Release Notes - Rev. F

OmniSwitch 6465, 6560, 6860(E), 6860N, 6865, 6900, 6900-V72/C32, 6900-X48C6/T48C6, 9900

Release 8.7R1

These release notes accompany release 8.7R1. 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.

Note - The original 8.7R1 GA release (8.7.277.R01) contains an SNMP memory leak issue when using net-snmp-5.8 version (CRAOS8X-21451). The issue has been fixed in this 8.7R01 release (8.7.354.R01) by reverting to net-snmp-5.7.3 version. This release also adds support for the OS6560, OS6860N-U28, OS68-QNI-U2 and OS9900.

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 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
OS6860N	4GB	32GB
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
OS6900-X48C6/T48C6	16GB	32GB
OS9900	16GB	2GB

U-Boot 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 U-Boot or FPGA upgrades but it's recommended to upgrade to the current verson to address any known issues. Use the '**show hardware-info**' command to determine the current versions.

Switches not running the minimum version required should upgrade to the latest U-Boot 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 8.7.354.R01 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6465-P6	8.5.83.R01	8.5.83.R01	0.10	0.10
OS6465-P12	8.5.83.R01	8.5.83.R01	0.10	0.10
OS6465-P28	8.5.89.R02	8.5.89.R02	0.5	0.7*
OS6465T-12	8.6.117.R01	8.6.117.R01	0.4	0.4
OS6465T-P12	8.6.117.R01	8.6.117.R01	0.4	0.4
*FPGA version 0.7 is optional to address issue CRAOS8X-12042.				

OmniSwitch 6560 – AOS Release 8.7.354.R01 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6560-24Z24	8.5.22.R01	8.5.22.R01	0.7	0.7

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6560-P24Z24	8.4.1.23.R02	8.4.1.23.R02	0.6	0.7*
OS6560-24Z8	8.5.22.R01	8.5.22.R01	0.7	0.7
OS6560-P24Z8	8.4.1.23.R02	8.4.1.23.R02	0.6	0.7*
OS6560-24X4	8.5.89.R02	8.5.89.R02	0.4	0.4
OS6560-P24X4	8.5.89.R02	8.5.89.R02	0.4	0.4
OS6560-P48Z16 (903954-90)	8.4.1.23.R02	8.4.1.23.R02	0.6	0.7*
OS6560-P48Z16 (904044-90)	8.5.97.R04	8.5.97.R04	0.3	0.6**
OS6560-48X4	8.5.97.R04	8.5.97.R04	0.4	0.7**
OS6560-P48X4	8.5.97.R04	8.5.97.R04	0.4	0.7**
OS6560-X10	8.5.97.R04	8.5.97.R04	0.5	0.8**
*FPGA version 0.7 is only required to address issue CRAOS8X-7207. **FPGA versions are required to address issue CRAOS8X-16452.				

OmniSwitch 6860(E) – AOS Release 8.7.354.R01 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6860/OS6860E (except U28)	8.1.1.70.R01	8.7.74.R01	0.9	0.10*
OS6860E-U28	8.1.1.70.R01		0.20	0.20
OS6860E-P24Z8	8.4.1.17.R01		0.5	0.7*
*FPGA versions 7 and 10 are optional on the PoE models for the fast and perpetual PoE feature support.				

OmniSwitch 6860N – AOS Release 8.7.354.R01 (GA)

Hardware	Minimum ONIE	Current ONIE	Minimum FPGA	Current FPGA
OS6860N-U28	2019.05.00.10	2019.05.00.10	12	12
OS6860N-P48Z			12	12
OS6860N-P48M			11	11
Note: These models use the **Uosn.img** image file.				

OmniSwitch 6865 – AOS Release 8.7.354.R01 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6865-P16X	8.3.1.125.R01	8.3.1.125.R01	0.20	0.25*

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6865-U12X	8.4.1.17.R01	8.4.1.17.R01	0.23	0.25*
OS6865-U28X	8.4.1.17.R01	8.4.1.17.R01	0.11	0.14*
*FPGA versions 0.25 and 0.14 are only required for the fast and perpetual PoE feature support. **Note**: CRAOS8X-4150 for the OS6865-U28X was fixed with FPGA version 0.12 and higher.				

