Release Notes – Rev. A

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

Release 8.5R2

These release notes accompany release 8.5R2. 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.

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 8.5.255.R02(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 8.5.255.R02(GA)

Hardware	Minimum Uboot	Minimum FPGA
OS6560-P24Z24	8.4.1.23.R02	0.6 (0x6)
OS6560-P24Z8	8.4.1.23.R02	-

Hardware	Minimum Uboot	Minimum FPGA
OS6560-P48Z16	8.4.1.23.R02	0.6
OS6560 (Non-PoE Models) OS6560-24X4 OS6560-P24X4	8.5.83.R01 8.5.89.R02 8.5.89.R02	0.7 0.4 0.4

OmniSwitch 6860(E) - AOS Release 8.5.255.R02(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)

***Note**: In previous AOS releases the FPGA version was displayed in hexadecimal format. Beginning in 8.4.1.R01 it is displayed in decimal format.

OmniSwitch 6865 - AOS Release 8.5.255.R02(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)

***Note**: In previous AOS releases the FPGA version was displayed in hexadecimal format. Beginning in 8.4.1.R01 it is displayed in decimal format.

OmniSwitch 6900-X20/X40 - AOS Release 8.5.255.R02(GA)

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

OmniSwitch 6900-T20/T40 - AOS Release 8.5.255.R02(GA)

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

OmniSwitch 6900-Q32 – AOS Release 8.5.255.R02(GA)

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

OmniSwitch 6900-X72 – AOS Release 8.5.255.R02(GA)

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

OmniSwitch 6900-V72/C32 – AOS Release 8.5.255.R02(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 8.5.255.R02(GA)

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

[IMPORTANT] *MUST READ*: AOS Release 8.5R2 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 B for important best practices, prerequisites, and step-by-step instructions. **Please note**: ISSU is not supported on a VC of OS9900s when using the 40G CMM ports with direct-attached cables as VFLs. See CRAOS8X-3846.
- Some switches that ship from the factory with AOS Release 8.5R2 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.

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 supports link aggregation only on the 2.5G and 10G ports. 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 8.5R2.
- The OS6560 supports a maximum of 384 user policies beginning in 8.5R2. If more than 384 policies are configured, the number should be reduced prior to upgrading.
- Beginning in 8.5R1, VLAN 4092 is a reserved VLAN on all OS6560 models for future feature support and can no longer be used for user traffic. If VLAN 4092 is configured on any OS6560 models, please reconfigure the switch to use a different VLAN before upgrading to 8.5R1.

- 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.

SPB L3 VPN Service-based (Inline Routing) and Loopback Protocol Support

The OmniSwitch supports SPB L3 VPN using either service-based (inline routing) or external loopback. The table below summarizes the currently supported protocols for each method in the 8.5R2 release.

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

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
EVB	Yes
FIP Snooping	Yes
FCoE VXLAN	Yes
Note: All other platforms do not support Data Center features.	

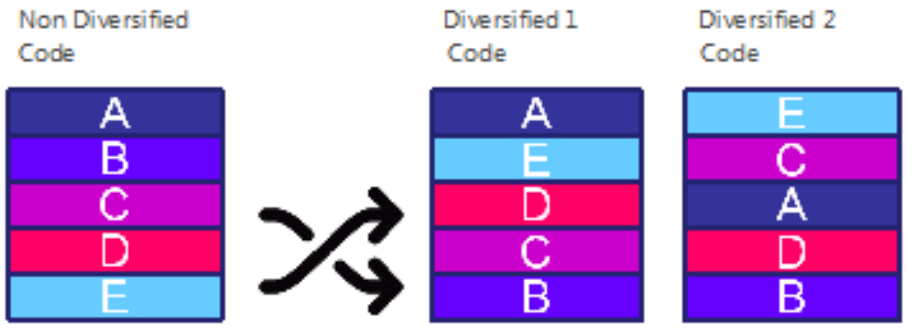
CodeGuardian

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.R02	AOS 8.5.RX2	AOS 8.5.LX2

- 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 6560-24X4
Fixed configuration chassis in a 1U form factor with:

- Twenty-four (24) - 10/100/1000 BaseT ports
- Two (2) - SFP 1G ports
- Four (4) - SFP+ (1G/10G) ports
- USB port
- RJ-45 console port

OmniSwitch 6560-P24X4
Fixed configuration chassis in a 1U form factor with:

- Twenty-four (24) - 10/100/1000 BaseT 802.3at PoE ports
- Two (2) - SFP 1G ports
- Four (4) - SFP+ (1G/10G) ports
- USB port
- RJ-45 console port

OmniSwitch 6900-V72
Fixed configuration chassis in a 1U form factor with:

- Forty-eight (48) – 10G/25G SFP28 ports
- Six (6) – 40G/100G QSFP28 ports
- USB port
- RJ-45 console port
- Front-to-rear or rear-to-front cooling
- AC or DC power supply
- Supports a VC of 2 chassis with another OS6900-V72 or an OS6900-C32 in static VFL mode.

OmniSwitch 6900-C32
Fixed configuration chassis in a 1U form factor with:

- Thirty-two (32) - 40G/100G QSFP28 ports
- USB port
- RJ-45 console port
- Front-to-rear or rear-to-front cooling
- AC or DC power supply
- Supports a VC of 2 chassis with another OS6900-C32 or an OS6900-V72 in static VFL mode.

