Release Notes – Rev. A

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

Release 8.6R1

These release notes accompany release 8.6R1. 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 8.6.289.R01 (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
OS6465T-12	8.6.117.R01	0.4
OS6465T-P12	8.6.117.R01	0.4

OmniSwitch 6560 – AOS Release 8.6.289.R01 (GA)

Hardware	Minimum Uboot	Minimum FPGA
OS6560-24Z24	8.5.22.R01	0.7

Hardware	Minimum Uboot	Minimum FPGA
OS6560-P24Z24	8.4.1.23.R02	0.6 (Minimum) 0.7 (Current)*
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 8.6.289.R01 (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 8.6.289.R01 (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 8.6.289.R01 (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 8.6.289.R01 (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 8.6.289.R01 (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 8.6.289.R01 (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 8.6.289.R01 (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 8.6.289.R01 (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 (903753-90) OS99-XNI-48 (904049-90)	8.3.1.103.R01 8.6.261.R01	1.3.0 1.4.0	0.6 0.7
OS99-XNI-U48 (903723-90) OS99-XNI-U48 (904047-90)	8.3.1.103.R01 8.6.261.R01	2.9.0 2.10.0	0.8 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
OS99-XNI-U12Q	8.6.117.R01	1.5.0	N/A
OS99-XNI-UP24Q2	8.6.117.R01	1.5.0	N/A

[IMPORTANT] *MUST READ*: AOS Release 8.6R1 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.

  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 or above.

- Change in NTP Functionality - Beginning with AOS Release 8.5R4, OmniSwitches will not synchronize with an unsynchronized NTP server (stratum 16), as per the RFC standard. Existing installations where

OmniSwitches are synchronizing from another OmniSwitch, or any other NTP server which is not synchronized with a valid NTP server, will not be able to synchronize their clocks.

The following NTP commands have been deprecated:
- ntp server synchronized
- ntp server unsynchronized

- MACsec Licensing Requirement
  Beginning in 8.6R1 the MACsec feature requires a site license, this license can be generated free of cost. After upgrading, the feature will be disabled until a license is installed. There is no reboot required after applying the license.

- DHCPv6 Guard - Configuration via an IPv6 interface name is deprecated in 86R1. Commands entered using the CLI must use the new '**ipv6 dhcp guard vlan** *vlan-id*' format of the command. The old format will still be accepted if present in a vcboot.cfg to preserve backwards compatibility.

- The vlan-priority and drop-eligible parameters have been deprecated from all SAA commands beginning in 8.6R1.

- MACsec is now supported on ports 33-48 of the 6560-(P)48X4. CR CRAOS8X-7910 is resolved.

- The 'ip helper' commands have been deprecated and replaced with 'ip dhcp relay'. The old format will still be accepted if present in a vcboot.cfg to preserve backwards compatibility.

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 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.	

	License Required			
	OS6465	OS6560	OS6860	OS9900
Licensed Features				
MACsec	Yes	Yes	Yes	Yes
10G support	No	Yes*	No	No
*10G license is optional for ports 25/26 (OS6560-24X4/P24X4) and ports 49/50 (OS6560-48X4/P48X4). Ports support 1G by default.				

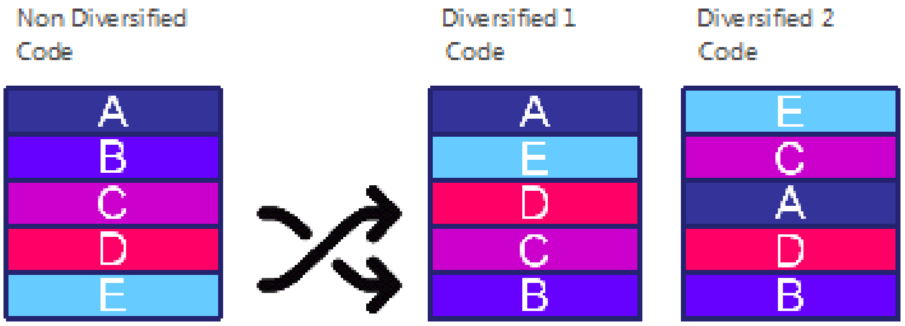
CodeGuardian

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 8.6.R01	AOS 8.6.RX1	AOS 8.6.LX1

- X=Diversified image 1-3
- ALE will have 3 different diversified images per AOS release (R11 through R33)
- Our partner LGS will have 3 different diversified images per AOS release (L11 through L31)

Please contact customer support for additional information.

New / Updated Hardware Support

The following new hardware is being introduced in this release.

OmniSwitch 6465T-12

Fixed configuration chassis in a 1U form factor with:

- Eight (8) - 10/100/1000Base-T RJ-45 ports
- Two (2) - 10/100/1000Base-T RJ-45 or 100/1000Base-X SFP combo ports
- Two (2) - 1000Base-X SFP ports
- USB port
- RJ-45 console port
- Supports extended temperature range (-10C - 60C)
- Supports a VC of up to 4 with other OS6465 models

OmniSwitch 6465T-P12

Fixed configuration chassis in a 1U form factor with:

- Eight (8) - 10/100/1000BaseT 802.3at PoE RJ-45 ports
- Two (2) - 10/100/1000Base-T RJ-45 or 100/1000Base-X SFP combo ports
- Two (2) - 1000Base-X SFP ports
- USB port
- RJ-45 console port
- Supports extended temperature range (-10C - 60C)
- Supports a VC of up to 4 with other OS6465 models

OS99-XNI-U12Q

OmniSwitch 9900 module with:

- Twelve (12) - 1G/10G SFP+ ports
- One (1) - 40G QSFP+ port

OS99-XNI-UP24Q2

OmniSwitch 9900 module with:

- Twelve (12) - 1G/10G SFP+ ports
- Twelve (12) – 1G/10GBaseT 802.3at PoE ports
- Two (2) - 40G QSFP+ ports

QSFP-40G-ER

40-Gigabit optical transceiver (QSFP+ MSA). Supports single mode fiber. Typical reach 40 km. Duplex LC receptacles.

SFP-10G-BX-D

10-Gigabit optical transceiver (SFP+) with an LC type interface.This bi-directional transceiver is designed for use over single mode fiber up to 10 km. Transmits 1330 nm and receives 1270 nm optical signal.

SFP-10G-BX-U

10-Gigabit optical transceiver (SFP+) with an LC type interface.This bi-directional transceiver is designed for use over single mode fiber up to 10 km. Transmits 1270 nm and receives 1330 nm optical signal.

SFP-10G -CWDM

10-Gigabit CWDM transceiver (SFP+ MSA) with an LC type interface. Supports single mode fiber over 1551 nm wavelength. Typical reach of 40Km.

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.

