125.R01	0.20 (0x14) (minimum) 0.22 (0x16) (current)
OS6865-U12X	8.4.1.17.R01	0.23 (0x17)
OS6865-U28X	8.4.1.17.R01	0.11 (0xB) (minimum) 0.12 (0xC) (current)*
***Note**: FPGA version 0.12 is only required to address issue CRAOS8X-4150.		

OmniSwitch 6900-X20/X40 – AOS Release 8.5.196.R04(GA)

Hardware	Minimum UBoot	Minimum FPGA
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
All Expansion Modules	N/A	N/A

OmniSwitch 6900-T20/T40 – AOS Release 8.5.196.R04(GA)

Hardware	Minimum UBoot	Minimum FPGA
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
All Expansion Modules	N/A	N/A

OmniSwitch 6900-Q32 – AOS Release 8.5.196.R04(GA)

Hardware	Minimum UBoot	Minimum FPGA
CMM	7.3.4.277.R01	0.1.8
All Expansion Modules	N/A	N/A

OmniSwitch 6900-X72 – AOS Release 8.5.196.R04(GA)

Hardware	Minimum Uboot	Minimum FPGA
CMM	7.3.4.31.R02	0.1.10
All Expansion Modules	N/A	N/A

OmniSwitch 6900-V72/C32 – AOS Release 8.5.196.R04(GA)

Hardware	ONIE	CPLD
OS6900-V72	2017.08.00.01	CPLD 1 – 0x5 CPLD 2 - 0x6 CPLD 3 – 0x8
OS6900-C32	2016.08.00.03	CPLD 1 – 0xA CPLD 2 – 0xB CPLD 3 – 0xB
Note: The OS6900-V72/C32 uses a different image file (Yos.img) than all other OS6900 models (Tos.img). Be sure to use the appropriate image file for the platform.		

OmniSwitch 9900 – AOS Release 8.5.199.R04(GA)

Hardware	Coreboot-uboot	Control FPGA	Power FPGA
OS99-CMM	8.3.1.103.R01	2.3.0	0.8

Hardware	Coreboot-uboot	Control FPGA	Power FPGA
OS9907-CFM	8.3.1.103.R01	-	-
OS99-GNI-48	8.3.1.103.R01	1.2.4	0.9
OS99-GNI-P48	8.3.1.103.R01	1.2.4	0.9
OS99-XNI-48	8.3.1.103.R01	1.3.0	0.6
OS99-XNI-U48	8.3.1.103.R01	2.9.0	0.8
OS99-GNI-U48	8.4.1.166.R01	0.3.0	0.2
OS99-CNI-U8	8.4.1.20.R03	1.7	N/A
OS99-XNI-P48Z16	8.4.1.20.R03	1.4	0.6
OS99-XNI-U24	8.5.76.R04	1.0	0.8
OS99-XNI-P24Z8	8.5.76.R04	1.1	0.7

[IMPORTANT] *MUST READ*: AOS Release 8.5R4 Prerequisites and Deployment Information

General Information

- Note: Early availability features are available in AOS and can be configured. However, they have not gone through the complete AOS validation cycle and are therefore not officially supported.

- Please refer to the Feature Matrix in Appendix A for detailed information on supported features for each platform.

- Prior to upgrading please refer to Appendix C for important best practices, prerequisites, and step-by-step instructions.

- Some switches that ship from the factory will default to VC mode (requiring a vcboot.cfg configuration file) and attempt to run the automatic VC, automatic remote configuration, and automatic fabric protocols. Please note that since the switches default to VC mode, automatic remote configuration does not support the downloading of a 'boot.cfg' file, only the 'vcboot.cfg' file is supported.

- Some switches may ship from the factory with a diag.img file. This file is for internal switch diagnostic purposes only and can be safely removed.

Note: None of the ports on the OS6865 or OS6465 models default to auto-vfl so automatic VC will not run by default on newly shipped switches. However, automatic remote configuration and automatic fabric will run by default. The OS9900 does not support automatic VC mode, only static VC mode is supported.

- Switches that ship from the factory will have the *Running Configuration* set to the **/flash/working** directory upon the first boot up. By default, the automatic VC feature will run and the vcboot.cfg and vcsetup.cfg files will be created in the **/flash/working** directory but not in the **/flash/certified** directory which results in the *Running Configuration* not being certified. This will result in the *Running Configuration* being set to the **/flash/certified** directory on the next reboot. Additionally, on the next reboot the switch will no longer be in the factory default mode and will have a chassis-id of 1 which could cause a duplicate chassis-id issue if the switch is part of a VC. To set the switch back to the factory defaults on the next reboot perform the following:

```
-> rm /flash/working/vcboot.cfg
-> rm /flash/working/vcsetup.cfg
-> rm /flash/certified/vcboot.cfg
-> rm /flash/certified/vcsetup.cfg
```

- The OS6560-P48Z16 (903954-90) supports link aggregation only on the 1G/2.5G multigig and 10G ports (33-52). The 1G ports (ports 1-32) do not support link aggregation (CRAOSX-1766). Linkagg configuration on unsupported ports in 85R1/841R03 config file will be removed internally from software during upgrade reboot to 8.5R4.

  Note: OS6560-P48Z16 (904044-90) - This is a new version of the OS6560-P48Z16 which does not have the link aggregation limitation mentioned above. The model number (OS6560-P48Z16) remains the same for both versions, only the part number can be used to differentiate between the versions.

- The OS6560 supports a maximum of 384 user policies beginning in 8.5R3. If more than 384 policies are configured, the number should be reduced prior to upgrading.

- Improved Convergence Performance
  Faster convergence times can be achieved on the following models with SFP, SFP+, QSFP+, and QSFP28 ports with fiber transceivers.

  Exceptions:
  - Copper ports or ports with copper transceivers do not support faster convergence.
  - OS6865-P16X and OS6865-U12X ports 3 and 4 do not support faster convergence.
  - VFL ports do not support faster convergence.
  - Splitter ports (i.e. 4X10G or 4X25G) do not support faster convergence.

- VRRP Configuration Changes
  Beginning in 8.5R2, the procedure for configuring VRRP has changed from a VLAN based configuration to an IP interface based configuration. Existing VLAN based configurations will be automatically converted to the new CLI format shown below:
  (old) -> vrrp *vrid vlan*
  (new) -> ip vrrp *vrid* interface *ip-interface*

  Additionally, VRRP-MIB and ALCATEL-IND1-VRRP3-MIB use the VLAN-ID in the MIB's ifIndex while ALCATEL-IND1-VRRP and VRRPV3-MIB use an interface index. VRRP-MIB and ALCATEL-IND1-VRRP3-MIB are currently supported but will be deprecated in an upcoming release due to the new VRRP IP interface based implementation.

- Feature Support Removed
  EVB - Beginning in 8.5R4, support for EVB is being removed. Any switches with an EVB configuration cannot be upgraded to 8.5R4.

Licensed Features

The table below lists the licensed features in this release and whether or not a license is required for the various models.

	Data Center License Installation Required?
	OmniSwitch 6900
Data Center Features	
DCB (PFC,ETS,DCBx)	Yes
FIP Snooping	Yes
FCoE VXLAN	Yes
Note: All other platforms do not support Data Center features.	

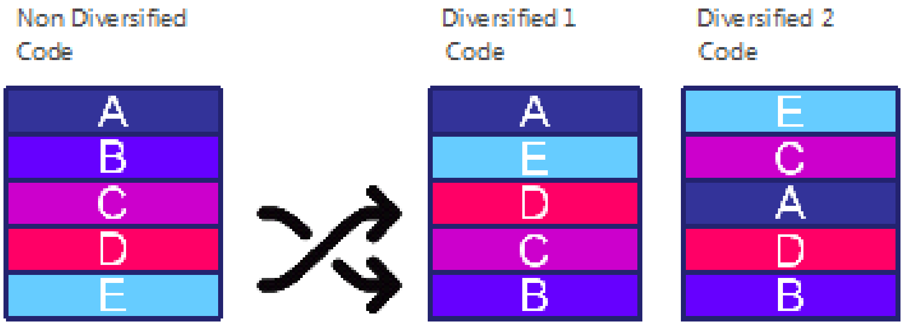
CodeGuardian

Alcatel-Lucent Enterprise and LGS Innovations have combined to provide the first network equipment to be hardened by an independent group. CodeGuardian promotes security and assurance at the network device level using independent verification and validation of source code, software diversification to prevent exploitation and secure delivery of software to customers.

CodeGuardian employs multiple techniques to identify vulnerabilities such as software architecture reviews, source code analysis (using both manual techniques and automated tools), vulnerability scanning tools and techniques, as well as analysis of known vulnerabilities in third party code.

Software diversification

Software diversification randomizes the executable program so that various instances of the same software, while functionally identical, are arranged differently. The CodeGuardian solution rearranges internal software while maintaining the same functionality and performance and modifies the deliverable application to limit or prevent/impede software exploitation. There will be up to 3 different diversified versions per GA release of code.