OmniSwitch 6900-X20/X40 – AOS Release 8.7.354.R01 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
CMM (if XNI-U12E support is not needed)	7.2.1.266.R02	7.2.1.266.R02	1.3.0/1.2.0	1.3.0/2.2.0
CMM (if XNI-U12E support is needed)	7.2.1.266.R02	7.2.1.266.R02	1.3.0/2.2.0	1.3.0/2.2.0

OmniSwitch 6900-T20/T40 – AOS Release 8.7.354.R01 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
CMM (if XNI-U12E support is not needed)	7.3.2.134.R01	7.3.2.134.R01	1.4.0/0.0.0	1.6.0/0.0.0
CMM (if XNI-U12E support is needed)	7.3.2.134.R01	7.3.2.134.R01	1.6.0/0.0.0	1.6.0/0.0.0

OmniSwitch 6900-Q32 – AOS Release 8.7.354.R01 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
CMM	7.3.4.277.R01	7.3.4.277.R01	0.1.8	0.1.8

OmniSwitch 6900-X72 – AOS Release 8.7.354.R01 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
CMM	7.3.4.31.R02	8.6.189.R02*	0.1.10	0.1.11*
*FPGA version 0.1.11 and U-boot version 8.6.189.R02 are only required to address CRAOS8X-11118.				

OmniSwitch 6900-V72/C32 – AOS Release 8.7.354.R01 (GA)

Hardware	Minimum ONIE	Current ONIE	Minimum CPLD	Current CPLD
OS6900-V72	2017.08.00.01	2017.08.00.01	CPLD 1 – 0x5 CPLD 2 - 0x6 CPLD 3 – 0x8	CPLD 1 – 0x5 CPLD 2 - 0x6 CPLD 3 – 0x8
OS6900-C32	2016.08.00.03	2016.08.00.03	CPLD 1 – 0xA CPLD 2 – 0xB CPLD 3 – 0xB	CPLD 1 – 0xA CPLD 2 – 0xB CPLD 3 – 0xB
Note: These models use the **Yos.img** image file.				

OmniSwitch 6900-X48C6/T48C6– AOS Release 8.7.354.R01 (GA)

Hardware	Minimum ONIE	Current ONIE	Minimum CPLD	Current CPLD
OS6900-X48C6	2019.08.00.01	2019.08.00.01	CPLD 1 – 0x2 CPLD 2 - 0x2 CPLD 3 – 0x2	CPLD 1 – 0x2 CPLD 2 - 0x2 CPLD 3 – 0x2
OS6900-T48C6	2019.08.00.01	2019.08.00.01	CPLD 1 – 0x2 CPLD 2 – 0x2 CPLD 3 – 0x4	CPLD 1 – 0x2 CPLD 2 – 0x2 CPLD 3 – 0x4
Note: These models use the **Yos.img** image file.				

OmniSwitch 9900 – AOS Release 8.7.354.R01 (GA)

Hardware	Minimum Coreboot-uboot	Current Coreboot-uboot	Mimimun Control FPGA	Current Control FPGA	Minimum/ Current Power FPGA
OS99-CMM	8.3.1.103.R01	8.3.1.103.R01	2.3.0	2.3.0	0.8
OS9907-CFM	8.3.1.103.R01	8.3.1.103.R01	-	-	-
OS99-GNI-48	8.3.1.103.R01	8.3.1.103.R01	1.2.4	1.2.4	0.9
OS99-GNI-P48	8.3.1.103.R01	8.3.1.103.R01	1.2.4	1.2.4	0.9
OS99-XNI-48 (903753-90)	8.3.1.103.R01	8.3.1.103.R01	1.3.0	1.3.0	0.6
OS99-XNI-48 (904049-90)	8.6.261.R01	8.6.261.R01	1.4.0	1.4.0	0.7
OS99-XNI-U48 (903723-90)	8.3.1.103.R01	8.3.1.103.R01	2.9.0	2.9.0	0.8
OS99-XNI-U48 (904047-90)	8.6.261.R01	8.6.261.R01	2.10.0	2.10.0	0.8
OS99-GNI-U48	8.4.1.166.R01	8.4.1.166.R01	0.3.0	0.3.0	0.2
OS99-CNI-U8	8.4.1.20.R03	8.4.1.20.R03	1.7	1.7	N/A
OS99-XNI-P48Z16	8.4.1.20.R03	8.4.1.20.R03	1.4	1.4	0.6
OS99-XNI-U24	8.5.76.R04	8.5.76.R04	1.0	2.9.0	0.8