8.6R1 New Feature/Enhancements Summary

Feature	Platform
Management / NMS Related Features	
AOS Micro Services (AMS)	6465, 6560, 6860, 6865, 6900, 9900, 6900-V72/C32
Auto-VFL - Enable by default on 10G SFP+ ports	6560-(P)24X4/(P)48X4
Boot Server Discovery Protocol (BSDP/Apple NetBoot) - Handle multiple responses from multiple servers	6860
Dying Gasp - EFM OAM (Link OAM) PDUs	6465, 6560, 6865
Event Log - Readable Event Log	6465, 6560, 6860, 6865, 6900, 9900, 6900-V72/C32
Licensing - MACsec Site-wide Licensing	6465, 6560, 6860, 9900
Licensing - 10G Ports	6560-(P)24X4/(P)48X4
SNMP Trap - ARP Limit Reached	6465, 6560, 6860, 6865, 6900, 9900, 6900-V72/C32
SNMP Trap - MAC Limit Reached	6465, 6560, 6860, 6865, 6900, 9900, 6900-V72/C32
Service / Access port / UNP Related Features	
Force-L3-Learning Support on Access Ports	6900, 9900
L2 GRE Tunnel Access (Edge) - Dynamic Service (UNP access ports)	6860, 6865, 6900-Q32/X72, 9900
L2 GRE Tunnel Access (Edge) - Multiple Services on an OmniSwitch 6560	6560
Multiple MAC Range Port Security	6465, 6560, 6860, 6865, 6900, 9900, 6900-V72/C32
SPB - Multicast Optimization for Dynamic Services	6860, 6865, 6900
SPB - IGMP Snooping for Services (Multicast Over SPB Optimization)	6900-V72/C32
VRRP Feature with Dynamic UNP	6860,6865,6900,9900
DHCP / UDP Related Features	
DHCP Snooping Global Admin Disable	6465, 6560, 6860, 6865, 6900, 9900, 6900-V72/C32
DHCP Snooping Binding Table - New CLI Commands and Behavior	6465, 6560, 6860, 6865, 6900, 9900, 6900-V72/C32
DHCPv6 Relay - Support for Services and Migration to the New CLI	6860, 6865, 6900, 9900, 6900-V72/C32
IPv4 and IPv6 Behavior Parity for DHCPv6/ISFv6	6860, 6865
IPv6 - UDP Relay	6465, 6560, 6860, 6865, 6900, 9900, 6900-V72/C32
IPv6 - DHCP Snooping Binding Table for ISF	6560
IPv4 - UDP Relay - Support for services and migration to the new CLI	6860, 6865, 6900, 9900, 6900-V72/C32
Layer 3 Related Features	
IP Black Hole Route (Null Route) - IPV4 and IPV6	6465, 6560, 6860, 6865, 6900, 9900, 6900-V72/C32
PIM Message Packing Optimization	6860,6900,6900-V72/C32

Feature	Platform
Security Related Features	
Device profiling - OV Support	6465, 6560, 6860, 6865, 6900, 9900, 6900-V72/C32
Device profiling - Support on OS6900-V72/C32	6900-V72/C32
RADIUS and TACACS Pre-shard Key Encryption Method	6465, 6560, 6860, 6865, 6900, 9900, 6900-V72/C32
Role-based Authentication	6900-V72/C32
Common Criteria Related Features	
Syslog-ng with TLS Encryption	6465, 6560, 6860, 6865, 6900, 9900, 6900-V72/C32
Configurable OpenSSL Cipers in Default Switch Operation	6465, 6560, 6860, 6865, 6900, 9900, 6900-V72/C32
SNMP with TLS Encryption	6465, 6560, 6860, 6865, 6900, 9900, 6900-V72/C32
Metro Features	
Ethernet Loopback Test	6860,6865
CPE Test Head	6465
IEEE 1588 Peer-2-Peer Transparent Clock	6465
Layer 2 Custom / New Protocol	6465, 6860, 6865
MAC Forced Forwarding	6860, 6865
PPPoE - Intermediate Agent	6465, 6865
SAA SPB Measurements using 1 Second Intervals	6860, 6865, 6900
Additional Features	
Policy-based Mirroring - Multiple Destination Ports	9900
Early Availability Features	
UDLD	OS6900-V72/C32
AOS PKI x.590v3 Certificates in Default Operation from CCE mode	6465, 6560, 6860, 6865, 6900, 9900, 6900-V72/C32
DHCP Guard Without IP Interface	6560, 6860, 6865
DHCPv6 / ISFv6 - Support for Client Guard/Guard Only Option	6860, 6865

AOS Micro Services (AMS)

AOS Micro Services (AMS) can be used to help propagate switch configurations, such as UNP profiles, across the network to other OmniSwitches. This feature leverages the publisher/subscriber relationship, community names and topics to publish configuration information between OmniSwitches. It can currently be used for the following:

- Device Profiling Signature Synchronization
- OmniSwitch 6465 power supply configuration synchronization

Auto-VFL - Enable by Default on OS6560 10G SFP+ Ports

The last two 10G SFP+ ports on the OS6560-(P)24X4 (ports 29-30) and the OS6560-(P)48X4 (ports 53-54) now have auto-VFL enabled by default.

Boot Server Discovery Protocol (BSDP/Apple NetBoot)

Support for this protocol was introduced in 8.5R4. In 8.6R1 the capability has been enhanced to allow for the forwarding of multiple ACK packets sent from multiple BSDP servers for each INFORM packet.

Dying Gasp - EFM OAM / Link OAM PDUs

As soon as the Dying Gasp event is detected, an 802.3ah OAM Information PDU is sent to ports on which Link OAM is enabled. The PDU will have the Dying Gasp bit set. Dying gasp packets will first be sent on high priority ports followed by least priority ports. Uplink ports are treated as high priority ports followed by combo ports and user ports.

Event Log - Readable Event Log

AOS is now designed to provide Readable Customer Event information about important events on the OmniSwitch in a user-friendly, consistent and customer readable format. A new set of CLI commands are introduced to view Readable Customer Events. Unlike AOS Syslog, Readable Customer Event feature provides logs for the most significant switch events.

Licensing - MACsec Site-wide Licensing

Beginning in 8.6R1 the MACsec feature requires a license. The MACsec license is a no-cost, site license and does not use the serial number and MAC address of the switch. The MACsec license file can be applied using the '**license apply file** *filename* **order-id** *order-id*' command. For switches being upgraded to 8.6R1 that have MACsec configured, MACsec will not be enabled after upgrading. The MACsec license must be applied and MACsec re-enabled after upgrading, there is no reboot required. The 'OS-SW-MACSEC' is the no-cost part number orderable for this license. The license can be generated by visiting https://businessportal2.alcatel-lucent.com.

Licensing - OS6560 10G Ports

A 10G license can be installed on the OS6560-24X4/P24X4/48X4/P48X4 models to upgrade ports 25/26 (24-port models) or ports 49/50 (48-port models) from 1G to 10G. There is no reboot required after applying this license but the ports should be administratively disabled and re-enabled. The 'OS6560-SW-PERF' is the orderable part number for this license. The license can be generated by visiting https://businessportal2.alcatel-lucent.com.

SNMP Trap - ARP Limit Reached

When the ARP table utilization threshold of 95% is reached an SNMP trap is generated to indicate the max-limit state has been reached. When the utilization falls back below 90% capacity the max-limit state is cleared and an SNMP trap is generated to indicate the cleared max-limit state. A single trap is generated for an entire virtual-chassis.

SNMP Trap - MAC Limit Reached

When the MAC table utilization threshold of 95% is reached an SNMP trap is generated to indicate the max-limit state has been reached. When the utilization falls back below 90% capacity the max-limit state is cleared and an SNMP trap is generated to indicate the cleared max-limit state. A single trap is generated for an entire virtual-chassis.