Note: The airflow direction for all power supplies and fans must match on the OS6900-V72 and OS6900-C32 models. Mixing front-to-rear and rear-to-front components is not supported. However, no warning will be issued by the switch, see CRAOS8X-4291.

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 6465-P28

Fixed configuration, fanless, din-mountable, industrial hardended chassis:

- Twenty-two (22) - 10/100/1000 BaseT 802.3at PoE+ ports (Ports 1-8 support 60W HPoE)
- Two (2) - SFP 100/1000FX SFP ports
- Four (4) – SFP+ 1G/10G ports
- USB port
- RJ-45 console port
- Two (2) Alarm connectors (1-input, 1-output)

PS-I180AC-P

180W AC power supply for the OS6465-P28 providing system power and up to 112W of PoE power.

PSI180DC-P

180W DC power supply for the OS6465-P28 providing system power and up to 112W of PoE power.

Transceivers

Support for the following transceivers has been added to this release for the platforms listed below. Please refer to the Transceivers Guide for additional details on existing transceivers and the supported platforms.

Platform Support	Transceivers	
OS6900-V72	SFP-10G-SR	QSFP-40G-SR
	SFP-10G-LR	QSFP-40G-SR-BD
	SFP-10G-ER	QSFP-40G-LR
	SFP-10G-ZR	QSFP-40G-CLR
	SFP-10G-C1M/3M/7M	QSFP-40G-C40CM/1M/3M/7M
	SFP-10G-24DWD80	QSFP-4X10G-SR
	SFP-10G-GIG-LR	QSFP-4X10G-C1M/3M/5M
		QSFP-40G-AOC20M
	SFP-25G-SR	
	SFP-25G-LR	QSFP-100G-SR4
	SFP-25G-CLR	QSFP-100G-LR4
	SFP-25G-A20M	QSFP-100G-CLR4
	SFP-25G-C1M/3M/5M	QSFP-100G-CWDM4
		QSFP-100G-A20M
		QSFP-100G-C1M/3M/5M
		QSFP-4X25G-C1M/3M/5M
OS6900-C32	QSFP-40G-SR	QSFP-100G-SR4
	QSFP-40G-SR-BD	QSFP-100G-LR4
	QSFP-40G-LR	QSFP-100G-CLR4
	QSFP-40G-CLR	QSFP-100G-CWDM4
	QSFP-40G-C40CM/1M/3M/7M	QSFP-100G-A20M
	QSFP-4X10G-SR	QSFP-100G-C1M/3M/5M
	QSFP-4X10G-C1M/3M/5M	QSFP-4X25G-C1M/3M/5M
	QSFP-40G-AOC20M	

Platform Support	Transceivers	
OS6465-P28	iSFP-100-MM iSFP-100-SM15 iSFP-100-SM40 iSFP-GIG-SX iSFP-GIG-LX iSFP-GIG-LH40 iSFP-GIG-LH70 iSFP-GIG-BX-D iSFP-GIG-BX-U iSFP-GIG-T	iSFP-10G-C1M/3M/7M iSFP-10G-ER iSFP-10G-LR
OS6560-24X4/P24X4	Supports the same transceivers as existing OS6560 models. Please refer to the Transceivers Guide.	
Note: When connecting any 25G/40G/100G direct-attached cable between any combination of OS6900-V72, OS6900-C32, or OS9900 modules, auto-negotiation must be disabled on both ends. (CRAOS9X-1379)		

New Software Features and Enhancements

The following software features are being introduced this 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 "Data Center" require a license to be installed.

8.5R2 New Feature/Enhancements Summary

Feature	Platform
Dual-Home Link Support	6465
Auto-negotiation on OS99-CNI-U8	9900
MACSec Support using Dynamic Secure-Association-Key (SAK)	6465, 6860, 9900
802.1x Failover to MAC Authentication	6465
Multicast *,G	6560, 6860
L2 GRE Tunneling	6465, 6560, 9900
DHCP Enhancements - DHCP Static Binding Table Entries – Config Snapshot - DHCP Snooping – Port Range - DHCP Snooping – Enhanced Troubleshooting - DHCP Snooping – Clear Violation Counters	6560, 6860, 6865, 6900, 9900
MVRP Support	6465
VRRP Support	6465
REST API, Python, CLI Scripting Support	6465
Virtual Chassis Topology Change Notification Trap Across Reboot	6465, 6560, 6860, 6865, 6900, 9900
Virtual Chassis of 4	6465
Access Guardian – UNP Re-authentication Enhancement	6465, 6560
SPB IPv6 L3 VPN (loopback)	6860, 6865, 6900
ERPv2 Support	6560
1588 Support Across VC	6900-X72
Encrypted USB	6465
Control Directed Broadcast	6465, 6560, 6860, 6865, 6900
Increased Routing Table Size	6900-V72, 6900-C32, OS6900-X72
VRRP for IP Interface	6465, 6560, 6860, 6865, 6900, 9900
SPB: Multicast Optimization Over Services (Headend mode)	9900