CodeGuardian AOS Releases

Standard AOS Releases	AOS CodeGuardian Release	LGS AOS CodeGuardian Release
AOS 8.5.R04	AOS 8.5.RX4	AOS 8.5.LX4

- X=Diversified image 1-3
- ALE will have 3 different diversified images per AOS release (R12 through R32)
- Our partner LGS will have 3 different diversified images per AOS release (L12 through L32)

Please contact customer support for additional information.

New / Updated Hardware Support

The following new hardware is being introduced in this release.

OmniSwitch 6560-48X4
Fixed configuration chassis in a 1U form factor with:

- Forty-eight (48) - 10/100/1000 BaseT ports
- Two (2) - SFP 1G ports
- Two (2) - SFP+ 1G/10G ports
- Two (2) - SFP+ (10G) ports
- USB port
- RJ-45 console port

OmniSwitch 6560-P48X4
Fixed configuration chassis in a 1U form factor with:

- Forty-eight (48) - 10/100/1000 BaseT 802.3at PoE ports
- Two (2) - SFP 1G ports
- Two (2) - SFP+ 1G/10G ports
- Two (2) - SFP+ (10G) ports
- USB port
- RJ-45 console port

OmniSwitch 6560-X10
Fixed configuration chassis in a 1U form factor with:

- Eight (8) - SFP+ (1G/10G) ports
- Two (2) – QSFP+ VFL ports
- USB port
- RJ-45 console port

OmniSwitch 6560-P48Z16
New version of OS6560-P48Z16 with additional feature support.

- OS6560-P48Z16 (903954-90) - Current version.
- OS6560-P48Z16 (904044-90) - New version.
    - Removes link aggregation limitation mentioned in prerequisites section.
    - Adds support for MACsec. (See MACsec feature description).
    - Adds support for L2 GRE Tunnel Access.

OS6560-BP-PH

A new version of the OmniSwitch 6560 600W AC power supply is being released in 8.5R4. The model number (OS6560-BP-PH) remains the same for both versions, only the part number can be used to differentiate between the versions. See table below for platform support.

- OS6560-BP-PH (903852-90) - Current version.
- OS6560-BP-PH (904071-90) - New version.

	OS6560-P24Z8	**OS6560-P24Z24**	**OS6560-P24X4**	**OS6560-P48X4 (New in 8.5R4)**	**OS6560-P48Z16 (903954-90)**	**OS6560-P48Z16 (904044-90) (New in 8.5R4)**
OS6560-BP-PH (903852-90)	Supported	Supported	Supported	Not Supported	Supported	Not Supported
OS6560-BP-PH (904071-90)	Supported	Supported	Supported	Supported	Supported	Supported

OS99-XNI-U24

OmniSwitch 9900 module with:

- Twenty-four (24) - SFP+ (1G/10G) ports

OS99-XNI-P24Z8

OmniSwitch 9900 module with:

- Eight (8) – 1/2.5/5/10G BaseT 802.3at PoE ports
- Sixteen (16) – 1/10G BaseT 802.3at PoE ports

QSFP-4X25G-C1M/3M/5M

Supported on the OS6900-V72, OS6900-C32.

OmniSwitch 6900 and OmniSwitch 9900 Auto-Negotiation Settings (40G/100G DAC Cables)

	40G Direct-Attached Cable	**100G Direct-Attached Cable**
OS6900-X Models	Auto-negotiation not supported.	N/A
OS6900-V72/C32	Auto-negotiation supported. (Default: Disabled)	Auto-negotiation supported. (Default: Enabled)
OS9900	Auto-negotiation supported. (Default: Disabled)	Auto-negotiation supported. (Default: Enabled)
Note: When connecting direct-attached cables between two OS99-CMMs it is recommended to enable auto-negotiation, including when being used as a VFL. If connecting an OS99-CMM to any other hardware, auto-negotiation should be disabled.		

New Software Features and Enhancements

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

8.5R4 New Feature/Enhancements Summary

Feature	Platform
IPv6 - DHCPv6 Snooping Support - (Support added in 8.5R3)	6860
IPv6 – IP Source Filtering (ISF) - (Support added in 8.5R3)	6860
VxLAN Support (Head-end mode only) - (Support added in 8.5R3)	OS6900-V72/C32
PIM over SPB - (Support added in 8.5R3)	9900
DHCP Relay Over Services - (Support added in 8.5R3)	9900
Multiple MAC Range Support - (Support added in 8.5R3)	6900
UNP Access Mode (SPB/VXLAN) support for Silent Devices. (static profile)	6860, 6865, 6900, 9900
Role based authentication across routed domains	6860, 6865, 6900 (except V72/C32), 9900
SPB: Inband management over services	6860, 6865, 6900, 9900
GTTS Enhancement - L2 GRE	6560, 6860, 6865, 6900, 9900
IPv6 L3VPN on 9900	9900
Tandem mode support on SPB mcast optmization in 9900	9900
SPB Convergence with HW Based LSP flooding in 9900	9900
OV Cirrus Enhancements: - Troubleshooting Enhancements - Configurable NAS IP Address - Default Admin Password Change - OS6900-C32/V72 Managed	6465, 6560, 6860, 6865, 6900, 9900
Upgrade NTP package to latest version	6465, 6560, 6860, 6865, 6900, 9900
STP TCN Dampening/Duplicate Handling	6465, 6560, 6860, 6865, 6900, 9900
Support of RFC-2868	6465, 6560, 6860, 6865, 6900, 9900
MACsec support on 6560	6560
Increase router interfaces on 6465 - (Support added in 8.5R3)	6465

Feature	Platform
ISF scalability enhancement (RTR-5181)	6560
TCAM Scalability for (RTR-5435)	6900-V72/C32
OSPF Scalability (RTR-5436)	9900
Apple Netboot Support with DHCP Snooping or Relay	6465, 6560, 6860, 6865, 6900, 9900

IPv6 - DHCPv6 Snooping Support - (Support added in 8.5R3)

DHCPv6 Snooping monitors DHCPv6 client/server exchanges passing through the switch. It builds a binding table database of DHCPv6-assigned addresses based on the contents of those exchanges. The binding table may be used by IPv6 Source Filtering to prevent unauthorized hosts from sending data via the switch.

When DHCPv6 Snooping is enabled at the switch level, all DHCPv6 packets received on all switch ports and link aggregates are screened/filtered by DHCPv6 Snooping.

When DHCPv6 snooping is enabled at the VLAN level, DHCPv6 Snooping functionality is only applied to ports that are associated with a VLAN that has this feature enabled.

IPv6 – IP Source Filtering (ISF) - (Support added in 8.5R3)

IPv6 source filtering uses the DHCPv6 snooping binding table information to protect the network from spoofing attacks. The binding table information is built by DHCPv6 snooping which monitors DHCPv6 client/server exchanges.

IPv6 source filtering applies to DHCPv6 Snooping ports, link aggregates, and VLANs and restricts port traffic to only packets that contain the client source MAC address, IPv6 address, and VLAN combination. The DHCPv6 Snooping binding table is used to verify the client information for the port/VLAN that is enabled for IPv6 source filtering. IPv6 source filtering can be enabled either on per-VLAN or per-port/link agg.

VXLAN Support – Head-end Mode Only - (Support added in 8.5R3)

VXLAN is now supported on an OmniSwitch 6900-V72/C32.

PIM Over SPB - (Support added in 8.5R3)

In addition to inline routing of unicast IP over SPB, inline routing of PIM over SPB is also supported. If the IP interface on which PIM is enabled is bound to an SPB service, then PIM can operate over an SPB L3 VPN in-line routing configuration (Inline routing supported only on the OmniSwitch 9900).

DHCP Relay Over Services - (Support added in 8.5R3)

DHCP Relay enables routing of DHCP traffic between clients and servers that are in different VLAN domains.

To enable routing of DHCP traffic between clients and servers across service domains, it is now possible to configure a DHCP relay agent for an IP interface that is bound to a Shortest Path Bridging (SPB) service. This is supported only on an OmniSwitch 9900.

Multiple MAC Range - (Support added in 8.5R3)

The LPS MAC range allows to restrict the source learning of the host MAC addresses. The MAC range command supported only one MAC range configuration. In this release AOS enhances the capability to configure up to eight MAC ranges per port. The multiple MAC ranges can be configured using the port-security mac-range CLI command.

ERP Support - (Support added in 8.5R3)

This release adds support for ERP on the OmniSwitch 9900.

Increase router interfaces on 6465 - (Support added in 8.5R3)

IPv4 interface and static route scalability numbers are increased to 24 and 32 respectively from 8.5R3 onwards.

UNP Access Mode (SPB/VXLAN) Support for Silent Devices

Allows for the configuration of a static SAP on aport that does not age out and continues to receive broadcast/multicast packets coming in on the service even if there are no MACs learned on the service.