Force L3 Learning on Access Ports

Adds support for forced Layer 3 learning on UNP access ports. When this functionality is enabled and IP-based classification rules are configured, only Layer 3 packets are used to learn devices connected to UNP ports. Previously, this functionality was supported only for Layer 3 packets received on UNP bridge ports; now this functionality is also supported for Layer 3 packets received on UNP access ports.

L2 GRE - Service on Static and Dynamic Ports

The L2 GRE service functionality was previously applied only to users learned on UNP bridge ports. This functionality has been extended to include users learned on UNP access ports. Additional enhancements to support this new capability include the following:

- Configurable VLAN translation for UNP profiles mapped to L2 GRE service parameters.

L2 GRE - Multiple Services on an OmniSwitch 6560

Configuring a reserved VLAN is required to activate L2 GRE functionality on an OmniSwitch 6560 tunnel access switch. If the reserved VLAN is not created on this switch, then UNP will not learn users in the L2 GRE service domain. Other supported platforms do not require a reserved VLAN to activate L2 GRE functionality.

A reserved VLAN corresponds to one L2 GRE service. To allow multiple L2 GRE services on the OmniSwitch 6560, configuring up to eight reserved VLANs is allowed. This will support eight UNP profiles each mapped to an L2 GRE service. UNP profiles mapped to an L2 GRE service are applied to users learned on UNP bridge ports; L2 GRE functionality is not supported on UNP access ports.

Other platforms that support L2 GRE functionality do not support multiple L2 GRE services for users learned on UNP bridge ports but do support multiples services for users learned on UNP access ports.

Multiple MAC Range - Learned Port Security

The LPS MAC range allows restricting the source learning of the host MAC addresses. The MAC range command supported only one MAC range configuration in previous releases. 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.

SPB - Multicast Optimization for Dynamic Services

Shortest Path Bridging (SPB) multicast optimization applies the functionality of IGMP/MLD snooping (OmniSwitch IP Multicast Switching) to static SPB services and associated Service Access Points (SAPs). This allows SPB backbone edge bridges to perform multicast filtering on a per-SAP, per-service basis to ensure that IP multicast traffic is not sent out SAP ports onto LANs where there are no devices requesting to receive the multicast stream. As a result, configuring IP Multicast Switching for SPB services helps to cut down on the unnecessary forwarding of IP multicast traffic.

This same functionality can also be applied to dynamic SPB services and associated SAPs that are created through the UNP framework. IGMP and MLD snooping options are configurable mapping attributes for UNP service profiles that are mapped to SPB service parameters. When a device is classified into the SPB service-mapped profile, a dynamic SPB SAP is created and the specified IGMP/MLD snooping functionality is applied to the dynamic SAP.

SPB - IGMP Snooping for Services

Support added to OS6900-V72/C32 in this release.

VRRP with Dynamic UNP

When a dynamic UNP SAP connects two VRRP routers over a Shortest Path Bridging (SPB) backbone service, VRRP advertisements are sent through the SPB service domain to elect one router as the master and one as the slave (backup router). The slave router does not send out VRRP advertisements; only listens for advertisements from the master router. This inactivity may cause the dynamic UNP SAP on which the slave router communicates to age out. When this occurs, the slave router will no longer receive advertisements from the master router and will elect itself as the master. This results in two dual VRRP master routers operating within the same SPB service domain.

To support a VRRP configuration over dynamic UNP SAP connections, the following configuration is required:

- Statically assign an SPB service-mapped UNP profile to a UNP access port to create a persistent SPB SAP on which the VRRP router will communicate. A persistent SAP does not age out and will ensure an uninterrupted flow of VRRP advertisements to the VRRP router.
- Enable MAC address mobility for the SPB service-mapped UNP profile. This provides support for VRRP MAC address movement that is required for the VRRP master/slave election process.

DHCP Snooping - Global Admin Disable

Disabling the DHCP Snooping status globally or for a specific VLAN retains the user-configured DHCP configuration and will flush dynamic binding entries. A “no” form was added to the global “dhcp snooping” command and the “dhcp snooping vlan” command which will remove the DHCP Snooping configuration and also flush dynamic binding entries.

A new command was also added to globally enable or disable DHCP Snooping IP Source Filtering. This decouples the IP Source Filtering functionality from the DHCP Snooping functionality. The disabling or removal of a DHCP Snooping configuration will not affect the IP Source Filtering functionality or configuration.

DHCP Snooping - Binding Table

Options added to the “show dhcp-snooping binding” command to filter the display of DHCP Snooping Binding Table entries based on port, link aggregate, and IP address. Binding table entries are also displayed in ascending order based on the associated port.

DHCP Guard Without L3 Interface (EA)

Beginning in 8.6R1 DHCP Guard is now configured on a VLAN. Previous implementeation implemented DHCP Guard on an IPv6 interface.

DHCPv6 / ISFv6 - Support for Client Guard / Guard Only Option (EA)

DHCPv6 Guard functionality is extended to optionally cover DHCPv6 client messages. If DHCPv6 Guard for client messages is enabled and trusted source ports are configured, then the client multicast messages are checked and sent out only on the trusted ports. If there are no trusted ports configured, then client messages are dropped.

DHCPv6 Relay - Support for Services and Migration to New CLI

DHCPv6 Relay enables routing of IPv6 DHCP traffic between clients and servers that are in different VLAN domains.

To enable routing of IPv6 DHCP traffic between clients and servers across service domains, it is now possible to configure a DHCPv6 relay agent for an IPv6 interface that is bound to a Shortest Path Bridging (SPB) service. This is supported only on an OmniSwitch 9900.

DHCPv6 / ISFv6 - Behavior Parity

Updates to the "dhcp-snooping binding timeout" and "dhcp-snooping binding action" commands for parity with the "dhcpv6-snooping binding timeout" and "dhcpv6-snooping binding action" commands. Also, static DHCP Snooping binding table entries take precedence over dynamic DHCP Snooping binding table entries.

IPv6 - UDP Relay

IPv6 UDP packet relay is now supported and operates in the same manner as IPv4 UDP packet relay. The generic IPv6 UDP Relay service relays packets with pre-configured destination UDP port information to destination VLANs, Shortest Path Bridging (SPB) service, or an IPv6 address

IPv6 - DHCP Snooping Binding Table for ISF

This release adds support for IPv6 Source Filtering on the OmniSwitch 6560. A new capability profile command for configuring the TCAM mode necessary to support source IPv6 filtering on these platforms has been added.

By default, the TCAM mode is set for destination IPv6 filtering; source IPv6 filtering is not allowed. When the TCAM mode is set to source IPv6 filtering, the TCAM will operate in an enhanced mode to support the use of source IPv6 conditions in QoS policy rules. When the enhanced mode is active, destination IPv6 source filtering is not allowed.

Changing the TCAM mode requires a reboot of the switch to activate the new mode.

Note: The OS6560-P48Z16 (903954-90) does not support this feature when used in a VC. This feature is supported on the newer version of the OS6560-P48Z16 (904044-90) when used in a VC.