Hardware	Minimum Coreboot-uboot	Current Coreboot-uboot	Mimimun Control FPGA	Current Control FPGA	Minimum/ Current Power FPGA
OS99-XNI-P24Z8	8.5.76.R04	8.5.76.R04	1.1	1.4.0	0.7
OS99-XNI-U12Q	8.6.117.R01	8.6.117.R01	1.5.0	1.5.0	N/A
OS99-XNI-UP24Q2	8.6.117.R01	8.6.117.R01	1.5.0	1.5.0	N/A

[IMPORTANT] *MUST READ*: AOS Release 8.7R1 Prerequisites and Deployment Information

General Information

- 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. Oversized frames will not be dropped on ingress of ports 1-32 (CRAOS8X-20939).

Note: OS6560-P48Z16 (904044-90) - This is a new version of the OS6560-P48Z16 which does not have the limitations 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.

- 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.

- 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.

- SHA-1 Algorithm - Chosen-prefix attacks against the SHA-1 algorithm are becoming easier for an attacker[1]. For this reason, we will be disabling the "ssh-rsa" public key signature algorithm by default in an upcoming AOS release. The better alternatives include:

  - The RFC8332 RSA SHA-2 signature algorithms rsa-sha2-256/512. These algorithms have the advantage of using the same key type as "ssh-rsa" but use the safer SHA-2 hash algorithms. RSA SHA-2 is enabled in AOS.
  - The RFC5656 ECDSA algorithms: ecdsa-sha2-nistp256/384/521. These algorithms are supported in AOS by default.

  To check whether a server is using the weak ssh-rsa public key algorithm, for host authentication, try to connect to it after disabling the ssh-rsa algorithm from ssh(1)'s allowed list using the command below:

  ```
  -> ssh strong-hmacs enable
  ```

  If the host key verification fails and no other supported host key types are available, the server software on that host should be upgraded.

  1. "SHA-1 is a Shambles: First Chosen-Prefix Collision on SHA-1 and Application to the PGP Web of Trust" Leurent, G and Peyrin, T (2020) https://eprint.iacr.org/2020/014.pdf

- With the continuous goal of preserving the environment in addition to the AOS software being preloaded on the switch and available on the Business Portal, we have begun removing the software access card previously included in the switch ship kit. For additional information or if in need of special assistance, please contact Service & Support.

Deprecated Features / Functionality Changes

The following table lists deprecated features and key functionality changes by release.

AOS Release 8.5R4
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.
NTP - 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
AOS Release 8.6R1
DHCPv6 Guard - Configuration via an IPv6 interface name is deprecated in 8.6.R1. 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.
IP Helper - The 'ip helper' commands have been deprecated in 8.6R1 and replaced with 'ip dhcp relay'. The old format will still be accepted if present in a vcboot.cfg to preserve backwards compatibility.
SAA - 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. CRAOS8X-7910 was resolved in 8.6R1.
AOS Release 8.6R2
Distributed ARP - Beginning 8.6R2 distributed ARP is no longer supported.
WRED - Beginning in 8.6R2 WRED is no longer supported.
QoS - Beginning in 8.6R2 the 'qos dscp-table' command is no longer supported.
NTP - The ntp parameter for the 'ip service source-ip' command was deprecated in 8.5R4. Support has been added back in 8.6R2.
AOS Release 8.7R1
MACsec - Static mode is not supported on OS6860N.
Transceivers - Beginning in AOS release 8.7R1 an error message will be displayed when the unsupported QSFP-4X25G-C transceiver is inserted on an OS99-CNI-U8 module.
SPB - Beginning in 8.7.R01 the default number of BVLANs created via Auto Fabric is reduced from 16 to 4. This new default value is only applicable to factory default switches running 8.7R1 with no vcboot.cfg file. Upgrading to 8.7.R1 will not change the number of configured BVLANs in an existing configuration. See Appendix B for additional information.
Quarantine Manager (QMR) - The number of allowed exception IP networks supported for remediation servers has been changed from 3 to 2 beginning in 8.7R1. For the OS6465, the supported servers is 1.