Also adds an enhancement to existing support for silent devices in UNP Bridge Mode. Previously, bridge mode had support for configuring only untagged VLANs on UNP port or linkagg template. This enhancement allows for configuring tagged VLANs.

Role-based Authentication Across Routed Domains

This feature can be used to authenticate IPv4 users when trying to access certain secure IPv4 destination networks. This can be used for granting access to authorized administrators in IOT networks on routed domains where end user MAC addresses wouldn't be available. The user traffic accessing the secure network can be either HTTP-based or IPV4-based. The users sending HTTP-based traffic are challenged using Captive-Portal authentication, whereas users sending IP-based traffic access would undergo IP address based authentication to either allow or deny access.

SPB Inband Management Over Services

In previous releases an IP interface was not permitted on a BVLAN. With this feature enhancement an IPv4 management interface can now be configured on a control BVLAN to provide in-band management access in the SPBM domain. ISIS-SPB is the only protocol supported on this interface, no dynamic routing protols are supported.

L2 GRE (GTTS) Enhancement

L2 GRE is now supported without the need for a loopback port for routing from service domain into vlan domain. An IP interface can be associated with an L2 GRE service.

IPv6 L3 VPN over SPB on OS9900

IPv6 is now supported on an SPB L3 VPN service-based (inline routing) interface.

Tandem Mode Support on SPB Multicast Optimization on OS9900

Previously only head-end mode was supported for multicast over SPB. Tandem mode is now supported.

SPB Convergence with Hardware Based LSP Flooding on OS9900

Improves convergence by improving how LSP packets are handled in a ring topology.

OV Cirrus Enhancements

The following OV Cirrus enhancments are now available:

- Troubleshooting Enhancements - This is to facilitate troubleshooting of network devices by remote operators, even when a device fails to get managed by OV Cirrus. To enable remote troubleshooting, OV Cirrus operators will be provided with a user interface in Device Catalog application, and can choose one or more troubleshooting commands as well as be able to view logs. These commands are sent one by one to the device whenever the device tries to go through the Activation procedure.
- Configurable NAS IP Address - The RADIUS client can be configured include the NAS IP address attribute value in all the outgoing authentication and accounting packets. Configuring this option will allow the local NAS IP address to be included in the outgoing RADIUS packets which helps to clearly identify the source. In case of OV the VPN IP address value is included.
- Default Admin Password Change - In the process of getting an OmniSwitch managed by OmniVista, we now have the ability to change the default password of the admin user. This is useful to avoid the security threat of leaving the switch running with the default admin password. Password change will happen only when admin user has the default password.
- OV Cirrus agent can now manage the OS6900-C32/V72.

Upgrade NTP Package

The current NTP code is based on version 4.1.1. As part of this enhancement the NTP version is upgraded to version 4.2.8.p11. In this release, NTP supports burst/iburst mode of operation, enable Preempt mode and also specify the maximum polling interval for NTP messages.

Burst mode of operation improves timekeeping quality with the server command and iburst mode of operation is designed to speed the initial synchronization acquisition with the server command.

By enabling preempt, the specified server is marked unavailable for selection if any error (authentication failure) is detected on a connection between the local device and reference clock. The server is marked available for selection if no other connections are available and no error is detected on the connection between the local device and reference clock.

STP TCN Dampening / Duplicate Handling

A new parameter “Last TC Rcvd Bridge” has been added to the output of the 'show spantree' command to display the adjacent designated bridge ID from TC received along with Last TC Rcvd Port RSTP and MSTP protocols. The default value is ‘None’ and is supported only for RSTP and MSTP protocols. A new parameter “FW State” has been added to the output of “debug show spantree <instance> ports“. This counter indicates specific number of State transition to Forwarding State.

Support of RFC 2868 (RADIUS Attributes for Tunnel Protocol Support)

This feature provides a provision to set the precedence to filter ID or tunnel private group ID attributes for selection of UNP profile in the event of both these attributes being returned from the RADIUS server.

With this enhancement, it is possible for the switch to receives both “Filter-ID” and “Tunnel-Private-Group-ID” attributes together, in which case “UNP-Profile name” would be used from only one of these attributes, based on the configured precedence. The default precedence would still be to use ‘Filter ID’ RADIUS attribute.

MACsec Support on OS6560

This release extends support of MACsec on OS6560 models.

- OmniSwitch 6560-P24X4/24X4
    - Ports 1-24 (Static and Dynamic modes)
    - Ports 25-30 (Not Supported)
- OmniSwitch 6560-P48X4/48X4
    - Ports 1-32 (Static and Dynamic modes)
    - Ports 33-48 (Not Supported. See CRAOS8X-7910)
    - Ports 49-52 (Dynamic mode only)
    - Ports 53-54 (Not Supported)
- OmniSwitch 6560-P48Z16 (Part number 904044-90 only. Part number 903954-90 does not support MACsec)
    - Ports 1-32 (Static and Dynamic modes)
    - Ports 33-48 (Static and Dynamic modes)
    - Ports 49-52 (Dynamic mode only)
    - Ports 53-54 (Not Supported)
- OmniSwitch 6560-X10
    - Ports 1-8 (Dynamic mode only)
    - Ports 9-10 (Not Supported)

Applet Netboot Support with DHCP Snooping or Relay

AOS DHCP Snooping or Relay now supports Boot Server Discovery Protocol (BSDP) in the network when an OmniSwitch is an intermediate switch. A NetBoot 2.0 client uses the BSDP to dynamically acquire resources that enable it to boot a suitable operating system. The client uses DHCP to acquire its IP address and BSDP to acquire boot image resources. The protocols are initiated by the client at boot time.

AOS currently supports NetBoot 2.0 over DHCP Relay and Snooping.

Open Problem Reports and Feature Exceptions

The problems listed here include problems known at the time of the product’s release.

System / General / Display

CR	Description	Workaround
CRAOS8X-862	On an OS9900, Link Fault Propagation (LFP) link state is not maintained after NI reload. The 'show link-fault-propagation group' command output shows the wrong status after NI reload.	There is no known workaround at this time.
CRAOS8X-2102	The 'show spantree vlan <num>' command displays incorrect Designated Root Bridge information, after multiple VC-takeovers.	There is no known workaround at this time.
CRAOS8X-3204	On an OS6900-V72/C32 approximately 16K multicast sessions are able to be established instead of the 20K expected.	There is no known workaround at this time.
CRAOS8X-3368	On an OS6465, management traffic response time experiences slowness when CPU utilization is high.	There is no known workaround at this time.
CRAOS8X-3877	On 6900 and 6900-V72/C32, untagged packets are mirrored as tagged traffic when monitored port is across VC chassis. On standalone chassis, monitored egress traffic is tagged.	There is no known workaround at this time.
CRAOS8X-4247	mDNS packets are dropped if system location configured to 255 characters.	Configure the system location with a maximum of 206 characters.
CRAOS8X-6605	Sometimes remote port mirroring does not work after takeover.	There is no known workaround at this time.
CRAOS8X-7095	SNMP getbulk fails for alaServiceMgrPortProfileID.	There is no known workaround at this time.

Hardware

PR	Description	Workaround
CRAOS8X-2539	OS99-CNI-U8 doesn't support QSFP-4X25-C1M/3M/5M transceivers.	There is no known workaround at this time.
CRAOS8X-4367	On an OS99-XNI-U24 some ports may take several minutes to link up when powered up at -5C ambient. All link-up delay problems were observed on ports 10 - 16.	There is no known workaround at this time.
CRAOS8X-7926	SFP-10G-C1M/C3M cables are not supported on ports 1-8 of the OS6560-X10.	Use the SFP-10G-C7M cable.
CRAOS8X-8078	The router-auth users that are supposed to get deleted after the session timeout expiry of 5 minutes (300 seconds) are not getting deleted. This issue is specific to the OS9900 and for router-auth users only.	Use command 'unp router-auth user flush'
CRAOS8X-8427	On an OS9900 with a static linkagg of 4 ports using SFP-GIG-T transceivers (2 ports on 2 different OS99-XNI-U48 modules), hot-swapping the OS99-XNI-U48 causes traffic loss until the OS99-XNI-U48 is back up and running.	Use dynamic LACP link aggregation.
CRAOS8X-8428	On an OS9900 using an OS99-XNI-U48, replacing an SFP-10G-SR transceiver that is being used in a static linkagg, with an SFP-GIG-T copper transceiver generates CRC errors and no LED link indicator on the OS99-XNI-U48 even though the link is up.	Use the '**interfaces admin-state *disable/enable***' commands to disable the interface before replacing and enable the interface after replacing the transceiver.

MACsec

PR	Description	Workaround
CRAOS8X-5812	On an OS6860 with MACsec configured in dynamic mode, if the pre-shared keys are mismatched a 'drop-all' will not be enforced allowing traffic to pass.	Ensure the pre-shared keys are configured correctly.