IPv4 UDP Relay - Support for Services and Migration to new CLI

All the "ip helper" commands have been deprecated and are replaced with "ip dhcp relay" commands. For example, "ip helper forward-delay" is now "ip dhcp forward-delay". When a command using the old syntax is attempted, the switch displays an error message along with a recommendation to use the new command syntax. For example:

-> **ip helper address 20.2.2.1**

ERROR: This command is depreciated. Please use : **ip dhcp relay [interface <name>] destination <IPv4 address>**

IP Black Hole Route (Null Route)

AOS supports configuration of IP Null (Black Hole) Routes for IPv6 and IPv4 feature.

A blackhole route is used to forward unwanted traffic to a black-hole. Static routes may be created for undesirable destinations by pointing them to a NULL interface instead of valid gateway address. Any traffic that has a destination matching this undesirable destination will be dropped automatically.

PIM Messaging Packing Optimization

The current PIM implementation results in sending numerous small join/prune messages for each (*,G) and (S,G) based on a timer. With this feature enhancement, the messages will be packed so that fewer packed messages are sent in a burst versus a large number of smaller messages. Additionally, a new join/prune timer will be tracked for each upstream neighbor.

Device Profiling - OV Support

In this enhancement of IoT Device Profiling, OmniSwitch will have an interface with OmniVista in concurrence with the local Device Profiling engine running on the switch. IoT device category and device type are assigned by OmniVista, based on the information collected and sent by switches to the OmniVista Device Profiling Engine. An extended collector cumulate information from different types of packets such as DHCP option 55 / 60, HTTP Get Request and DNS queries is used in profiling of IoT devices.

Device Profiling - OS6900-V72/C32 Support

Device profiling is supported on the OS6900-V72/C32 beginning in 8.6R1.

RADIUS, TACACS, LDAP - Pre-shared Key Encryption Method

Currently the RADIUS and TACACS pre-shared keys are stored in the configuration file (vcboot.cfg) using 3DES. This enhancement will now encrypt the pre-shared keys using SHA256. Additionally, previous configurations will be decrypted with 3DES and then encrypted with SHA256 to allow for backward compatibility with configurations generated with AOS releases prior to 8.6R1.

Role-Based Authentication

This release adds support for role-based authentication to the OS6900-V72 and OS6900-C32 models.

Syslog-NG with TLS Encryption

The syslog-ng with TLS encryption layer is already supported when the common-criteria mode is enabled on the switch. This releases allows for the configuration of syslog-ng with TLS encryption outside the common-criteria mode as part of normal switch operation. The swlog can be sent to external syslog server over TLS encrypted layer. The TLS encryption can be configured using the swlog output command.

Configurable OpenSSL Cipers in Default Switch Operation

Many applications use OpenSSL to communicate. OpenSSL allows the application to select their own cipher suites (i.e. a list of cryptography algorithms which will be used for the connection establishment, key exchange and data encryption).

Most of the applications using the OpenSSL do not share common cipher suites, which make it difficult for the network administrator to know which cipher suite is used by which application.

Open SSL cipher security level configuration allows to configure common SSL cipher suites for RADIUS client, LDAP client, Captive Portal, Syslog-ng client and SNMP which are using OpenSSL.

OpenSSL cipher security level configuration provides four security levels for the network administrator to choose from. Each level specifies the strength of the cipher and indicates the minimum level of ciphers that are supported. The following security levels can be configured:

- All: Includes all the cipher suites, including NULL-SHA.
- Low: Includes all cipher suites, except NULL-SHA.
- Medium: Includes all ciphers suites except NULL-SHA, DES-CBC-SHA, and RC4-MD5.
- High: Includes only AES-256 with SHA-2 ciphers (Applicable only for TLSv1.2).

By default, the cipher security level is set to medium in default switch mode and high in common criteria mode.

Apart from the predefined cipher security level, the administrator can also define custom cipher suites as per requirement using the custom configuration.

AOS PKI x.590v3 Certs in Default Switch Operation

Applications using OpenSSL can select the public key to communicate with external servers when servers require to verify client certificate. Likewise, clients can also validate the server certificate. This prevents the spoofing attacks.

The following three public key security modes can be configured for TLS client to communicate with external servers:

- No Validation: This is the default mode, in this mode the client applications do not provide certificate and not validate server certificate.
- Server Certificate Validation: In this mode, the client application is required to provide clients certificate but the client will validate the server certificate using the pre-installed CA certificate.
- Mutual Authentication: In this mode, the client application must load their certificates and key files and provide clients certificate to server.

The applications can also limit the TLS version it uses.

The PKI feature allows to select common certificate and public key security mode and configure the TLS version for the applications (RADIUS client, LDAP client, Captive Portal, Syslog-ng client and SNMP) using OpenSSL.

SNMP over TLS

TLS encryption can be enabled for SNMP connections and SNMP traps. This enhances the security level. OmniSwitch allows to customize and configure the SNMP security requirements.

Two security models TSM and USM can be configured for SNMP traps. The security model can be configured only for SNMP version 3. The TSM security model allows to configure the TSM user with the certificate identities. The local and remote identity must be configured.

The TLS encryption can also be enabled for SNMP access on the switch. This is supported for SNMP version 3 connections only. The remote identity must be mapped to the user in TSM mode.

Ethernet Loopback Test Support

This enhancement allows for the loopback-test capability available in AOS 6.X releases to be supported on the OS6860 and OS6865 platforms.

CPE Test Head

Centralized Test Head traffic generator and analyzer (CPE) is a Test-OAM tool used in the Metro Ethernet Network to validate the customer Service Level Agreements (SLA). This is critical when a new service is provisioned in the Metro Ethernet Network and when a live service needs troubleshooting. This allows the operator to validate the Metro Ethernet Network between the end points of the customer ethernet service. Feature support is being added in this release on the OmniSwitch 6465.

Layer 2 Custom Protocol

Custom L2 protocol (OS6465) is configured globally. The configured custom L2 protocol name can be associated to a UNI profile for specific packet control for proprietary protocol with multicast MAC as well as Cisco proprietary protocols such as PGP, CDP, PVST, and DTP. The custom L2 protocol can be applied specific actions (tunnel, MAC-tunnel and discard).

Built-in UNI Profile (OS6465)

Two built-in UNI profiles IEEE-FWD-ALL and IEEE-DROP-ALL are created to forward and drop the L2 protocol control frames having a destination mac-address of 01-80-C2-00-00-XX.

- IEEE-FWD-ALL - When a UNI port is attached to this profile, all L2 protocol control frames having a destination MAC-address of 01-80-C2-00-00-XX are forwarded as normal data in hardware. The frames are forwarded without modification (i.e. no mac tunnel) .Exceptions is 01-80-C2-00-00-01 and 01-80-C2-00-00-04 (always discarded). When a tunneled L2 protocol control frames (i.e. tagged frame with SVLAN-ID) is received on NNI ports, the L2 protocol control frames is forwarded in hardware as normal data.
- IEEE-DROP-ALL - When a UNI port is attached to this profile, all L2 protocol control frames having a destination MAC-address of 01-80-C2-00-00-XX are discarded in hardware. When a tunneled L2 protocol control frames (i.e. tagged frame with SVLAN-ID) is received on NNI ports, the L2 protocol control frames is still forwarded in hardware as normal data.