Feature	Platform
IoT Device Profiling	6465, 6560, 6860, 6865, 6900, 9900
Auto QoS – New IP Phone MAC Address Ranges	6465, 6560, 6860, 6865, 6900, 9900
OV Cirrus – Zero Touch Provisioning enhancements	6465, 6560, 6860, 6865, 6900
Access Guardian – Display Port-range	6465, 6560, 6860, 6865, 6900, 9900
Captive Portal Authentication – No Flag Required on Final Profile	6465, 6560, 6860, 6865, 6900, 9900
IPv6 - Router Advertisement Filtering (RA Guard for IPv6)	6560
IPv6 - DHCP Guard	6560
Tandem Mode Support for SPB Multicast	6860, 6865, 6900
SPB Convergence with HW Based LSP flooding	9900
Early Availability	
Critical Voice VLAN	6465
Radius Health Check	6465, 6560
HAVLAN Support	6465, 9900
SPB: Multicast Optimization Over Services (Tandem mode)	9900
UDLD	9900
IPSec (IPv6)	9900
LBD – SAP	9900
Policy based routing	9900
Ethernet OAM (ITU Y1731 and 802.1ag)	9900
DHCPv6 Server	OS6900-V72/C32
Policy based mirroring	OS6900-V72/C32
MVRP	OS6900-V72/C32
sFlow	OS6900-V72/C32
Interface violation recovery	OS6900-V72/C32
Port mirroring - remote	OS6900-V72/C32
Spanning Tree (PVST+, Loop Guard)	OS6900-V72/C32, 9900

Dual-Home Link (DHL) Support

This release adds support for DHL on the OS6465.

Auto-negotiation on OS99-CNI-U8

This release adds supports for auto-negotiation on the OS99-CNI-U8.

MACSec Support using Dynamic Secure-Association-Key (SAK)

Adds MACSec support for Dynamic SAK using MACSec Key Agreement (MKA) Protocol on OmniSwitch 6465, 6860, 9900 platforms.

The MKA, as described in IEEE 802.1X-2010, is an extension to 802.1X, which provides the required session keys and manages the required encryption keys used by the underlying MACSec protocol. The MKA protocol allows peer discovery with confirmation of mutual authentication and sharing of MACSec secret keys to protect data exchanged by the peers.

In Dynamic SA Mode, Secure-Channel (SCI-TX/SCI-RX) and Secure-Association-Key (SAK) are exchanged between MACSec connected links using MKA protocol. The MKA protocol selects one of the nodes as the key server, which creates a dynamic SAK and shares it with the node at the other end over the secure channel. Once the other end also creates this dynamic SA key, subsequent traffic is secured using the new SA. The key server periodically and randomly creates and exchanges new SA to replace the older SA, using the MKA protocol for as long as the MACSec link is enabled.

There are two modes of provisioning the Connectivity Association Keys (CAK/CKN) between two MACSec endpoints. OmniSwitch supports the following:

- Dynamic SAK using Pre-Shared Key (PSK) - MACSec using Static Connectivity Association Key (static-CAK) using PSK
- Dynamic SAK using Extensible Authentication Protocol (EAP) - MACSec using Dynamic Connectivity Association Key (dynamic-CAK) using EAP.

MACSec platform support:

- OS6465-P6 and P12 - MACSec is supported on all ports.
- OS6860(E) – 10G ports on all E/non-E models
- OS6860E-P24Z8/P24 – 1G/10G ports (not supported on 2.5G ports)
- OS9900 Supported Modules - OS99-CMM (4X10G mode only), OS99-GNI-48/P48, OS99-XNI-48/P48/U48,P48Z16.
- MACSec is not supported on the OS99-CNI-U8, OS99-GNI-U48, and OS99-CMM in 40G mode.
- Due to the additional encryption/decryption operation required for MACsec, the wire-rate performance of any OmniSwitch port with MACsec enabled will differ from those ports where the feature is disabled.
- To confirm MACSec support use the **show interface capability** command. MACSec support is listed in the "MACSec Supported" field with the module exceptions noted above.

802.1x Failover to MAC Authentication

The option allows basic network access to trusted devices that failed in 802.1x supplicant authentication by subjecting the user through non-supplicant MAC authentication.

When 802.1x supplicant authentication fails, the supplicant users will be removed from 802.1x database and will be created in non-supplicant database, when the fail policy is set to MAC Authentication. The supplicant users will be classified based on non-supplicant policy. The MAC address of the failed supplicant user is sent to the RADIUS server for authentication, since the MAC address of the failed supplicant user is already present in the database.

On authentication, the user gets classified based on the returned VLAN or based on local authorization on non-supplicant policy.

This release adds support for the OS6465.

Multicast *,G

This release adds support for the multicast *,G feature on the OS6560 and OS6860.

L2 GRE Tunneling

Layer 2 Generic Routing Encapsulation (L2 GRE) tunnel. Similar to the OmniSwitch VXLAN implementation, L2 GRE provides a Layer 2 overlay network that is used to isolate and tunnel device traffic between tunnel end points over the underlying IP network.