CRAOS8X-7910	MACsec is not supported on ports 33 through 48 on an OS6560-48x4 or OS6560-P48X4.	There is no known workaround at this time. Issue to be fixed in AOS Release 8.6R1.

QoS

PR	Description	Workaround
CRAOS8X-434	Complete traffic drop is observed when traffic for non-spoofed IP is sent through userport enabled linkagg.	There is no known workaround at this time.
CRAOS8X-1082	When Rapid STP is enabled, after 2nd takeover, some of the QoS trusted ports are not assigned as Root Port and indicate as none.	There is no known workaround at this time.
CRAOS8X-2081	On an OS6560 10% of P7 traffic loss is seen when P0 traffic is oversubscribed with max Egress-bandwidth.	There is no known workaround at this time.
CRAOS8X-2927	A policy port group with split source ports fails after reload if two or more ports are on the same NI.	Disable and re-enable QoS.
CRAOS8X-3931	Traffic is not forwarded to cluster when SLB type l2 is configured in QoS policy condition.	There is no known workaround at this time.
CRAOS8X-4424	WRED is not supported in AOS Release 8.5R4 on any platforms.	There is no known workaround at this time.
CRAOS8X-4767	Sometimes the packet counter is not accurate on "show policy list rule". This is only a display issue with destination port policy condition.	There is no known workaround at this time.

Service Related

PR	Description	Workaround
CRAOS8X-2587	In VLAN domain, double tagged packet ingressing on a port will egress out as single tagged packet (original inner tag is removed).	There is no known workaround at this time.

CRAOS8X-4103	Traffic is not tunneled over L2GRE service when traffic is sent from Edge to GTTS via another Edge switch where links between two edges are configured as static linkagg.	There is no known workaround at this time.
CRAOS8X-4125	Traffic is not tunneled over L2GRE service When SAP port on one NI and SDP port on diffferent NI with multiple ECMP routes to reach far-end IP.	There is no known workaround at this time.
CRAOS8X-5051	One out of many SDPs associated with individual multicast groups sometimes does not come up.	There is no known workaround at this time.
CRAOS8X-5483	Not able to configure service creation CLI command specifying the range.	Create one service at a time using CLI command.
CRAOS8X-5354	User defined VxLAN UDP port for default VRF is currently not supported.	There is no known workaround at this time.
CRAOS8X-5855	Service related counters using the 'show service counters' command are not supported on an OS6900-V72 or OS6900-C32.	There is no known workaround at this time.
CRAOS8X-5985	In some cases on an OS6465 and OS6560, the CVLAN in a DHCP packet is not kept when the packet traverses the SVLAN. - DHCP packets on VLAN stacking with dhcp-snooping disabled - Supported. - DHCP packets on VLAN stacking with DHCP-snooping enabled - Not Supported - DHCP snooping option-82 CVLAN - Not supported.	There is no known workaround at this time.
CRAOS8X-6042	User may not be able to change VxLAN TTL value from Webview.	Use corresponding CLI command to change the value.
CRAOS8X-6088	UDP port config for VxLAN for non-default VRF may not be saved over	Configure VRF name containing alphanumeric value.

	reboot if the VRF name contains only numeric value.	
CRAOS8X-7428	IPMS Proxy is not supported on a service.	There is no known workaround at this time.

Virtual Chassis

PR	Description	Workaround
CRAOS8X-172	If a UDLD port is toggled on a slave chassis and then a takeover occurs, the UDLD link state may be undetermined instead of bi-directional if UDLD is configured in aggressive mode.	There is no known workaround at this time.
CRAOS8X-914	Sometimes after a VC-takeover, one of the users that was learned in blocking state on UNP access linkagg is getting flushed though the mac-aging timer has not expired.	There is no known workaround at this time.

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.

- When connecting or disconnecting a power supply to or from a chassis, the power supply must first be disconnected from the power source.
- For the OS6900-X40 wait for first module to become operational before adding the second module.
- All NI module extractions must have a 30 second interval before initiating another hot swap activity. CMM module extractions should have between a 15 and 20 minute interval.
- All new module insertions must have a 5 minute interval AND the LEDs (OK, PRI, VC, NI) have returned to their normal operating state.
- Any OS9900 CMM hotswap, NI hotswap, CMM takeover, NI reload or Chassis reload should be followed by performing a QoS Audit Procedure Status before any further actions.

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
OS99-CMM	OS99-CMM
OS9907-CFM	OS9907-CFM
OS99-GNI-48	OS99-GNI-48
OS99-GNI-P48	OS99-GNI-P48
OS99-XNI-48	OS99-XNI-48

OS99-XNI-U48	OS99-XNI-U48
OS99-XNI-P48Z16	OS99-XNI-P48Z16
OS99-CNI-U8	OS99-CNI-U8
OS99-GNI-U48	OS99-GNI-U48
OS99-XNI-U24	OS99-XNI-U24
OS99-XNI-P24Z8	OS99-XNI-P24Z8

OS9900 Hot Swap/Insertion Compatibility

Hot Swap Procedure

The following steps must be followed when hot-swapping 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. For a CMM wait approximately 15 to 20 minutes after insertion. On an OS9900 check the QoS Audit Procedure Status, see below.
5. Follow any messages that may displayed.
6. Re-insert all transceivers into the new module.
7. Re-connect all cables to transceivers.
8. Hot swap one CFM at a time. Please ensure all fan trays are always inserted and operational. CFM hot-swap should be completed with 120 seconds.

OmniSwitch 9900 - QoS Audit Procedure Status Completion Example

Run the following command on an OS9900 to ensure the QoS Audit has completed before performing another hot-swap activity on an OS9900. For each audit that has 'started' there must be an associated 'ended' as well as 'QOS Audit Procedure is now complete' message. The order will be different depending on the chassis configuration.

```
-> show log swlog | grep -i   "QOS audit"
2016 Sep 25 09:21:02.291 DC-CORE-01 swlogd qosCmm Config INFO: QOS Audit with local NI 1 started
2016 Sep 25 09:21:02.291 DC-CORE-01 swlogd qosCmm Config INFO: QOS Audit with local NI 3 started
2016 Sep 25 09:21:02.291 DC-CORE-01 swlogd qosCmm Config INFO: QOS Audit with local NI 4 started
2016 Sep 25 09:21:02.291 DC-CORE-01 swlogd qosCmm Config INFO: QOS Audit with local NI 5 started
2016 Sep 25 09:21:02.291 DC-CORE-01 swlogd qosCmm Config INFO: QOS Audit with local NI 6 started
2016 Sep 25 09:21:02.291 DC-CORE-01 swlogd qosCmm Config INFO: QOS Audit with local NI 7 started
2016 Sep 25 09:21:25.798 DC-CORE-01 swlogd qosCmm Config INFO: QOS Audit with local NI 6 ended
2016 Sep 25 09:21:26.097 DC-CORE-01 swlogd qosCmm Config INFO: QOS Audit with local NI 3 ended
2016 Sep 25 09:21:26.664 DC-CORE-01 swlogd qosCmm Config INFO: QOS Audit with local NI 1 ended
2016 Sep 25 09:21:28.700 DC-CORE-01 swlogd qosCmm Config INFO: QOS Audit with local NI 5 ended
2016 Sep 25 09:22:03.070 DC-CORE-01 swlogd qosCmm Config INFO: QOS Audit with local NI 4 ended
2016 Sep 25 09:22:05.611 DC-CORE-01 swlogd qosCmm Config INFO: QOS Audit with local NI 7 ended
2016 Sep 25 09:22:05.629 DC-CORE-01 swlogd qosCmm Config INFO: QOS Audit Procedure is now complete
2016 Sep 25 09:26:02.751 DC-CORE-01 swlogd qosCmm Config INFO: QOS Audit with local NI 2 started
2016 Sep 25 09:26:35.253 DC-CORE-01 swlogd qosCmm Config INFO: QOS Audit with local NI 2 ended
2016 Sep 25 09:26:35.275 DC-CORE-01 swlogd qosCmm Config INFO: QOS Audit Procedure is now complete
```

```
2016 Sep 25 09:27:34.400 DC-CORE-01 swlogd qosCmm Config INFO: QOS Audit(CMM) with peer chassisId 2 started
2016 Sep 25 09:27:43.635 DC-CORE-01 swlogd qosCmm Config INFO: QOS Audit with peer chassisId 2 ended
2016 Sep 25 09:27:43.653 DC-CORE-01 swlogd qosCmm Config INFO: QOS Audit Procedure is now complete
```

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: ebg_global_supportcenter@al-enterprise.com

Internet: Customers with service agreements may open cases 24 hours a day via the support web page at: businessportal2.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 hardware configuration, module types and version by slot, software version, 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**.

The Alcatel-Lucent name and logo are trademarks of Nokia used under license by ALE. To view other trademarks used by affiliated companies of ALE Holding, visit: www.al-enterprise.com/en/legal/trademarks-copyright. All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Neither ALE Holding nor any of its affiliates assumes any responsibility for inaccuracies contained herein.