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, including the OS6900-V72/C32, do not support these Data Center features.	

	License Required				
	OS6465	OS6560	OS6860	OS6860N	OS9900
Licensed Features					
MACsec (OS-SW-MACSEC)	Yes	Yes	Yes	Yes	Yes
10G support (OS6560-SW-PERF)	No	Yes*	No	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.					

ALE Secure Diversified Code

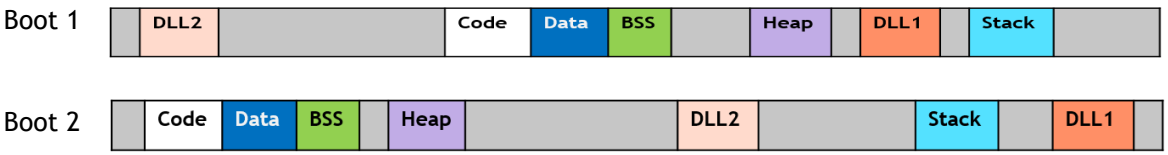
Alcatel-Lucent Enterprise provides network equipment that is hardened in conjunction with an independent 3rd party organization. ALE secure diversified code promotes security and assurance at the network device level using independent verification and validation of source code and software diversification to prevent exploitation. OmniSwitch products can also be delivered that are TAA Country of Origin USA compliant with AOS software loaded from US based servers onto the OmniSwitch in a US factory. This is the default operation of AOS, there is no charge or additional licensing required.

ALE secure diversified code 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 rearranges the memory map of the executable program so that various instances of the same software, while functionally identical, are arranged differently in memory. In AOS 8.6.R01, ALE has adopted address system layout randomization(ASLR) as a standard feature. ASLR results in a unique memory layout of the running software each time the OmniSwitch reboots to impede or prevent software exploitation. ASLR is depicted below showing that two different system boots results in two different memory layouts for code segments, data segments, dynamic libraries, etc.

ASLR



Please contact customer support for additional information.

New / Updated Hardware Support

The following new hardware is being introduced in this release.

OS6900-X48C6
Fixed configuration chassis in a 1U form factor with:

- Forty-eight (48) – 10G SFP+ ports
- Six (6) – 100G QSFP28 ports
- USB port
- RJ-45 console port
- EMP port
- Front-to-rear or rear-to-front cooling
- AC or DC power supply

Note: The 6900-X48C6 does not support auto-negotiation with 1G transceivers . Always disable auto-negotiation on the peer switch.

OS6900-T48C6
Fixed configuration chassis in a 1U form factor with:

- Forty-eight (48) – 10GBaseT ports
- Six (6) – 100G QSFP28 ports
- USB port
- RJ-45 console port
- EMP port
- Front-to-rear or rear-to-front cooling
- AC or DC power supply

OS6860N-U28
Fixed configuration chassis in a 1U form factor with:

- Twenty-four (24) – SFP ports
- Four (4) – SFP+ ports
- Four (4) - SFP28 ports
- Two (2) - QSFP28 VFL ports
- USB port
- RJ-45 console port
- EMP port
- AC (PS-150W-AC) or DC (PS-150W-DC) power supply

OS6860N-P48Z
Fixed configuration chassis in a 1U form factor with:

- Thirty-six (36) – 10/100/1000BaseT PoE ports
- Twelve (12) – Multigig (2.5G) PoE ports
- Four (4) - SFP28 ports
- Two (2) - QSFP28 VFL ports
- USB port
- RJ-45 console port
- EMP port
- 600W or 920W AC power supply

OS6860N-P48M
Modular chassis in a 1U form factor with:

- Thirty-six (36) – Multigig (2.5G) PoE ports
- Twelve (12) – Multigig (10G) PoE ports
- One (1) - Expansion slot
- Two (2) - QSFP28 VFL ports
- USB port
- RJ-45 console port

- EMP port
- 600W, 920W, or 2000W AC power supply

Note: Does not currently support hot-swap or hot-insertion of expansion modules. See Hot-Swap Guidelines.