- L2 GRE assumes that the tunnel end points (IP addresses) are reachable for tunneling traffic; configuring static routes or routing protocols (such as RIP or OSPF) to ensure end point reachability is required. The BFD protocol can be used to learn the ARP of the next-hop gateway.
- On switches that will operate as a tunnel aggregation switch, L2 GRE services and associated service objects are configured through Service Manager commands to create multiple tunnel end points.
- On switches that will operate as a tunnel access switch, a single tunnel end point is created by configuring a UNP profile that defines L2 GRE service parameters. When qualifying traffic is assigned to the profile, the necessary L2 GRE service objects are dynamically created. See Chapter 39, "Access Guardian Commands," for information about how to configure an L2 GRE UNP profile.

DHCP Enhancements

DHCP Static Binding Table Entries – Config Snapshot

This feature allows the display of the configured static bindings in the same output as the 'show configuration snapshot dhcp-snooping' command. The format of the output is in the form of the configuration command.

DHCP Snooping – Port Range

This feature allows for a port range to be used with the 'dhcp-snooping ip-source-filter port' command.

DHCP Snooping - Enhanced Troubleshooting

Debug commands for DHCP:

- debug dhcp admin-state {enable | disable}
- debug dhcp dump-packet admin-state {enable | disable}
- debug show dhcp
- debug dhcp clear log
- show dhcp-snooping counters
- dhcp-snooping clear counters
- show dhcp-snooping isf-statistics
- dhcp-snooping clear isf-statistics

DHCP Snooping - Clear Violation Counters

DHCP violation counters are displayed through the show output of 'show dhcp-snooping port' command. This feature enhancement allows the violation counters to be cleared using the 'dhcp-snooping clear violation-counters' command.

MVRP Support

This release adds support for MVRP on the OS6465.

VRRP Support

This release adds support for VRRP feature on the OS6465.

REST API, Python, CLI Scripting Support

This release adds support for the REST API, Python and CLI scripting features on the OS6465.

Virtual Chassis Topology Change Notification Trap

This feature will send a trap whenever there is a change to the VC topology such as an element being removed or added to the VC. Additionally, when issuing the **write memory** command, if any one of the VC elements is down a warning will be displayed about a possible configuration purge for the down element and ask for confirmation from the user to proceed.

Virtual Chassis of 4

This release adds support for Virtual Chassis of up to 4 OS6465s.

Access Guardian – UNP Re-authentication Enhancement

Previously, when re-authentication was performed for an already authenticated client, the context of the user in UNP and the MAC address from respective hardware tables were removed and the user was subjected to new authentication, this process impacted user data traffic since the MAC address was deleted. This feature enhancement reduces traffic loss by only removing the user context but leaving the MAC address in the table until the server returns the result of the new authentication.

UNP delay learning time interval specifies the amount of time, in seconds, that UNP will delay learning packets received on UNP ports.

- The configured time interval is triggered when the switch boots up. During this time, any packets received on all UNP ports are dropped until the timer expires.
- Configuring a delay learning interval gives the switch time to bring up IP interfaces and for route convergence to complete before any attempt to reach an authentication server is made.

SPB IPv6 L3 VPN

The SPB IPv6 L3 VPN solution supports two methods for routing L3 IPv6 traffic over an L2 SPBM network: VPN-Lite and L3 VPN. Both of these methods require an L3 VPN interface to serve as an IP gateway for accessing remote networks.

There are two options for defining an L3 VPN interface:

- Configuring a service-based IPv6 interface (OmniSwitch 9900 only – Not supported in this release). When this option is used, an IPv6 interface is created and bound to an SPB service ID. The service ID is associated with an I-SID.
- Configuring an external loopback port configuration (supported on all platforms except OS9900). When this option is used, a physical cable connects a regular port to a service access port. The regular port is tagged with an IPv6 interface VLAN; the access port is associated with an SPB Service Access Point (SAP). The VLAN-based IPv6 interface serves as the L3 VPN interface.

The external loopback configuration option defines an L3 VPN loopback interface, and the service-based IPv6 interface option defines an L3 VPN service-based interface.

ERPv2 Support

This release adds support for ERPv2 on the OS6560.

1588 Support Across Virtual Chassis

PTP end-to-end transparent clock is supported in standalone mode, virtual chassis of one, and virtual chassis of two. PTP end-to-end on a virtual chassis of two is supported only on the OmniSwitch 6900-X72. Single loopback port per chassis is required to support PTP in a virtual chassis of two.

Encrypted USB

Beginning in AOS Release 8.5R1 the OS6465 supports USB backup and restore capabilities. For target deployments of the OS6465 in mission critical networks, the sanctity of configuration and its protection is very important. This feature enhancement encrypts all the data during the USB backup process on the USB drive, including software images and configuration files, in a way that can only be decrypted by the switch during the restore process.

Control Directed Broadcast

The Control Directed Broadcast feature can be configured to direct only the packet from trusted source to the destined network, while the other directed broadcast packets are dropped.

To support the control directed broadcast, specify the source IP address, destination IP address and destination VLAN information to broadcast the packets in controlled manner. The specified information is considered as the trusted information to broadcast the packets received from the defined parameters, and the remaining broadcast packets are dropped.

Increased Routing Table Size

Allows an OS6900-V72, OS6900-C32, or OS6900-X72 to be configured in either a ‘switch’ or ‘router’ profile. The ‘switch’ profile provides more Layer 2 entries and the ‘router’ profile provides more LPM entries. The profile can be chosen based upon the network requirements. Refer to the Specifications Guide for table entry details.