Appendix A: Feature Matrix

The following is a feature matrix for AOS Release 8.5R4.

Note: Early availability features are available in AOS and can be configured. However, they have not gone through the complete AOS validation cycle and are therefore not officially supported.

Feature	6465	6560	6860(E)	6865	6900	6900-V72/C32	9900	Notes
Management Features								
Automatic Remote Configuration	8.5R1	Y	Y	Y	Y	N	Y	
Automatic/Intelligent Fabric	8.5R1	Y	Y	Y	Y	N	Y	
Automatic VC	N	Y	Y	Y	Y	N	N	
Bluetooth for Console Access	N	N	Y	N	N	N	N	
EEE support	N	N	Y	Y	Y	N	N	
Embedded Python Scripting / Event Manager	8.5R1	Y	Y	Y	Y	N	N	
IP Managed Services	N	N	Y	Y	Y	8.5R2	Y	
ISSU	N	N	Y	Y	Y	8.5R2	Y	
NAPALM Support	8.5R1	8.5R1	8.5R1	8.5R1	8.5R1	N	N	
NTP	8.5R1	Y	Y	Y	Y	8.5R2	Y	
OpenFlow	N	N	Y	N	Y	N	N	
OV Cirrus – Zero touch provisioning	Y	Y	Y	Y	Y	N	N	
Remote Chassis Detection (RCD)	N	N	N	N	Y	N	Y	
SAA	8.5R1	N	Y	Y	Y	N	N	
SNMP v1/v2/v3	8.5R1	Y	Y	Y	Y	8.5R2	Y	
UDLD	8.5R1	Y	Y	Y	Y	N	EA	
USB Disaster Recovery	8.5R1	Y	Y	Y	Y	N	Y	
USB Flash	8.5R1	Y	Y	Y	Y	N	N	
USB as Backup and Restore	8.5R1	8.5R1	8.5R1	8.5R1	N	N	Y	
USB – Encrypted	8.5R2	N	N	N	N	N	N	
Virtual Chassis (VC)	8.5R2	Y	Y	Y	Y	8.5R2 (VC of 2)	Y	V72/C32 cannot be mixed with other OS6900s and support static VFL only.
Virtual Chassis TCN	8.5R2	8.5R2	8.5R2	8.5R2	8.5R2	8.5R2	8.5R2	
Virtual Chassis Split Protection (VCSP)	N	Y	Y	Y	Y	8.5R2	Y	
VRF	N	N	Y	Y	Y	8.5R2	Y	

Feature	6465	6560	6860(E)	6865	6900	6900-V72/C32	9900	Notes
VRF – IPv6	N	N	Y	Y	Y	8.5R2	Y	
VRF – DHCP Client	N	N	Y	Y	Y	8.5R2	Y	
Web Services & CLI Scripting	8.5R1	Y	Y	Y	Y	N	Y	
Layer 3 Feature Support								
ARP	8.5R1	Y	Y	Y	Y	8.5R2	Y	
ARP - Distributed	N	N	N	N	Y	N	N	
ARP - Proxy	8.5R1	Y	Y	Y	Y	8.5R2	Y	
BFD	N	N	Y	Y	Y	8.5R2	Y	
BGP with graceful restart	N	N	Y	Y	Y	8.5R2	Y	
BGP route reflector for IPv6	N	N	Y	Y	Y	8.5R2	Y	
BGP ASPATH Filtering for IPv6 routes on IPv6 peering	N	N	Y	Y	Y	8.5R2	Y	
BGP support of MD5 password for IPv6	N	N	Y	Y	Y	8.5R2	Y	
BGP 4-Octet ASN Support	N	N	Y	Y	Y	8.5R2	Y	
DHCP Client / Server	EA-8.5R4	Y	Y	Y	Y	8.5R4	Y	
DHCP Relay	8.5R1	Y	Y	Y	Y	8.5R4	Y	
DHCPv6 Server	N	N	Y	Y	Y	EA	Y	
DHCPv6 Relay	8.5R1	Y	Y	Y	Y	EA - 8.5R4	Y	
DHCP Snooping / IP Source Filtering	8.5R4	Y	Y	Y	Y	N	Y	
ECMP	8.5R1	Y	Y	Y	Y	8.5R2	Y	
IGMP v1/v2/v3	8.5R1	Y	Y	Y	Y	8.5R2	Y	
GRE	N	N	Y	Y	Y	8.5R2	8.5R2	
IP-IP tunneling	N	N	Y	Y	Y	8.5R2	8.5R2	
IP routed port	8.5R1	Y	Y	Y	Y	8.5R2	Y	
IPv6	8.5R1	Y	Y	Y	Y	8.5R2	Y	
IPv6 - DHCPv6 Snooping / source filtering	N	N	8.5R3	8.5R4	N	N	N	
IPv6 - DHCP Guard	N	8.5R2	8.5R2	N	N	N	N	
IPv6 RA Guard (RA filter)	N	8.5R2	Y	Y	Y	N	N	
IPv6 DHCP relay and Neighbor discovery proxy	8.5R1	Y	Y	Y	Y	N	Y	
IP Multinetting	8.5R1	Y	Y	Y	Y	8.5R2	Y	
IPSec (IPv6)	N	N	Y	Y	Y	N	EA	
ISIS IPv4/IPv6	N	N	Y	Y	Y	8.5R2	8.5R2	
M-ISIS	N	N	Y	Y	Y	8.5R2	8.5R2	
OSPFv2	N	8.5R2	Y	Y	Y	8.5R2	Y	OS6560 (stub area only)
OSPFv3	N	N	Y	Y	Y	8.5R2	Y	

Feature	6465	6560	6860(E)	6865	6900	6900-V72/C32	9900	Notes
RIP v1/v2	8.5R1	Y	Y	Y	Y	8.5R2	Y	
RIPng	8.5R1	Y	Y	Y	Y	8.5R2	Y	
UDP Relay (IPv4)	8.5R4	8.5R4	Y	Y	Y	8.5R4	8.5R4	
UDP Relay (IPv6)	N	N	N	N	N	N	N	
VRRP v2	8.5R2	Y	Y	Y	Y	8.5R2	Y	
VRRP v3	8.5R2	Y	Y	Y	Y	8.5R2	Y	
Server Load Balancing (SLB)	N	N	Y	Y	Y	N	N	
Static routing	8.5R1	Y	Y	Y	Y	8.5R2	Y	
Multicast Features								
DVMRP	N	N	Y	Y	Y	8.5R2	N	
IPv4 Multicast Switching	8.5R1	Y	Y	Y	Y	8.5R2	Y	
Multicast *,G	Y	8.5R2	8.5R2	Y	Y	8.5R2	Y	
IPv6 Multicast Switching	8.5R1	Y	Y	Y	Y	8.5R2	Y	
PIM-DM	N	N	Y	Y	Y	8.5R2	Y	
PIM-SM	N	N	Y	Y	Y	8.5R2	Y	
PIM-SSM	N	N	Y	Y	Y	8.5R2	Y	
PIM-SSM Static Map	N	N	N	N	N	N	N	
PIM-BiDir	N	N	Y	Y	Y	8.5R2	Y	
Monitoring/Troubleshooting Features								
Ping and traceroute	8.5R1	Y	Y	Y	Y	8.5R2	Y	
Policy based mirroring	N	N	Y	Y	Y	EA	8.5R4	
Port mirroring	8.5R1	Y	Y	Y	Y	8.5R2	Y	
Port monitoring	8.5R1	Y	Y	Y	Y	8.5R2	Y	
Port mirroring - remote	8.5R1	Y	Y	Y	Y	EA	EA	
Port mirroring – remote over linkagg	N	N	Y	Y	Y	N	N	
RMON	8.5R1	Y	Y	Y	Y	N	N	
SFlow	8.5R1	Y	Y	Y	Y	EA	Y	
Switch logging / Syslog	8.5R1	Y	Y	Y	Y	8.5R2	Y	
TDR	N	N	Y	N	N	N	N	
Layer 2 Feature Support								
802.1q	8.5R1	Y	Y	Y	Y	8.5R2	Y	
DHL	8.5R1	Y	Y	Y	N	N	N	
ERP v2	8.5R1	8.5R2	Y	Y	Y	N	8.5R3	
HAVLAN	EA	N	Y	Y	Y	N	EA	
Link Aggregation (static and LACP)	8.5R1	Y	Y	Y	Y	8.5R2	Y	
LLDP (802.1ab)	8.5R1	Y	Y	Y	Y	8.5R2	Y	