OS68-XNI-U4
Expansion module for OS6860N-P48M with four (4) SFP+ ports.

OS68-VNI-U4
Expansion module for OS6860N-P48M with four (4) SFP28 ports.

OS68-QNI-U2
Expansion module for OS6860N-P48M with two (2) QSFP+ ports.

OS68-CNI-U1
Expansion module for OS6860N-P48M with one (1) QSFP28 ports. (future availability)

OS6860N-BPPH (YPEB0600AM)
600W AC System and PoE power supply for the OS6860N-P48Z and OS6860N-P48M.

OS6860N-BPPX (YPEB0920AM)
920W AC System and PoE power supply for the OS6860N-P48Z and OS6860N-P48M.

OS6860N-BPXL (YPEE2000CM-1A01P10)
2000W AC System and PoE power supply for the OS6860N-P48M. This power supply is not supported on any other model. (future availability).

Note: OS6860N 600W/920W and OS6860(E) 600W/920W power supplies are not interchangeable.

Transceivers
The following transceiver support has been added to 87R1 for the OS6465, OS6465T and OS6865:

- iSFP-10G-ZR is supported on OS6465 and OS6865.
- OS6465T-CBL-60 (60cm DAC cable for VFLs)
- OS6465T-CBL-1M (1M DAC cable for VFLs)
- OS6465T-CBL-3M (3M DAC cable for VFLs)

3FE46541AA - GPON SFP ONT
Support for this transceiver has been added for the platforms/1G SFP ports listed below:

- OS6465-P12 (ports 9-12)
- OS6465T-12 (ports 9-12)
- OS6560-X10 (ports 1-8)
- OS6560-P48Z16 (ports 49-52)
- OS6560-P48X4 (ports 49-54)
- OS6560-P24Z24 (ports 25-28)

For additional transceiver information refer to the Transceivers Guide.

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.

8.7R1 New Feature/Enhancements Summary

Feature	Platform
Management / NMS Related Features	
Programmability - Open vSwitch Database Management Protocol (OVSDB)	6900-X72, 6900-Q32, 6900-V72/C32
IPv6 support for MQTT infrastructure	6465, 6560, 6860, 6860N, 6865, 6900, 6900-V72/C32, 6900-X48C6/T48C6, 9900
Support for Larger USB Flashdrive	6465, 6560, 6860, 6860N, 6865, 6900, 6900-V72/C32, 6900-X48C6/T48C6
App & Package Manager	6465, 6560, 6860, 6860N, 6865, 6900, 6900-V72/C32, 6900-X48C6/T48C6, 9900
Webview 2.0 refresh with localization	6465, 6560, 6860, 6860N, 6865, 6900, 6900-V72/C32, 6900-X48C6/T48C6, 9900
SAA VRF Support	6465, 6860, 6865, 6900, 6900-V72/C32, 6900-X48C6/T48C6, 9900
USB Adapter with Bluetooth Technology	6900- X72, Q32, T40 and T20
Service / Access port / UNP Related Features	
SPB L3VPN using external loopback (S-hook) cable (two-pass)	6860N, 6900-X48C6/T48C6
SPB Over Shared Ethernet	6860, 6860N, 6865, 6900, 6900-V72/C32, 6900-X48C6/T48C6, 9900
SAA SPB	6900-V72/C32, 6900-X48C6/T48C6
Quarantine manager on SAP port	6860, 6865
mDNS on SAP port	6465, 6560, 6860, 6860N, 6865, 6900, 9900
Stellar AP mode on SPB	6860, 6860N, 6865, 6900, 6900-V72/C32, 6900-X48C6/T48C6, 9900
Appmon support on SPB	6860, 6860E
DHCP / UDP Related Features	
Support for RFC 8106 - IPv6 Router Advertisement Options for DNS Configuration	6860, 6900, 9900, 6900-V72/C32, 6465, 6560, 6865
DHCPv6 Snooping/ ISFv6 support on 9900	9900
Layer 3 / Multicast Related Features	
IPv4/v6 BGP	6860, 6860N, 6865, 6900, 6900-V72/C32, 6900-X48C6/T48C6, 9900
Security / Device Profiling Related Features	
IoT IPv6 support for device profile	6465, 6560, 6860, 6860N, 6865, 6900, 6900-V72/C32, 6900-X48C6/T48C6, 9900
Update to 802.1x 2010	6465, 6560, 6860, 6860N, 6865, 6900, 6900-V72/C32, 6900-X48C6/T48C6, 9900
IoT Device Profiling - full solution with OV and cloud-based IoT signature engine.	6465, 6560, 6860, 6860N, 6865, 6900, 6900-V72/C32, 6900-X48C6/T48C6, 9900
Separate File for APPMON Configuration	6860, 6860E