VRRP for IP Interface

This feature allows VRRP to be configured based on an IPv4 or IPv6 interface. Prior to this implementation VRRP was configured on a VLAN basis. Supporting VRRP on an IP interface expands VRRP capability to either a VLAN or service, depending on how the IP interface is configured.

SPB: Multicast Optimization Over Services

Allows for the configuration of IPMS commands on an SPB service. This feature enhancement adds support for this capability on the OS9900 when the SPB service is configured to use the head-end mode (tandem mode is EA only).

IoT Device Profiling

IoT (Internet of Things) device profiling allows network administrators to support and manage smartphones, tablets and other devices connecting to the network. IoT device profiling uses DHCP FingerPrinting and MAC OUI to identify IoT devices.

MAC OUI: allows devices to be recognized by identifying their MAC addresses.

DHCP FingerPrinting: allows to track the devices on the network and block those are not allowed access. It also helps in analyzing the future growth by accessing the trending information.

IoT Device Profiling allows for the following:

- Identify and categorize various IoT devices connecting to the network.
- Identify the IoT devices based on local device signature database.
- Collect signature and various packet meta data required for IoT device identification.
- Profile devices based on identification.
- Use built-in UNPs for IoT device categories such as PoE camera, yemperature sensor, heart-rate monitor, medical imaging, etc. for the identified device.
- Maintain a database of identified IoT devices and un-identified IoT devices for qualitative and quantitative analysis.
- Classify the unidentified IoT devices based on UNP of choice.

Auto Qos – New IP Phone MAC Address Ranges

The IP phone MAC range is updated to automatically apply the QoS IP phone priority for the packets received from the source MAC in the following range:

MAC Address Range	Description
00:80:9F:00:00:00 to 00:80:9F:FF:FF:FF	Enterprise IP Phones Range
78:81:02:00:00:00 to 78:81:02:FF:FF:FF	Communications IP Phones Range
00:13:FA:00:00:00 to 0:13:FA:FF:FF:FF	Lifesize IP Phones Range
48-7A-55-00-00-00 to 48-7A-55-FF-FF-FF	ALE 8008 IP Phone MAC Range

OV Cirrus – Zero Touch Provisioning enhancements

Periodic Call Home of OV Cirrus : OmniSwitch is now enhanced for automatic Call Home to retrieve the latest configuration from OV Cirrus during device managed state or restart of Call Home with user mentioned time during error state. Periodic Call Home is triggered based on timer value from the server. VPN will be undisturbed during each Call Home, if there is no difference in VPN parameters from the previous one.

FQDN support for NTP server : NTP server configuration can also be configured with hostname/FQDN. The CLI commands "show ntp client, show ntp client server-list" will now display IP address as well as FQDN format according to the format in which the particular server was configured.

Default NTP pool server configuration for OV Cirrus : A new provision for configuring default NTP servers is added, when the DHCP server does not send any NTP configuration to cloud agent. This avoids issues during deployment, in which the certificate verification has failed due to a mismatch in time as NTP configuration is not present in the switch. The NTP pool server configuration provides a default NTP source for cloud operations, when there is no NTP server specified in the device configuration file and none is supplied by DHCP.

Access Guardian – Display Port-range

As part of the optimization in the snapshot display for Access Guardian the port configuration in the snapshot will be displayed in port-range format. The snapshot will merge the port configuration to range format only if the ports are contiguous and have the same configuration.

Captive Portal Authentication – No Flag Required on Final Profile

Previously, AOS expected the captive-portal flag to be enabled on both the initial (pre-authentication) and final (post-authentication) profile. This feature enhancement no longer requires the captive-portal flag to be enabled on the final post-authentication profile.

IPv6 - Router Advertisement Filtering (RA Guard for IPv6)

The IPv6 Router Advertisement (RA) filtering feature supports blocking or rejecting rogue RAs received on an IP VLAN. Router Advertisements are used by routers to announce themselves on a network. This feature provides a mechanism to reject RAs that are sent from unknown or unauthorized entities. When RA filtering is enabled on an IP VLAN, all RA packets received on untrusted ports or linkaggs of the VLAN are discarded. Only RA packets received on trusted ports will be re-transmitted out on all ports of the VLAN.

This release adds support for this feature on the OS6560.

IPv6 - DHCP Guard

DHCPv6 Guard is a feature for protecting hosts connected to a switched network against rogue DHCPv6 servers. When enabled, the OmniSwitch will filter DHCPv6 packets intended for DHCPv6 clients (UDP port 546) and discard packets that are not received on the specified trusted ports. Only ports on which a DHCPv6 server or relay is connected should be configured as trusted ports. If DHCPv6 packets are received on untrusted ports, they will be dropped.

- **Note:** On an OS6860, user configured ACLs for UDP port 546 will take precedence over the DHCPv6 Guard feature.
- **Note:** On an OS6560, the DHCPv6 Guard feature will take precedence over user configured ACLs for UDP port 546.

Tandem Mode Support for SPB Multicast

This feature adds support for IPMS on an SPB service configured in Tandem mode, except on the OS9900. Previously only head-end mode was supported.