MAC Forced Forwarding (Dynamic Proxy ARP)

MAC Forced Forwarding - Dynamic Proxy ARP is used to forward all traffic from Layer 2 clients to a head-end router. This head-end router filters and forwards the traffic from the local network or back to other clients in the same VLAN/IP subnet. In order to accomplish this, Dynamic Proxy ARP combines the functionality of other switch features to dynamically learn router addresses and act as a proxy for that router. Dynamic Proxy ARP - MAC Forced Forwarding uses the following features:

- Port Mapping - Port Mapping forwards traffic from user-ports only to network-ports, preventing communication between L2 clients in the same VLAN. Port mapping prevents direct communication between clients in the same VLAN forcing all traffic to be forwarded to the head end router.
- Proxy ARP - All ARP requests received on port mapping user-ports are answered with the MAC address of the head end router. Dynamic Proxy ARP dynamically learns the IP and MAC address of a head end router and responds with that router MAC address instead of flooding the ARP request.
- DHCP Snooping - Snoops the DHCP packets between the server and clients. DHCP snooping is used to dynamically learn the IP address of the head end router.

PPPoE - Intermediate Agent

PPPoE-IA is a means by which the discovery packets of PPPoE are tagged at the access switch of the service provider using Vendor Specific Attributes (VSA) to add the line-specific information at the switch. The purpose of an IA is to help service provider and the Broadband Network Gateway to distinguish between different end hosts connected over Ethernet to the access switch. The Ethernet frames from different users are appropriately tagged by the IA to provide this distinction. The AOS implementation of PPPoE-IA enables the rate limiting and insertion of VSA tags into the PPPoE Active Discovery (PAD) messages. The tag is allowed to contain information such as the base MAC address of the switch, interface, customer VLAN, system name, and a user-defined string depending on the configuration.

SAA SPB Measurements Using One-Second Intervals

Currently there is an imposed limitation to keep the total execution time to less than 10sec. The total execution time is calculated as the product of (number of packets * inter-pkt-delay). In order to allow for increased execution time with 1 second inter-pkt-delay (i.e. 60 packets), this limitation is being removed in this release.

Policy-based Mirroring - Multiple Destination Ports

This feature is extended to support multiple destination mirroring port and link aggregates per session, seven port mirroring sessions, and 128 destination mirroring ports or link aggregates on the switch. This functionality is supported on OmniSwitch 9900.

Also, supports policy based multiple destination mirroring on a single port mirroring session on OmniSwitch 9900.

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-4222	Not able to configure Source port range on an OS6900-C32.	There is no known workaround at this time.
CRAOS8X-5600	The 'show mvrp port <port-no> stats' command shows output for all ports after that port instead of that port alone.	There is no known workaround, this is a display issue only.
CRAOS8X-10420	On an OS6860 and OS6865, traffic for a HAVLAN cluster is also forwarded to the non-HAVLAN cluster port.	There is no known workaround at this time.
CRAOS8X-10570	Error messages are displayed on the console when a port is disabled on one side of a P2P connection.	Toggle the admin state of the enabled port.
CRAOS8X-11263	On a OS6465-P28 model, the mac aging value cannot be set larger than 414 seconds.	There is no known workaround at this time.
CRAOS8X-11350	Client is unable to get an IPv6 address when ISF is enabled on an intermediate switch to which the client is not directly connected.	ISF should be configured on the switch the client is connected to.
CRAOS8X-11437	The 'swlog clear' cli not clearing the event logs on the switch.	There is no known workaround at this time.

Access Guardian / UNP / Captive Portal / Security

PR	Description	Workaround
CRAOS8X-6307	With "Syslog over TLS" configured on a VC, the swlog from Slave units are not transferred to the Syslog server over TLS.	Ensure the Syslog server is directly reachable from all Master/Slave units of a VC via the EMP or other management ports.
CRAOS8X-6308	On an OS9900 when Syslog over TLS is configured, the CMM host swlog and the NI swlogs are not sent to the external syslog server over TLS.	There is no known workaround at this time.
CRAOS8X-8078	The routerauth users that are supposed to get deleted after the session timeout expiry – 5 mins(300 seconds) are not getting deleted. This is seen only on an OS9900 and is specific to routerauth users only.	Use the command 'unp router-auth user flush'.
CRAOS8X-10303	If UNP users are learned in the auth-server-down profile due to the RADIUS server being unreachable, when the server becomes reachable even if failover is enabled, the users don't move out of the auth-server-down profile.	There is no known workaround at this time.

CRAOS8X-11719	Description: When admin configures the captive-portal name as https://captive-portal.com the CLI internally creates a webserver config file which also prepends https:// to the configured string as a result in the webserver configuration file the configured captive-portal name is written as https://https://captive-portal.com and the web server fails to start with a config file parsing error.	Use the command without https:// since CLI internally creates a webserver config file which also prepends https:// to the configured string.
CRAOS8X-11720	Captive portal internal DHCP mode is not functional.	There is no known workaround at this time.

Hardware

PR	Description	Workaround
CRAOS8X-3334	On an OS6900-V72, intermittent CRCs may temporarily occur when performing an abrupt/fast hot-swap of SFP-10G-SR/LR/ER.	Allow a small of time between removal and insertion when performing a hot-swap.
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	1M and 3M DAC are not supported on the OS6560-X10 port 1-8 and the OS6560-48X4/P48X4 ports 53 and 54.	Use a different transceiver type.
CRAOS8X-8020	On an OS99-XNI-UP24Q2/OSXNI-U12Q a link up delay of several minutes or longer is observed when NI is powered up at -5C or 0C ambient on ports 9 - 12.	There is no known workaround at this time.
CRAOS8X-8231	OS99-XNI-UP24Q2/OS99-XNI-U12Q: Link up delay of several minutes or longer observed when NI is powered up at -5C or 0C ambient on the first QSFP port (port 25 on UP24Q2 and port 13 on U12Q).	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	There is no known workaround at this time.

	oversubscribed with max Egress-bandwidth.	
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 at this time. Happens only at very low bandwidth settings on 10G ports.
CRAOS8X-4424	With color-only policy action configured, egress queues are not honiring the color marking and packet drop is observed and expected traffic rate is not achieved.	There is no known workaround at this time.
CRAOS8X-6003	QoS policy condition with VxLAN tunnel IP is currently not supported.	There is no known workaround at this time.
CRAOS8X-9961	QoS drop not working on igmp packekts with multicast keyword on policy condition.	There is no known workaround at this time
CRAOS8X-10498	"qos port 1/1/3 maximum ingress-bandwidth 80M" doesn't work after vc-takeover and reload because it gets overwritten by default ingress-bandwidth of a port.	Configure ingress-bandwidth through "interfaces port c/s/p ingress-bandwidth mbps <num> burst <num>" instead of "qos port c/s/p maximum ingress-bandwidth <num>".