Feature	6465	6560	6860(E)	6865	6900	6900-V72/C32	9900	Notes
Loopback detection – Edge (Bridge)	8.5R1	Y	Y	Y	N	N	Y	
Loopback detection – SAP (Access)	N	N	Y	Y	Y	N	EA	
Spanning Tree (1X1, RSTP, MSTP)	8.5R1	Y	Y	Y	Y	8.5R2	Y	
Spanning Tree (PVST+, Loop Guard)	N	N	Y	Y	Y	N	EA	
MVRP	8.5R1	Y	Y	Y	Y	8.5R4	Y	
Port mapping	Y	Y	Y	Y	Y	8.5R2	Y	
Private VLANs	N	N	Y	Y	Y	N	N	
SIP Snooping	N	N	Y	N	N	N	N	
SPB	N	N	Y	Y	Y	8.5R2	Y	See protocol table below.
SPB – HW-based LSP flooding	N	N	N	N	N	N	8.5R4	
QoS Feature Support								
802.1p / DSCP priority mapping	8.5R1	Y	Y	Y	Y	8.5R2	Y	
IPv4	8.5R1	Y	Y	Y	Y	8.5R2	Y	
IPv6	8.5R1	Y	Y	Y	Y	8.5R2	Y	
Auto-Qos prioritization of NMS/IP Phone Traffic	8.5R1	Y	Y	Y	Y	8.5R2	Y	
Auto-Qos – New MAC range	8.5R2	8.5R2	8.5R2	8.5R2	8.5R2	8.5R2	8.5R2	
Groups - Port	8.5R1	Y	Y	Y	Y	8.5R2	Y	
Groups - MAC	8.5R1	Y	Y	Y	Y	8.5R2	Y	
Groups - Network	8.5R1	Y	Y	Y	Y	8.5R2	Y	
Groups - Service	8.5R1	Y	Y	Y	Y	8.5R2	Y	
Groups - Map	8.5R1	Y	Y	Y	Y	8.5R2	Y	
Groups - Switch	8.5R1	Y	Y	Y	Y	8.5R2	Y	
Ingress/Egress bandwidth limit	8.5R1	Y	Y	Y	Y	8.5R2	Y	
Per port rate limiting	N	N	Y	Y	Y	8.5R2	N	
Policy Lists	8.5R1	Y	Y	Y	Y	N	Y	
Policy Lists - Egress	N	N	Y	Y	Y	N	N	
Policy based routing	N	N	Y	Y	Y	N	EA	
Tri-color marking	N	N	Y	Y	Y	N	N	
QSP Profiles 1	8.5R1	Y	Y	Y	Y	8.5R2	Y	
QSP Profiles 2/3/4	N	N	Y	Y	Y	N	N	
QSP Profiles 5	8.5R1	Y	N	N	N	N	Y	
Metro Ethernet Features								
Ethernet Services (VLAN Stacking)	8.5R1	N	Y	Y	Y	8.5R4	N	

Feature	6465	6560	6860(E)	6865	6900	6900-V72/C32	9900	Notes
Ethernet OAM (ITU Y1731 and 802.1ag)	8.5R1	N	Y	Y	Y	N	EA	
EFM-OAM (802.3ah)	N	N	8.5R4	8.5R4	N	N	N	
1588v2 End-to-End Transparent Clock	8.5R1	N	Y	Y	Y (X72/Q32)	N	N	
1588v2 Across VC	N	N	N	N	8.5R2 (X72)	N	N	
Security Features								
802.1x fail to MAC Authentication	8.5R2	Y	Y	Y	Y	N	Y	
Access Guardian – Bridge	8.5R1	Y	Y	Y	Y	N	Y	
Access Guardian - Access	N	N	Y	Y	Y	8.5R4	Y	
Application Fingerprinting	N	N	N	N	Y	N	N	
Application Monitoring and Enforcement (Appmon)	N	N	Y	N	N	N	N	
ARP Poisoning Protection	8.5R1	Y	Y	Y	Y	8.5R2	Y	
BYOD - COA Extension support for RADIUS	N	Y	Y	Y	N	N	Y	
BYOD - mDNS Snooping/Relay	N	Y	Y	Y	N	N	Y	
BYOD - UPNP/DLNA Relay	N	Y	Y	Y	N	N	Y	
BYOD - Switch Port location information pass-through in RADIUS requests	N	Y	Y	Y	N	N	Y	
Captive Portal	8.5R4	Y	Y	Y	N	N	Y	
IoT device profiling	8.5R2	8.5R2	8.5R2	8.5R2	8.5R2	N	8.5R2	
Directed broadcasts - Control	8.5R2	8.5R2	8.5R2	8.5R2	8.5R2	N	N	
Interface Violation Recovery	8.5R1	Y	Y	Y	Y	EA	Y	
L2 GRE Tunnel Access	N	Y	Y	Y	N	N	Y	
L2 GRE Tunnel Aggregation	N	N	Y	Y	Y	N	Y	OS6900-Q32/X72
Learned Port Security (LPS)	8.5R1	Y	Y	Y	Y	8.5R4	Y	
LPS – Multiple MAC Range	N	N	N	N	8.5R3	N	N	
LLDP	8.5R1	Y	Y	Y	Y	8.5R2	Y	
MACsec	8.5R1	8.5R4	Y	N	N	N	8.5R2	
MACsec MKA Support	8.5R2	8.5R4	8.5R2	N	N	N	8.5R2	
Quarantine Manager	N	N	Y	Y	N	N	N	
Radius test tool	8.5R1	Y	Y	Y	Y	N	Y	
Storm Control	N	N	Y	Y	Y	N	N	
TACACS+ Client	8.5R1	Y	Y	Y	Y	N	Y	
TACACS+ command based authorization	N	N	Y	Y	Y	N	N	
PoE Features								

Feature	**6465**	**6560**	**6860(E)**	**6865**	**6900**	**6900-V72/C32**	**9900**	**Notes**
802.1af and 802.3at	8.5R1	Y	Y	Y	N	N	Y	
Auto Negotiation of PoE Class-power upper limit	8.5R1	Y	Y	Y	N	N	Y	
Display of detected power class	8.5R1	Y	Y	Y	N	N	Y	
LLDP/802.3at power management TLV	8.5R1	Y	Y	Y	N	N	Y	
HPOE support	8.5R1 (60W)	Y (95W)	Y (60W)	Y (75W)	N	N	Y (75W)	
Time Of Day Support	8.5R1	Y	Y	Y	N	N	Y	
Data Center Features								
CEE DCBX Version 1.01	N	N	N	N	Y	N	N	
Data Center Bridging (DCBX/ETS/PFC)	N	N	N	N	Y	N	N	
EVB	N	N	N	N	N	N	N	
FCoE / FC Gateway	N	N	N	N	Y	N	N	
VXLAN	N	N	N	N	Q32/X72	8.5R3	N	L2 head-end only on V72/C32.
VM/VXLAN Snooping	N	N	N	N	Y	N	N	
FIP Snooping	N	N	N	N	Y	N	N	

Appendix B: SPB L3 VPN-Lite Service-based (Inline Routing) and Loopback Protocol Support

The OmniSwitch supports SPB L3 VPN-Lite using either service-based (inline routing) or external loopback. The table below summarizes the currently supported protocols for each method in this release.

	OmniSwitch 9900 (Inline)	OmniSwitch 9900 (loopback)	OmniSwitch 6860/6865 (loopback)	OmniSwitch 6900 (loopback)	OmniSwitch 6900 V72/C32 (loopback)
IPv4 Protocols					
Static Routing	Y	8.5R4	Y	Y	8.5R4
RIP v1/v2	Y	8.5R4	Y	Y	8.5R4
OSPF	Y	8.5R4	Y	Y	8.5R4
BGP	Y	8.5R4	Y	Y	8.5R4
VRRP	Y	N	8.5R4	Y	N
IS-IS	N	N	N	N	N
PIM-SM/DM	8.5R3	8.5R4	Y	Y	8.5R4
DHCP Relay	8.5R3	8.5R4	8.5R4	8.5R4	8.5R4
UDP Relay	8.5R4	8.5R4	8.5R4	8.5R4	8.5R4
DVMRP	N	N	N	N	N
BFD	N	N	N	N	N
IGMP Snooping	Y	8.5R4	Y	Y	N
IP Multicast Headend Mode	Y	8.5R4	Y	Y	N
IP Multicast Tandem Mode	8.5R4	8.5R4	Y	Y	N
IPv6 Protocols					
Static Routing	8.5R4	8.5R4	Y	Y	8.5R4
RIPng	8.5R4	8.5R4	Y	Y	8.5R4
OSPFv3	8.5R4	8.5R4	Y	Y	8.5R4
BGP	8.5R4	8.5R4	Y	Y	8.5R4
VRRPv3	8.5R4	8.5R4	8.5R4	Y	N
IS-IS	N	N	N	N	N
PIM-SM/DM	8.5R4	8.5R4	8.5R4	8.5R4	8.5R4
DHCP Relay	N	N	N	N	N
UDP Relay	N	N	N	N	N
DVMRP	N	N	N	N	N
BFD	N	N	N	N	N
IPv6 MLD Snooping	Y	8.5R4	Y	Y	N
IPv6 Multicast Headend Mode	Y	8.5R4	Y	Y	N
IPv6 Multicast Tandem Mode	8.5R4	8.5R4	Y	Y	N

Appendix C: 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 resulting in sub-second convergence 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).