SPB Convergence with HW Based LSP flooding

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

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, LFP link state is not maintained after NI reload. The "show lfp group" command output shows the wrong status after NI reload.	There is no known workaround at this time.
CRAOS8X-2587	On an OS9900, SPB double tagged packets are egressing as single tag in VLAN translation mode.	There is no known workaround at this time.
CRAOS8X-3078	The dhcp-snooping and ISF on 6900-Q32 for ports above 16D will not work.	There is no known workaround at this time.
CRAOS8X-3351	When extracting a CMM on an OS9900 with a sub-port configuration, the sub-port configuration will be lost or incorrect if a 'write memory' is entered.	Re-insert the CMM prior to entering 'write memory'.
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-3718	Device is dropping mDNS packets if system location configured to 255 characters.	Configure the system location with a maximum of 206 characters.
CRAOS8X-3897	"show vrrp3" displays error message for user to use "show ip vrrp3". But the correct command is "show ipv6 vrrp".	There is no known workaround at this time.
CRAOS8X-3941	Sometimes an SDP entry is not getting created for tagged traffic when the system-default service base is 512 and service-mod is 256.	There is no known workaround at this time.
CRAOS8X-4070	PTP is not supported on ports 1/1/25 and 1/1/26 on 6465-P28 for release 85R2. All other ports have PTP support.	There is no known workaround at this time.
CRAOS8X-4171	On an OS9900 VC, the following message is seen on the console	There is no known workaround at this time.

	during bootup: "error msg "[slot 1] Thu Aug 30 00:15:56 ChassisSupervisor fpgaMgr ERR fpgaMgrVMSetupFd: error creating host socket - 4 (Interrupted system call)".	There is no functional impact the switch comes up after SYSTEM READY.

Layer 2 GRE

PR	Description	Workaround
CRAOS8X-4103	On an OS9900, traffic is not tunneled over L2GRE service when traffic is sent from access to aggregation switch via another access switch where links between two access switches are configured as static linkagg.	There is no known workaround at this time.
CRAOS8X-4124	On an OS9900, traffic is not tunneled over L2GRE service when sending traffic from access to aggregation switch via another access switch where SAP/loopback port on aggregation switch is configured as static linkagg.	There is no known workaround at this time.
CRAOS8X- 4125	On an OS9900, 6860, traffic is not tunneled over L2GRE service when SAP port on one NI and SDP port on different NI with multiple ECMP routes to reach far-end IP.	There is no known workaround at this time.
CRAOS8X-4145	On an OS6860, mac-addresses learned on L2GRE service on access side are removed after second takeover at the aggregate switch end.	There is no known workaround at this time.

Port Mirroring / Monitoring / Mapping

PR	Description	Workaround
CRAOS8X-1596	On an OS6900, all mirrored egress packets contain a VLAN header even if the port is untagged.	There is no known workaround at this time.
CRAOS8X-2518/4271	Port mapping on linkagg ports is not supported on OS6560 platforms.	There is no known workaround at this time.
CRAOS8X-3184	802.1q information is missing when mirroring VRRPv3 packets.	There is no known workaround at this time.

QoS

PR	Description	Workaround
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-3369	On an OS65650 with egress port bandwidth set to a decimal value the traffic gets dropped to 50 percent of configured value.	There is no known workaround. Happens only at very low bandwidth settings on 10G ports.
CRAOS8X-4191	During reload, UNP users are moved to auth-server-down profile and entries created for auth-server-down profile VLAN. Once users move to final profile (when RADIUS server comes back up), entries should be created for new VLAN and old entry should be deleted. But a few old entries are not deleted which results in traffic drop for those users.	Configure unp delay-learning to 360 seconds.
CRAOS8X-4222	Not able to configure source port range on an OS6900-C32.	Configure first port of range individually and then configure the port range. For example: policy condition test1 source port 2/1/1 policy condition test1 source port 2/1/1-28.
CRAOS8X-4224	On OS6465, OS6560, OS6900-V72/C32, OS9900 when using the 'reload chassis' command, TCAM entries are being reduced and the QoS configuration is getting corrupted.	If QoS policies have been configured at runtime and a reload has not been performed, it is advised to perform following steps: 1) Save the QoS configuration snapshot in a backup file.

		2) Flush and apply. 3) Reapply the config from backup file.
CRAOS8X-4226	Policy condition CLI does not display an error when attempting to configure on VFL ports for OS6560, OS6465 and OS9900 platforms.	There is no known workaround at this time.

Hardware

PR	Description	Workaround
CRAOS8X-1379	100G DAC transceivers do not come up between OS9900-CNI-U8 and OS6900-V72.	Disable auto-negotiation on both ends.
CRAOS8X-3828	100G link flaps twice when disabled and then re-enabled.	There is no known workaround at this time.
CRAOS8X-3832	Port links are down between CNI-U8 and OS6900-V72 using a QSFP28 4x25G DAC splitter.	Disable auto-negotiation when using DAC cables.
CRAOS8X-3334	On an OS6900-V72, intermittent CRCs may temporarily occur when performing a hot- swap of SFP-10G-SR/LR/ER.	There is no known workaround at this time.
CRAOS8X-3846	Due to having different default auto-negotiation settings (disabled by default beginning in 8.5R2), ISSU is not supported on a VC of OS9900s when using the 40G CMM ports with direct-attached cables as VFLs.	Temporarily use 10G ports as VFLs for performing ISSU. Once the upgrade is complete, the 40G VFLs will become operational.
CRAOS8X-4291	AOS fails to detect when there is mis-match of front-to-rear and rear-to-front power supplies and fans.	There is no known workaround at this time. Ensure all power supplies and fans have the same airflow direction.