Service Related

PR	Description	Workaround
CRAOS8X-3941	Sometimes 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-4124	Traffic is not tunneled over L2GRE service when sending traffic from edge to aggregate switch via another edge switch where SAP/loopback port on aggregate switch is configured as static linkagg.	There is no known workaround at this time.
CRAOS8X-5354	User defined VXLAN UDP port for default VRF is currently 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 'service sdp <num> vxlan ttl <num>.
CRAOS8X-6255	IPMS over services does not currently work with proxying.	There is no known workaround at this time.
CRAOS8X-7428	IPMS Proxy is not supported on a service.	There is no known workaround at this time.
CRAOS8X-9958	DHCP packets from LINKAGG UNP to SAP Port is getting dropped .	There is no known workaround at this time.

Virtual Chassis

PR	Description	Workaround
CRAOS8X-914	Sometimes after a VC-takeover, one of the users that was learned in blocking on UNP access linkagg is getting flushed though the mac-aging timer has not expired.	There is no known workaround at this time.
CRAOS8X-3877	On 6900 and 6900V72, untagged packets are mirrored as tagged traffic when when monitored port is across VC chassis. On standalone box, monitored egress traffic is tagged.	Use port mirroring.

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.

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
OS99-XNI-U12Q	OS99-XNI-U12Q
OS99-XNI-UP24Q2	OS99-XNI-UP24Q2

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.
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: 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 8.6R1.

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								
Apple Netboot Support with DHCP Snooping or Relay	8.5R4	8.5R4	8.5R4	8.5R4	8.5R4	8.5R4	8.5R4	
AOS Micro Services (AMS)	8.6R1	8.6R1	8.6R1	8.6R1	8.6R1	8.6R1	8.6R1	
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	
Dying Gasp	Y	Y	Y	Y	N	N	N	
Dying Gasp (EFM OAM / Link OAM)	8.6R1	8.6R1	8.6R1	8.6R1	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	
In-Band Management over SPB	N	N	8.5R4	8.5R4	8.5R4	8.5R4	8.5R4	
ISSU	N	N	Y	Y	Y	8.5R2	Y	
NAPALM Support	8.5R1	8.5R1	8.5R1	8.5R1	8.5R1	N	N	
NTP - Version 4.2.8.p11.	8.5R4	8.5R4	8.5R4	8.5R4	8.5R4	8.5R4	8.5R4	
OpenFlow	N	N	Y	N	Y	N	N	
OV Cirrus – Zero touch provisioning	Y	Y	Y	Y	Y	N	N	
OV Cirrus - Configurable NAS Address	8.5R4	8.5R4	8.5R4	8.5R4	8.5R4	8.5R4	8.5R4	
OV Cirrus - Default Admin Password Change	8.5R4	8.5R4	8.5R4	8.5R4	8.5R4	8.5R4	8.5R4	
OV Cirrus - OS6900-C32/V72 Managed	8.5R4	8.5R4	8.5R4	8.5R4	8.5R4	8.5R4	8.5R4	
Readable Event Log	8.6R1	8.6R1	8.6R1	8.6R1	8.6R1	8.6R1	8.6R1	
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	

Feature	6465	6560	6860(E)	6865	6900	6900-V72/C32	9900	Notes
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 supports 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	
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	8.6R1	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	8.6R1	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	
IPv4/IPv6 Blackhole Route (Null)	8.6R1	8.6R1	8.6R1	8.6R1	8.6R1	8.6R1	8.6R1	

Feature	6465	6560	6860(E)	6865	6900	6900-V72/C32	9900	Notes
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	8.6R1	8.6R1	8.5R3	8.5R4	N	N	N	
IPv6 - Source filtering	N	8.6R1	8.5R3	8.5R4	N	N	N	
IPv6 - DHCP Guard	EA	EA	EA	EA	N	N	N	
IPv6 - DHCP Client Guard	EA	EA	EA	EA	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	
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)	8.6R1	8.6R1	8.6R1	8.6R	8.6R1	8.6R1	8.6R1	
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	
PIM Message Packing	N	N	8.6R1	N	8.6R1	8.6R1	N	
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	

Feature	6465	6560	6860(E)	6865	6900	6900-V72/C32	9900	Notes
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	
Loopback detection – Edge (Bridge)	8.5R1	Y	Y	Y	N	N	Y	
Loopback detection – SAP (Access)	N	N	Y	Y	Y	N	EA	
MAC Forced Forwarding	N	N	8.6R1	8.6R1	N	N	N	
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	
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	
STP - TCN Dampening/Duplicate Handling	8.5R4	8.5R4	8.5R4	8.5R4	8.5R4	8.5R4	8.5R4	
MVRP	8.5R1	Y	Y	Y	Y	8.5R4	Y	
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	

Feature	6465	6560	6860(E)	6865	6900	6900-V72/C32	9900	Notes
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								
CPE Test Head	8.6R1	N	N	N	N	N	N	
Ethernet Loopback Test	N	N	8.6R1	8.6R1	N	N	N	
Ethernet Services (VLAN Stacking)	8.5R1	N	Y	Y	Y	8.5R4	N	
Ethernet OAM (ITU Y1731 and 802.1ag)	8.5R1	N	Y	Y	Y	N	EA	
EFM OAM / Link OAM (802.3ah)	8.6R1	8.6R1	8.5R4	8.5R4	N	N	N	
PPPoE Intermediate Agent	8.6R1	N	N	8.6R1	N	N	N	
1588v2 End-to-End Transparent Clock	8.5R1	N	Y	Y	Y (X72/Q32)	N	N	
1588v2 Peer-to-Peer Transparent Clock	8.6R1	N	N	N	N	N	N	
1588v2 Across VC	N	N	N	N	8.5R2 (X72)	N	N	
Access Guardian / 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	8.6R1	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	

Feature	6465	6560	6860(E)	6865	6900	6900-V72/C32	9900	Notes
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	
Critical Voice VLAN	EA	N	N	N	N	N	N	
IoT Device Profiling	8.5R2	8.5R2	8.5R2	8.5R2	8.5R2	8.6R1	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 (Edge) (bridge ports)	N	Y	Y	Y	8.6R1	N	Y	OS6900-Q32/X72
L2 GRE Tunnel Access (Edge) (access ports)	N	N	8.6R1	8.6R1	8.6R1	N	8.6R1	OS6900-Q32/X72
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	8.6R1	8.6R1	8.6R1	8.6R1	8.5R3	8.6R1	8.6R1	
LLDP	8.5R1	Y	Y	Y	Y	8.5R2	Y	
MACsec	8.5R1	8.5R4	Y	N	N	N	8.5R2	Site license in 8.6R1
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	
RADIUS - RFC-2868 Support	8.5R4	8.5R4	8.5R4	8.5R4	8.5R4	8.5R4	8.5R4	
Role-based Authentication for Routed Domains	N	N	8.5R4	8.5R4	8.5R4	8.6R1	8.5R4	
Storm Control	N	N	Y	Y	Y	N	N	
TACACS+ Client	8.5R1	Y	Y	Y	Y	8.6R1	Y	
TACACS+ command based authorization	N	N	Y	Y	Y	N	N	
UNP Access Mode (SPB/VXLAN) for Silent Devices	N	N	8.5R4	8.5R4	8.5R4	8.5R4	8.5R4	
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	