Supported Upgrade Paths and Procedures

The following releases support upgrading using ISSU. All other releases support a Standard upgrade only.

Platform	AOS Releases Supporting ISSU to 8.5R4 (GA)
OS6465	8.5.164.R01 (GA) 8.5.255.R02 (GA) 8.5.54.R03 (GA)
OS6560	ISSU not supported in 8.5R4.
OS6860(E)	8.4.1.141.R03 (GA) 8.5.164.R01 (GA) 8.5.255.R02 (GA) 8.5.54.R03 (GA)
OS6865	8.4.1.141.R03 (GA) 8.5.164.R01 (GA) 8.5.255.R02 (GA)
OS6900	8.4.1.141.R03 (GA) 8.5.164.R01 (GA) 8.5.255.R02 (GA) 8.5.54.R03 (GA)
OS9900	8.4.1.229.R02 (GA) 8.4.1.141.R03 (GA) 8.5.255.R02 (GA) 8.5.54.R03 (GA) **Note:** ISSU on a VC of 1 OS9900 is only supported from 8.5R2 and above.
Note: For any switch with a multicast configuration ISSU is only supported from 8.4.1.R02 GA or MR. Earlier releases must use a standard upgrade.	

8.5R4 ISSU Supported Releases

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 8.4.1.229.R02 Service Release, September 05, 2017.,
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 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
```

Additionally, the '**show tech-support eng complete'** command will create a TAR file with multiple tech-support log files as well as the SWLOG files from the switches.

```
6900-> show tech-support eng complete
```

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.

- If upgrading a standalone chassis or VC using a standard upgrade procedure please refer to Appendix D for specific steps to follow.

- If upgrading a VC using ISSU please refer to Appendix E for specific steps to follow.

Appendix D: Standard Upgrade - OmniSwitch Standalone or Virtual Chassis

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

1. Download the Upgrade Files

Go to the Service and Support website and download and unzip the upgrade files for the appropriate model and release. The archives contain the following:

- OS6465 – Nos.img
- OS6560 – Uos.img (**Note**: If upgrading an OS6560-P24Z24/P48Z16 (903954-90)/P24Z8, upgrading the FPGA to version 0.7 may be required to address CRAOS8x-7207. AOS must be upgraded prior to upgrading the FPGA. See Appendix F.)
- OS6860 – Uos.img
- OS6865 – Uos.img (**Note**: If upgrading an OS6865-U28X, upgrading the FPGA to version 0.12 may be required to address CRAOS8X-4150. AOS must be upgraded prior to upgrading the FPGA. See Appendix F.)
- OS6900 **-** Tos.img (V72/C32 – Yos.img)
- OS9900 – Mos.img, Mhost.img, Meni.img
- imgsha256sum (not required) –This file is only required when running in Common Criteria mode. Please refer to the Common Criteria Operational Guidance Document for additional information.

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** command.

```
OS6900-> show microcode
/flash/working
Package           Release                  Size     Description
-----------------+-------------------------+--------+----------------------------------
```

```
Tos.img           8.5.196.R04           210697424 Alcatel-Lucent OS


6900-> 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

-> 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 E: ISSU – OmniSwitch Chassis or Virtual Chassis

These instructions document how to upgrade a modular chassis or virtual chassis using ISSU. Upgrading using ISSU consists of the following steps. The steps should be performed in order:

1. Download the Upgrade Files

Go to the Service and Support Website and download and unzip the ISSU upgrade files for the appropriate platform and release. The archive contains the following:

- OS6900 **-** Tos.img
- OS6860 – Uos.img
- OS6865 – Uos.img (**Note**: If upgrading an OS6865-U28X, upgrading the FPGA to version 0.12 may be required to address CRAOS8X-4150. AOS must be upgraded prior to upgrading the FPGA. See Appendix F.)
- OS6560 – Uos.img (ISSU not supported in this release)
- OS9900 – Mos.img, Mhost.img, Meni.img
- ISSU Version File – issu_version
- imgsha256sum (not required) –This file is only required when running in Common Criteria mode. Please refer to the Common Criteria Operational Guidance Document for additional information.

Note: The following examples use **issu_dir** as an example ISSU directory name. However, any directory name may be used. Additionally, if an ISSU upgrade was previously performed using a directory named **issu_dir**, it may now be the *Running Configuration*, in which case a different ISSU directory name should be used.

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 effect 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. Wait for the System ready or [L8] state which gets displayed in the ssh/telnet/console session before performing any write-memory or configuration changes.

```
6900-> debug show virtual-chassis topology
Local Chassis: 1
Oper                                        Config   Oper                      System
Chas  Role         Status              Chas ID  Pri   Group  MAC-Address        Ready
-----+------------+-------------------+--------+-----+------+------------------+-------
1     Master        Running             1        100   19     e8:e7:32:b9:19:0b  Yes
2     Slave         Running             2        99    19     e8:e7:32:b9:19:43  Yes
```

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** command**.**

```
OS6900-> show microcode
/flash/working
Package           Release                 Size     Description
-----------------+-------------------------+--------+-----------------------------------
Tos.img           8.5.196.R04
```

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

-> 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 F: FPGA Upgrade Procedure

- For issue CRAOS8X-7207 an FPGA upgrade may be required for the OS6560-P24Z24, OS6560-P48Z16 (903954-90 only), or the OS6560-P24Z8 models.
- For issue CRAOS8X-4150 an FPGA upgrade (0.12) may be required for the OS6865-U28X.

Note: AOS must be upgraded to 8.5R4 prior to performing an FPGA upgrade.

1. Download and extract the upgrade archive from the Service & Support website. In addition to the AOS images, the archive will also contain the following FPGA upgrade kit.

- CPLD File - fpga_kit_6002

2. FTP (Binary) the FPGA upgrade kit listed above to the **/flash** directory on the primary CMM.

3. Enter the following to upgrade the FPGA. The '**all**' parameter should be used when upgrading with an FPGA kit. Additionally, this will update all the elements of a VC.

```
-> update fpga-cpld cmm all file fpga_kit_6002
Parse /flash/fpga_kit_6002
Please wait...
fpga file: fpga_6560_v07.vme
update chassis 1
Starting CMM ALL FPGA Upgrade
CMM 1/1
Successfully updated
Reload required to activate new firmware.
```

Once complete, a reboot is required.

Appendix G: Fixed Problem Reports

The following problem reports were closed in this AOS Release.

PR	Summary
CRAOS8X-1208 TSref: 00292838	OS-9900 error logs enabling QoS.
CRAOS8X-1583 TSref: 00297325	Need RCA: master unit from the stack of 2*OS6900 not responding.
CRAOS8X-1684 TSref: 00298832	Crash svcCmm process after displaying show l2profile.
CRAOS8X-1995 TSref: 00298977	LED from card OS99-XNI-U48 is not working when Copper SFP is being used.
CRAOS8X-3236 TSref: 00314815	OS6900: VC of 4 running SPB: Reachability issue between server to Core.
CRAOS8X-3242 TSref: 00311869	OS6465-P12 no PoE after AC BP Powerless.
CRAOS8X-3322 TSref: 00315959	Over utilization bug in TCAM
CRAOS8X-3324 TSref: 00314014	2xOS6900VC crash RCA.
CRAOS8X-3991 TSref: 00319674	Need update with 7.1.3 OpenSSH 'sftp-server' Security Bypass Vulnerability ility (CVE-2017-15906).
CRAOS8X-4087 TSref: 00321427	OS9900 licMgr and FlashMgr Message - We are seeing the following messages on some of the OS9900 switches.
CRAOS8X-4170 TSref: 00318739	DHCP not working when DHCP Snooping & Port-Security is configured.
CRAOS8X-4197 TSref: 00325935	OS6860E CPU high when apply Application Visibility.
CRAOS8X-4262 TSref: N/A	Revert the PS LED Amber setting on input voltage falling below 52V.
CRAOS8X-4381 TSref: N/A	6900-X72 sends wrong physical Index within PowerSupply Trap.
CRAOS8X-4150 TSref: 00323763	Virtual chassis LED functionality has been changed in the latest update 8.5 release and there is no documentation for this change. Issue fixed with upgrade to FPGA version 0.12.
CRAOS8X-4637 TSref: 00332174	OS9900 Modules Reloaded Excepting for CMM-B.
CRAOS8X-4712 TSref: 00325538	DHCP packets dropped on GTTS switch.
CRAOS8X-4778/4779 TSref: 00317045	Random Port drops when using SFP-Gig-T.
CRAOS8X-4874 TSref: 00327155	Cannot change rtr-port MTU.
CRAOS8X-4913 TSref: 00313952	2xOS6560VC unp users “In progress” status.
CRAOS8X-4926 TSref: 00336187	Reload of slave chassis of an ospf router make the ospf neighborship being down during the time the slave is coming up.