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 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
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

OS9900 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. 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.

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: support.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 hardware configuration, module types 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: Feature Matrix

The following is a feature matrix for AOS Release 8.5R2.

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	N	Y	Y	Y	Y	N	Y	
DHCP Relay	8.5R1	Y	Y	Y	Y	N	Y	
DHCPv6 Server	N	N	Y	Y	Y	EA	Y	
DHCPv6 Relay	8.5R1	Y	Y	Y	Y	N	Y	
DHCP Snooping	N	Y	Y	Y	Y	N	Y	
DHCP Snooping IP source filter	N	Y	Y	Y	Y	N	Y	
DHCP static binding table entries through show config	N	8.5R2	8.5R2	8.5R2	8.5R2	N	8.5R2	
DHCP snooping config consolidation	N	8.5R2	8.5R2	8.5R2	8.5R2	N	8.5R2	
DHCP snooping enhanced troubleshooting	N	8.5R2	8.5R2	8.5R2	8.5R2	N	8.5R2	
DHCP snooping clear command	N	8.5R2	8.5R2	8.5R2	8.5R2	N	8.5R2	
DHCP Guard – IPv6	N	8.5R2	N	N	N	N	N	
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 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	

Feature	6465	6560	6860(E)	6865	6900	6900-V72/C32	9900	Notes
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	N	Y	Y	Y	8.5R2	Y	
OSPFv3	N	N	Y	Y	Y	8.5R2	Y	
RIP v1/v2	8.5R1	Y	Y	Y	Y	8.5R2	Y	
RIPng	8.5R1	Y	Y	Y	Y	8.5R2	Y	
VRRP v2	8.5R2	Y	Y	Y	Y	8.5R2	Y	
VRRP v3	8.5R2	Y	Y	Y	Y	8.5R2	Y	
VRRP v2/v3 – IP Interface	8.5R2	8.5R2	8.5R2	8.5R2	8.5R2	8.5R2	8.5R2	
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	Y	Y	Y	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	N	
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	N	
HAVLAN	EA	N	Y	Y	Y	N	EA	

Feature	6465	6560	6860(E)	6865	6900	6900-V72/C32	9900	Notes
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	
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	EA	EA	
MVRP	8.5R1	Y	Y	Y	Y	EA	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 (L2 only)	Y	
SPB IPv4 L3 VPN (loopback)	N	N	8.5R2	8.5R2	8.5R2	N	N	
SPB IPv4 L3 VPN (serviced-based / inline routing)	N	N	N	N	N	N	Y	
SPB IPv6 L3 VPN (loopback)	N	N	8.5R2	8.5R2	8.5R2	N	N	
SPB IPv6 L3 VPN (serviced-based / inline routing)	N	N	N	N	N	N	N	
SPB – Multicast optimization over services using head-end mode	N	N	Y	Y	Y	N	8.5R2	
SPB – Multicast optimization over services using tandem mode	N	N	8.5R2	8.5R2	8.5R2	N	EA	
SPB – HW-based LSP flooding	N	N	N	N	N	N	Y	
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	

Feature	6465	6560	6860(E)	6865	6900	6900-V72/C32	9900	Notes
Policy Lists	8.5R1	Y	Y	Y	Y	N	Y	
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	N	N	
Ethernet OAM (ITU Y1731 and 802.1ag)	8.5R1	N	Y	Y	Y	N	EA	
EFM-OAM (802.3ah)	N	N	N	N	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	N	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	N	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	Y	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	N	Y	
LLDP	8.5R1	Y	Y	Y	Y	8.5R2	Y	

Feature	6465	6560	6860(E)	6865	6900	6900-V72/C32	9900	Notes
MACSec	8.5R1	N	Y	N	N	N	8.5R2	
MACSec MKA Support	8.5R2	N	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								
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	Y	N	N	
FCoE / FC Gateway	N	N	N	N	Y	N	N	
VXLAN	N	N	N	N	Q32/X72	N	N	
VM/VXLAN Snooping	N	N	N	N	Y	N	N	
FIP Snooping	N	N	N	N	Y	N	N	

Appendix B: 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 8.5R2 (GA)
OS6465	Not Supported
OS6560	Not Supported
OS6860(E)	8.4.1.229.R02 (GA) 8.4.1.233.R02 (MR) 8.4.1.141.R03 (GA) 8.5.164.R01 (GA)
OS6865	8.4.1.229.R02 (GA) 8.4.1.141.R03 (GA) 8.5.164.R01 (GA)
OS6900	8.4.1.170.R01 (GA) 8.4.1.229.R02 (GA) 8.4.1.233.R02 (MR) 8.4.1.141.R03 (GA) 8.5.164.R01 (GA)
OS9900	8.4.1.229.R02 (GA) 8.4.1.141.R03 (GA) **Note**: ISSU supported on VC of 2 only. **Note**: ISSU is not supported on a VC of OS9900s when using the 40G CMM ports with direct-attached cables as VFLs. See CRAOS8X-3846.
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.	