Feature	Platform
MACsec Support on OS6860N	6860N
PoE Related Features	
Perpetual PoE	6860, 6860N, 6865
Fast PoE	6860, 6860N, 6865
LLDP extension to support 802.3bt	6560, 6860N
802.3bt Support on OS6860N	6860N
QoS Related Features	
Application Monitoring - Application Attribute Extraction	6860E
GOOSE Messaging Prioritization	6465, 6865
QSP-5 and custom profile support	6860, 6865, 6900-X72 (custom is EA)
Virtual Chassis Related Features	
VC (of 6) for OS6900-X48C6/T48C6	OS6900-X48C6/T48C6
Mixed VC for OS6900 with V72/C32	6900-V72/C32, OS6900-X48C6/T48C6
Additional Features	
Hardware loopback	6465
L2CP Statistics	6860, 6860N, 6865
MAC Forced Forwarding / Dynamic Proxy ARP	6465, 6900-V72/C32, OS6900-X48C6/T48C6
Support for Jumbo EAP Frames	6860, 6860N, 6900, 6900-V72/C32, OS6900-X48C6/T48C6, 9900
Link Fault Propagation	6900-X72, 6900-V72/C32
JITC Enhancements	6465, 6560, 6860, 6860N, 6865, 6900, 6900-V72/C32, 6900-X48C6/T48C6, 9900
EA Features	
L2 GRE	6900-V72/C32
Custom QSP on X72	6900-X72
Allow non-default QSP on VFL for 6900s	6900

Management / NMS Related Features

Open vSwitch Database Management Protocol (OVSDB)

Open vSwitch is an open-source software switch designed to be used as a vSwitch (virtual switch) in virtualized server environments. A vSwitch forwards traffic between different virtual machines (VMs) on the same physical host and also forwards traffic between VMs and the physical network. Open vSwitch is open to programmatic extension and control using OpenFlow and the OVSDB (Open vSwitch Database) management protocol.

OmniSwitch supports programmability using OVSDB to be able to integrate with Nuage SDN solutions. An AOS to OVSDB connector allows the OmniSwitch to be managed and integrated into Nuage using the vtep(5) schema. The connector permits creation, deletion and modification of VXLAN services, SAPs, end-points and QoS controls. VXLAN services and SAPs can be organised to extend workloads over the network and stretch to the cloud.

OmniSwitch can be configured as a hardware VTEP using the same OVSDB database protocols from the SDN Controller. The SDN controller and the OmniSwitch act as VXLAN tunnel endpoints. The SDN Graphical User Interface is used to configure VXLAN tunnels on the OmniSwitch.

The following CLI commands are associated with this feature:

- A new parameter **mac-orchestration** is added in existing **unp profile map service-type vxlan** CLI to map unp-profile to service type VXLAN.

IPv6 Support for MQTT Infrastructure

AOS Micro Services (AMS) functionality is supported since 8.6R1 where AMS clients connect to AMS broker for information exchange. This connectivity could be based on IPV4 or IPv6 level.