Feature	**6465**	**6560**	**6860(E)**	**6865**	**6900**	**6900-V72/C32**	**9900**	**Notes**
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 (License Required)								
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	8.6R1
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	8.6R1	8.6R1	8.6R1	8.6R1	8.6R1
UDP Relay	8.6R1	8.6R1	8.6R1	8.6R1	8.6R1
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 8.6R1 (GA)
OS6465	8.5.164.R01 (GA) 8.5.255.R02 (GA) 8.5.54.R03 (GA) 8.5.196.R04 (GA)
OS6560	8.5.196.R04 (GA)
OS6860(E)	8.4.1.141.R03 (GA) 8.5.164.R01 (GA) 8.5.255.R02 (GA) 8.5.54.R03 (GA) 8.5.196.R04 (GA)
OS6865	8.4.1.141.R03 (GA) 8.5.164.R01 (GA) 8.5.255.R02 (GA) 8.5.196.R04 (GA)
OS6900	8.4.1.141.R03 (GA) 8.5.164.R01 (GA) 8.5.255.R02 (GA) 8.5.54.R03 (GA) 8.5.196.R04 (GA)
OS9900	8.4.1.229.R02 (GA) 8.4.1.141.R03 (GA) 8.5.255.R02 (GA) 8.5.54.R03 (GA) 8.5.199.R04 (GA) **Note:** ISSU on a VC of 1 OS9900 is only supported from 8.5R2 and above.

8.6R1 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           8.6.285.R01            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 (V72/C32 – Yos.img)

  Note: When performing an ISSU upgrade on an OS6900-V72/C32 from the 8.5R2 GA Release the following error is displayed on the console. This is a display issue only, the upgrade will be completed successfully. For example:

```
6900-V72-VC-2-> issu from issu
Are you sure you want an In Service System Upgrade? (Y/N) : y
md5sum: can't open '/flash/issu/Tos.img': No such file or directory
sh: 9260: unknown operand
sh: 9260: unknown operand
```