8.5R2 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 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
```

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

Appendix C: 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
- OS6860 – Uos.img
- OS6865 – Uos.img
- 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           8.5.255.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

-> 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 D: 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
- OS6560 – Uos.img
- 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           8.5.255.R02


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   : 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

-> 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: Fixed Problem Reports

The following problem reports were closed in this AOS Release.

PR	Summary
CRAOS8X-252 TS:00272615	OS9907 : Uplinks between the OS9907 and the OS6450 are flapping continuously.
CRAOS8X-610 TS:00274853	OS6860E: QOS logging is not working.
CRAOS8X-642 TS:00276847	"Network Time Protocol (NTP) Mode 6 Scanner" is detected with Medium Severity.
CRAOS8X-669 TS:00277677	mac-learning not working with port-security enabled.
CRAOS8X-674 TS:00284614	Issue with SNMPwalk slMacAddressGblRowStatus.
CRAOS8X-730 TS:00276689	SNMP traps not sent out to NMS from the VC of three OS6860 if any of the slave units reboted.
CRAOS8X-735 TS:00290569	DHCP-snooping option 82 bypass check issue.
CRAOS8X-1348 TS:00286438	SNMP Trap in OS6900.
CRAOS8X-1804 TS:00296044	OS6900- document correct request regarding loopback advertisement in OSPFv3.
CRAOS8X-1847 TS:00299983	DHCP snooping fails after the hard-reboot.
CRAOS8X-1860 TS:00300067	Change in DHCPd.conf without disabling dhcp service causes continuous reboot.
CRAOS8X-1976 TS:00296912	OS6865-P16X : Unable to do SNMP walk using the ifXTable.
CRAOS8X-2030 TS:00296912	OS6865-P16X : Unable to do SNMP walk using the ifXTable.
CRAOS8X-2039 TS:00299001	OS6900/OS6860 Unable to configure BFD on OSPF IPV6 interface with dr-only.
CRAOS8X-2072 TS:00295560	Case creation for NI3 Module OS99-XNI-U48 unexpected reboot.
CRAOS8X-2199 TS:00276689	SNMP traps not sent out to NMS from the VC of three OS6860 if any of the slave units reboted.
CRAOS8X-2202 TS:00294483	OS6900/OS6860VC MIB "dot1dStpPortTable" not showing information from the slave units.
CRAOS8X-2336 TS:00303366	OS6560 : Remote Auto-config failed.
CRAOS8X-2399 TS:00305053	Adding lldp port configuration for 2x ports make the cli 'show configuration snapshot' and write memory failing on OS10K Good Shepperd Standalone.
CRAOS8X-2593 TS:00275783	OS6900 - ICMP Flood on the SAP ports for one specific IP address part of VLAN 10 (service 10010).

CRAOS8X-2678 TS:00308169	Radius NAS-Identifier is not sent on RADIUS Access-Request, wrong NAS-Port-ID on SSH Authentication.
CRAOS8X-2717 TS:00305883	Switch crashed after configuring the jumbo frame in client connected to OS6860E-48.
CRAOS8X-2786 TS:00308031	OS6860E-U28 strange behaviour when connect 10G DAC cable on 1G port.
CRAOS8X-2836 TS:00305053	Adding lldp port configuration for 2x ports make the cli 'show configuration snapshot' and write memory failing on OS10K Good Shepperd Standalone.
CRAOS8X-2957 TS:00292073	UNP user state stuck "in progress" after CoA-Request/ACK.
CRAOS8X-3107 TS:00293451	4xOS6900VC continuously generating TCN.
CRAOS8X-3225 TS:00307194	802.1x authentication for LDAP users does not work after upgrading to 8.5.R01.
CRAOS8X-3259 TS:00304091	OS9900 not showing config, show tech and saving configuration.
CRAOS8X-3284 TS:00300325	OS9900-VC - write memory failed to retrieve Qos configuration - MIP_GATEWAY mipgwd warning(4) ERROR response for MIP_GET(1) 68/0->13 (APPID_SNMP_AGENT->APPID_QOS).
CRAOS8X-3428 TS:00287128	Random issue with UNP supplicant clients to go into filtering mode and falling into VLANs 1 and 4095.
CRAOS8X-3435 TS:00316752	If Dhl feature is enabled, with no cable connected on ports 1/1/51-52, only a SFP-10G-LR
CRAOS8X-3636 TS:00310521	OS9900 port is up but vlan status is inactive, and can't write memory.
CRAOS8X-3779 TS:00319631	OS6560: none of the show commands work to show the reload is scheduled.
CRAOS8X-3851 TS:00321110	OS9900 CMM-B Down after CMMA crashed.
CRAOS8X-3858 TS:00321136	After a reload of the 6560, with a configured dhl, having both links down (not connected), Removing the dhl configuration make vlan members ports being forwarding.
CRAOS8X-3990 TS:00290553	OS10K: LInkagg ports removed from Config after CMM-A was extracted.
CRAOS8X-4116 TS:00323879	OS6860E UNP user authentication issue "un-replied count 200".