CRAOS8X-4988 TSref: 00335557	Connectivity issue seen between a 6860 behind 9907 and any device connected behind linkagg 20 on the other side of 9907.
CRAOS8X-4999 TSref: 00327936	Issues in the Web interface.
CRAOS8X-5068 TSref: 00325110	Netsec Commands not loaded on 6865-u28x switch.
CRAOS8X-5101* TSref: 00335557	Connectivity issue seen between an OS6860 behind OS9907 and any device connected behind linkagg 20 on the other side of OS9907.
CRAOS8X-5165 TSref: 00337398	OS6900-X72 F-R Power Supply (P/No 903196-90) - show powersupply command reports Airflow Rear to Front instead of Front to Rear.
CRAOS8X-5232 TSref: 00322535	OS6865 DDM values being read from SFP are wrong.
CRAOS8X-5233 TSref: 00327799	6900-X72 sends wrong physical Index within PowerSupply Trap.
CRAOS8X-5255* TSref: 00313952	2XOS6560 VC UNP users "in progress" status.
CRAOS8X-5285* TSref: N/A	Logic to sync agcmmUnrepliedAuthReqCount with AAA context count.
CRAOS8X-5286 TSref: N/A	Logic to sync agcmmUnrepliedAuthReqCount with AAA context count.
CRAOS8X-5290 TSref: 00336187	Reload of slave chassis of an ospf router make the ospf neighborship being down during the time the slave is coming up.
CRAOS8X-5301 TSref: 00338392	Ports bloqués après une mise à jour vers 8.5R02.
CRAOS8X-5334 TSref: 00334482	OmniSwitch 6865-U28X shows having an EMP port but the hardware does not actually have an EMP port.
CRAOS8X-5351 TSref: 00334168	OS9900-VC: SQL traffic getting dropped on SPB Core switch.
CRAOS8X-5352 TSref: 00334168	OS9900-VC: SQL traffic getting dropped on SPB Core switch.
CRAOS8X-5366* TSref: 00338392	Centre Hospitalier Régional Universitaire de Lille (CHRU): ports bloqués après une mise à jour vers 8.5R02.
CRAOS8X-5393 TSref: 00340918	Trap generation issue between OS6865 & OV.
CRAOS8X-5403 TSref: 00325538	DHCP packets dropped on GTTS switch.
CRAOS8X-5404 TSref: 00336187	Reload of slave chassis of an ospf router make the ospf neighborship being down during the time the slave is coming up.
CRAOS8X-5413 TSref: 00298977	LED from card OS99-XNI-U48 is not working when Copper SFP is being used.
CRAOS8X-5486 TSref: 00341904	OS6860-Unable to login into secondary unit of the VC.
CRAOS8X-5517 TSref: 00340744	In PALM Operating System Release status is not displayed for switches in 8.5.255.R02.
CRAOS8X-5528* TSref: 00342960	Critical Request - Links missing between the devices in OV2500 due to Getbulk enabled.

CRAOS8X-5535* TSref: 00338392	Centre Hospitalier Régional Universitaire de Lille (CHRU): ports bloqués après une mise à jour vers 8.5R02.
CRAOS8X-5550 TSref: 00341682	OS6900-V72 No License Issue.
CRAOS8X-5577 TSref: 00343880	A CFM2 became defective in master chassis 1 and started to impact traffic depending on the hashing happening on the linkagg 20 of 9907. First no swlog message indicated CFM2 had a power failure issue, no trap sent and board info showed the CFM as OK.
CRAOS8X-5579 TSref: 00313316	Tunnel protocol attributes are not supported per RFC 2868 which is mentioned in the datasheet for OS6560.
CRAOS8X-5585 TSref: 00333147	OS6465-P12: Memory usage constantly increasing.
CRAOS8X-5589 TSref: 00333147	OS6465-P12: Memory usage constantly increasing.
CRAOS8X-5593 TSref: 00343164	OS6560-P48 switch is showing incorrect output for PoE command.
CRAOS8X-5599* TSref: 00327155	Cannot change rtr-port MTU.
CRAOS8X-5608 TSref: 00344005	Lanpower is not getting enabled on the switch and connected device does not get the power.
CRAOS8X-5644 TSref: 00343430	Error message "qosGetPlInfoFromModidDport 129" seen constantly after ISSU upgrade.
CRAOS8X-5671 TSref: 00344250	qosGetPlInfoFromModidDport Error Message Constantly Being Seen.
CRAOS8X-5737 TSref: 00345329	SPB out of service.
CRAOS8X-5738* TSref: 00343880	From CRAOS8X-5577 for 8.5.R03.
CRAOS8X-5744 TSref: 00343164	OS6560-P48 switch is showing incorrect output for PoE command.
CRAOS8X-5756 TSref: 00344244	OS6900: ECMP not working with OSPF externel E2 routes.
CRAOS8X-5778 TSref: 00343430	OS6900-X72: Error message "qosGetPlInfoFromModidDport 129" seen constantly after ISSU upgrade.
CRAOS8X-5790 TSref: 00345866	Part of password is visible in sh log swlog.
CRAOS8X-5866* TSref: 00339767	Error message "can't mmap MBUS resource: Bad file descriptor".
CRAOS8X-5867* TSref: 00334888	OS9907 - CMMB of a VC-2 is reported as down.
CRAOS8X-5895 TSref: 00346844	SNMP trap with 9900.
CRAOS8X-5928 TSref: 00347864	OSPF adjacency going down on random vlan (in default or specific Vrf), every 35 to 50 mn, seen on SAC-9907 switch.
CRAOS8X-5929 TSref: 00356068	MDNS: Activate MDNS stack on enabling responder. Close all unwanted socket connections. This issue was causing high CPU utilization which resulted in RIP flapping.

CRAOS8X-5935* TSref: 00334900	OS9900-(8.4.1.141.R03) rebooted after executing "write memory" and "show configuration snapshot" commands.
CRAOS8X-5938 TSref: 00325974	Link-monitoring recovery does not always work.
CRAOS8X-5990 TSref: 00334900	OS9900-(8.4.1.141.R03) rebooted after executing "write memory" and "show configuration snapshot" commands.
CRAOS8X-6009 TSref: 00347863	OS9900: BFD flaps in OS9907. Need to verify compatibility of BFD feature between OS9907 and Cisco 6509.
CRAOS8X-6039 TSref: 00348594	OS6860E- Switches are Randomly Re-booting.
CRAOS8X-6074 TSref: 00344332	SR # 00344332:MIB ifLastChange does not shows the right value.
CRAOS8X-6078/6104/6105 TSref: 00349453	Pim crash file generated on VC-5 OS6860E when issuing sh ip pim sgroutes
CRAOS8X-6164 TSref: 00298832	Crash svcCmm process after displaying show l2profile
CRAOS8X-6216 TSref: 00348920	Related to 6860E need to know if there is any setting to change the 2.5 Port to 1 Gigabyte.
CRAOS8X-6240 TSref: 00344901	Network Issue, High CPU and Ports on Blocking State on OS6860.
CRAOS8X-6316 TSref: 00342960	Links missing between the devices in OV2500 due to Getbulk enabled.
CRAOS8X-6334 TSref: 00347863	OS9900: BFD flaps in OS9907. Need to verify compatibility of BFD feature between OS9907 and Cisco 6509.
CRAOS8X-6392 TSref: 00350070	DDM warning in OS6900-C32.
CRAOS8X-6522 TSref: 00353893	Reload does not shows scheduled reload.
CRAOS8X-6744 TSref: 00338810	OS6900: SPBM pbit behavior in Q-in-Q.
CRAOS8X-6768 TSref: 00350539	"show chassis' only displays first 4 switches in stack.
CRAOS8X-6807 TSref: 00357059	User ports went down, one remained connected but was not showing a MAC address on the port.
CRAOS8X-6869 TSref: 00357478	OS6860, OS9900: encryption key to be masked.
CRAOS8X-7207 TSref: N/A	VC: Chassis 5 [OS6560-P24Z24] reboots twice to join in VC. Issue fixed with upgrade to FPGA version 0.7.
CRAOS8X-7308 TSref: 00361049	OS6860: Need PSU related SNMP alerts in the NMS.
CRAOS8X-7362/7597* TSref: 00359705	Following migration from OS9702 to OS9907, faced connectivity issues in AOS 6X devices doing Q-n-Q as double tagged VLAN get stripped while crossing the OS9907.
CRAOS8X-7374 TSref: 00357604	DVMRP not restoring communication after loss

CRAOS8X-7407 TSref: 00357604	DVMRP not restoring communication after loss.
CRAOS8X-7667 TSref: 00346609	SSH strong HMAC working.

* Status is "IN QA".