- 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           8.6.285.R01
```

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 8.6R1 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_6285

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_6285
Parse /flash/fpga_kit_6285
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
Case: **00349405** *CRAOS8X-6370*	**Summary:** MAC Sec operational status inaccurate in dynamic mode. **Explanation:** CLI command “show interfaces macsec dynamic” returns Operational Status UP whereas MAC Sec link is not established. 🔒 Click for Additional Information
Case: **00351693** *CRAOS8X-6381*	**Summary:** OS6860/6860E/6900: Support for syslog and port number used. **Explanation:** syslog communication uses UDP port number 514. When the option to use TCP has been enabled in the syslog server, the communication has been failed with improper TCP handshake. Fix has been issued in the AOS 8.6R01 release, where syslog communication follows RFC 5425. 🔒 Click for Additional Information
Case: **00342928** *CRAOS8X-7144*	**Summary:** Spanning tree BPDUs with multicast root bridge MAC address are accepted in AOS switches **Explanation:** Code changes are done to validate the Designate Bridge MAC as non-multicast MAC in received BPDU before processing it. Dropping such BPDUs with DESG MAC as multicast MAC(01:XX:XX) instead of processing further. 🔒 Click for Additional Information
Case: **00357743** *CRAOS8X-7248*	**Summary:** OS9900: Intermittent ping loss noticed to the uplink IP addresses. **Explanation:** ARP requests are forwarded to every port including the STP blocking port and any replies to these ARP requests too forwarded to that blocking port which would drop the traffic. Bug has been fixed under 8.6R01. 🔒 Click for Additional Information
Case: **00360736** *CRAOS8X-7253*	**Summary:** OS6900: Multiple linkaggs on core are toggling **Explanation:**

	Noticed a specific static linkagg port was in a Down state, however operational status shown as UP, for that reason, all the packets got drop instead of passing through the secondary link of the same Agg. Fix will be available in 8.6R01. 🔒 Click for Additional Information
Case: **00363458** *CRAOS8X-7595*	**Summary:** OS6900: In swlog "No organizational unit named bop-logging" message is printed continuously. **Explanation:** Switch enabled with accounting session is expecting OU (Organizational Unit) in accounting response from OV2500 which is configured as LDAP server. The OU name cannot be created in OV as this feature is not available. Switch is not receiving the OU from OV2500 and hence printing "No organizational unit named bop-logging". The changes have been made in AOS 8.6R01 to not print the "bop-logging" message in swlog. 🔒 Click for Additional Information
Case: **00363001** *CRAOS8X-7764*	**Summary:** OS6900 Stale SVP entries and connectivity issues in SPB network. **Explanation:** SVC NI errors are seen in the swlogs. The errors are seen due to leak of stats index which in turn causes SVP mismatch in SPB. 🔒 Click for Additional Information
Case: **00360587** *CRAOS8X-7872*	**Summary:** OS9907 PS LED color on CMM is solid Amber. **Explanation:** When OS9900 runs with a non-fully loaded power supplies, the PS LED color turns to Solid Yellow. The observed problem has been determined as a bug and fixed the behavior of PS LED color to lit Solid Green with non-fully loaded power supplies. The issue is fixed in AOS 8.6R01. 🔒 Click for Additional Information
Case: **00369684** *CRAOS8X-8103*	**Summary:** Accounting tab is not displaying for the users connected to OS6860 switch in the clearpass server. **Explanation:** Clearpass serve sends the class 25 attribute in the Access-Accept packet to be used in the Accounting-Request packet by the switch. Switch is modifying the class 25 attribute when sending the Accounting-Request packet to the clearpass server, which is causing the clearpass to ignore the class 25 attribute and thus not displaying the Accounting tab for the users connected to the OS6860 switch. 🔒 Click for Additional Information

Case: **00365597** *CRAOS8X-8342*	**Summary:** Switch crashed with error SIP CMM task due to segmentation fault. **Explanation:** The virtual chassis rebooted without any manipulation on the switch. PMD files were generated. From the PMD file, there was a segmentation fault triggered when QOS messages are processed through sip. The sip dialogs/transactions are invalid at times due to corrupted packets from the media. Issue has been fixed under 8.6R01. 🔒 Click for Additional Information
Case: **00358640** *CRAOS8X-8385*	**Summary:** OS6900 : Switch uses incorrect IP interface to forward DHCP discover packet when PXE support is enabled. **Explanation:** The issue was due to incorrect socket ID for UDP relay was returned. 🔒 Click for Additional Information
Case: **00370262** *CRAOS8X-8413*	**Summary:** OS6860 switch crashes when PTP packet is received. **Explanation:** Since PTP packet is a multicast packet, it is being processed by CPU even though PTP is disabled on the switch. When this PTP packet is handled by CPU, PTP packet's offset is calculated incorrectly. This causes the switch to crash every time a PTP packet is received. Bug fixed in 8.6R01. 🔒 Click for Additional Information
Case: **00371582** *CRAOS8X-8446*	**Summary:** OS6860: User profile is not changing with Internal captive portal. **Explanation:** User profile information are unchanged during CP authentication. Fix has been issued in AOS 8.6R01 and profiles will be changed as per the stages of Captive portal authentication. 🔒 Click for Additional Information
Case: **00373466** *CRAOS8X-8468*	**Summary:** OS6560: On PALM, slave chassis firmware information was not seen. **Explanation:** On PALM Operating System Version, the Software Version of the slave chassis is not present in json file, hence unable to display operating system information. As from AOS Release 8.6R01, Software Version of the slave chassis is included in json file. 🔒 Click for Additional Information

Case: **00370061** *CRAOS8X-8548*	**Summary:** EEE configuration causing vcboot.cfg.err after reboot. **Explanation:** When EEE is enabled in OS6865, it is working fine, however, after rebooting the switch vcboot.cfg.err file is created containing error "EEE configure auto negotiation Failed". Even though vcboot.cfg.err is generated, EEE is properly configured in the respective port. This behavior has been changed in AOS Release 8.6R01 to prevent the EEE configuration to generate a "vcboot.cfg.err" file after VC reboot. 🔒 Click for Additional Information
Case: **00374849** **00379577** **00380788** **00375691** *CRAOS8X-8777*	**Summary:** OS6900-T40 is generating the ChassisSupervisor, vcmCmm chas_sup, vcmNi port_mgr appid's info logs after upgrading the chassis from 7.3.4.248 R02 to 8.5.196 R04. **Explanation:** In code 8.5 R04, event is sent to all registered application in every 10 to 20 sec. Hence the logs (with ChassisSupervisor, vcmCmm chas_sup, vcmNi port_mgr appid's) are seen continuously in swlog after upgrade to 8.5 R04. The above event's log printing mechanism has been suppressed under 8.6R01. 🔒 **Click for Additional Information**
Case: **003763654** *CRAOS8X-8824*	**Summary:** OS6900: Getting svcCmm mVXLN ERR messages in swlog. **Explanation:** Below error messages are seen continuously on a OS6900 X72 (Standalone) which was upgraded from 8.5.R02 to 8.5.R04, however no impact on switch. -> swlogd svcCmm mVXLN ERR: smgrProcessVxlanPkt@1380 Not Valid UDP Port 7.The b ug has be fixed in 8.6R01. 🔒 Click for Additional Information
Case: **00373466** *CRAOS8X-8468*	**Summary:** PALM – Virtual Chassis AOS 8.x – Software Version missing for slave chassis. **Explanation:** PALM doesn’t display the Operating System Version of the slave chassis because the baseSoftwareVersion is not sent by switch. 🔒 Click for Additional Information
Case: **00375128** *CRAOS8X-8844*	**Summary:** Tunnel-attributes (VLAN) returned from CPPM for the 802.1x clients are not taking effect in 6860. **Explanation:** On OS6860, the UNP Ports are moved to default vlan instead of returned vlan via tunnel-attributes from the CPPM. The issue is due to error in decoding values of Tunnel-Attributes.

	Code changes done to decode the values correctly by the OmniSwitch, which helps to make the 802.1x client ports to forward in the VLAN (tunnel-attribute) returned by the CPPM after successful authentication from AOS.8.6.R01 and above. 🔒 Click for Additional Information
Case: **00378953** *CRAOS8X-9178*	**Summary:** OS9900: VC Split is noticed upon CMM takeover. **Explanation:** The issue is caused by internal communication problem between the CMM modules. The fix is available in 8.6 R01. 🔒 Click for Additional Information
Case: **00380094** *CRAOS8X-9494*	**Summary:** OS9900: VRRP state on BACKUP switch changes to MASTER when primary CMM is removed and reinserted. **Explanation:** The toggle event is due to advertisement interval being set in VRRP. The VRRP advertisement packet is not sent to VRRP Backup switch due to which "vrrpMasterDownTimer" event happened and VRRP is getting toggled. 🔒 Click for Additional Information
Case: **00382083** *CRAOS8X-9658*	**Summary:** How to configure Ethernet-OAM on AOS 8.x switches. **Explanation:** In the AOS 8.x documentation are missing some configuration steps in order to set up an Ethernet OAM Maintenance End Point. 🔒 Click for Additional Information
Case: **00382558** *CRAOS8X-9755*	**Summary:** The OS6860 switch crashes and generating PMD file, when configuring auth type key-chain for the OSPF interface. **Explanation:** The crash happened due to ENDIANNESS problem in the AOS codes 8.4.1.141.R03/8.5.196.R04. To correct ENDIANNESS problem, the byte order has to be changed. Since fix involves byte order change, there is no workaround for the current AOS microcode releases. 🔒 Click for Additional Information
Case: **00387294** *CRAOS8X-10300*	**Summary:** OS9900: CMM-A not able to join the chassis when the chassis is with one CFM. **Explanation:**

	Using OS9900, CMM-A was not joining where chassis is having only one CFM (CFM-B) and CMM-B along with Ni modules. The observed issue has been determined as bug. 🔒 Click for Additional Information
Case: **00388435** *CRAOS8X-10657*	**Summary:** OS6900-Mac Learning issue on a SAP port. **Explanation:** The OS6900VC(SPB-BEB) was not learning MAC address on a SAP port. Network connectivity broken and impacted SPB services. Stale VP is created by service stats leak. In this case, the new created VP was not carrying traffic. Bug has been fixed under 8.6R01. 🔒 Click for Additional Information
Case: **00382432** *CRAOS8X-10079*	**Summary:** In a VC of OS6900-V72 switches, VFL links connected using 10 GIG DAC cable, do not come UP if the cables are removed and reconnected again physically. **Explanation:** In OS6900 V72 even port 1-48 has splitter information. When the cables are unplugged and re-plugged, This VFL ports splitter mode from Slave Ether NI is not updated in Master Ether CMM hence the VFL link remains down. Issue is fixed in 8.6 R01. 🔒 Click for Additional Information
Case: **00386777** *CRAOS8X-10312*	**Summary:** OS9900: Momentary high CPU on OS9907 for portmgrcmm task with CMM-A not joining the chassis. **Explanation:** An upgrade (by reload), from 8.4.1R03 to 8.5R04 on a dual CMM OS9907 chassis failed because CMMA kept rebooting. Issue has been fixed under 8.6R01. 🔒 Click for Additional Information
Case: **00388058** *CRAOS8X-10432*	**Summary:** SPB: Ping between 2 non adjacent SPB switches did not work. **Explanation:** Ping between 2 non adjacent SPB switches(switch 1 to switch 3) did not work even though the ping between switch 2 to switch 3 was working. Issue has been fixed under 8.6R01. 🔒 Click for Additional Information
Case: **00389263** *CRAOS8X-10562*	**Summary:** OS6860: Need a command to enable AP-MODE on per port basis. **Explanation:** In 8.5 R01 AP-mode can be enabled only globally. The command is introduced in 8.6 R01 to enable this on per port.

	🔒 Click for Additional Information
Case: **00389847** *CRAOS8X-10838*	**Summary:** OS9900: Command “Show policy network group Switch “ output is missing few IP interface on the switch. **Explanation:** This is a bug and is fixed in 8.6 R01. 🔒 Click for Additional Information
Case: **00390278** *CRAOS8X-11036*	**Summary:** OS6865: IP PIM DENSE mode is dropping flows after link takeover. **Explanation:** As soon as link between OS6865 and OS9702 breaks, OS6865 would send craft message to all PIM-DM neighbors in order to reform the SPF table. In this scenario, OS6865 sending the craft message to OS6855, however due to bug in the code the internal context is not getting cleared/updated, hence OS6855's response is not getting treated which led to traffic drop due to link takeover. Bug has been fixed in 8.6R01. 🔒 Click for Additional Information