However, AOS has limitations of not having DHCPv6 clients on AOS hence clients can receive IP interface address as IPv4 only and not IPv6.

The following CLI commands are associated with this feature:

- No new CLI

Support for Larger USB Flashdrive

Previously the OmniSwitch supported the Alcatel-Lucent Enterprise 512MB OS-USB-FLASHDR. Expanded support for USB flash drives up to 32GB has been added. This is supported on all platforms except for the OS9900.

The following CLI commands are associated with this feature:

- No new CLI

The following USB devices were tested:

- HP x740w 32GB Flash Drive
- SanDisk Ultra Flair C273 32GB Flash Drive

App & Package Manager

To modularize AOS applications, a new framework is implemented. The framework provides a generic infrastructure to install the AOS or non-AOS/ Third party Debian packages and to support start, stop, and restart of applications residing in the Debian packages without the need for a system reboot. The framework consists of three functional components:

- Package manager (pkgmgr) - responsible for validation, extraction and installation of the non-AOS Debian packages on the AOS switch.
- Application manager (appmgr) - responsible for launching (i.e. start/stop/restart) the applications present in the Debian packages using a package-specific installation script present in a prescribed format in the Debian packages.
- File synchronization utility - responsible for relaying commands and synchronizing the Debian packages and application-specific configuration files across multiple units in a VC or Stack.
- This feature also allows for hitless-security patch upgrades for OpenSSL & NTP.

The following packages are available: WebView 2.0, AMS, OVSDB, NTP and OpenSSL. See Appendix I for installation and removal information.

The following CLI commands are associated with this feature:

For Package Manager (pkgmgr)

- pkgmgr install
- pkgmgr commit
- pkgmgr verify
- pkgmgr list
- pkgmgr remove

For Application Manager (appmgr)

- appmgr start
- appmgr stop
- appmgr restart
- appmgr commit
- appmgr list

WebView 2.0 Refresh with Localization

French and Spanish language support is added to WebView. Enhanced application specific Dashboard is added to each application in WebView.

To install the WebView 2.0 package run the command below. The package is in the */flash/working/pkg* directory.

```
-> pkgmgr install package-webview-8.7.R01-###.deb
```

In some cases a memory threshold message may be displayed. The memory threshold can be increased using the 'health memory threshold' command, for example:

```
-> health threshold memory 85
```

Once verified that the new WebView 2.0 package is working properly, it can be commited making it available even after a system reboot.

```
-> pkgmgr commit
```

To access WebView 2.0 enter the IP address of the switch on which the package is installed followed by *new#*. For example: **`https://ip_address/new#/`**

The following CLI commands are associated with this feature:

- pkgmgr install
- pkgmgr commit
- pkgmgr list

SAA VRF Support

In previous releases, SAA IP ping configuration was allowed only on the management VRF.

In a production network it is mandatory to monitor network performance of applications within the individual VRFs. This enhancement allows users to configure SAA IP Ping across multiple VRFs and monitor performance in VRFs.

The following CLI commands are associated with this feature:

- show saa vrf (new)

- saa, saa start, saa stop, saa type ip-ping, show saa, show saa type config, show saa statistics - modified to add VRF support.

USB Adapter with Bluetooth Technology

Support for a USB Adapter with Bluetooth Technology is now available on an OS6900- X72, Q32, T40 and T20 (not supported on X20/X40 models). **Note**: The code '0000' may need to entered if prompted.

The following CLI commands are associated with this feature:

- bluetooth admin-state

- bluetooth transmit-power

Service / Access port / UNP Related Features

SPB L3VPN using external loopback (S-hook) cable (two-pass)

Support added for 6860N, 6900-X48C6/T48C6.

The following CLI commands are associated with this feature:

- No new CLI

SPB Over Shared Ethernet

By default, SPB-ISIS operates over point-to-point (P2P) links which allows only one adjacency on an SPB network interface. However, an SPB network interface can be configured to allow multiple adjacencies to form on the interface. This is particularly useful for extending an SPB backbone over a multiple access (multi-access) domain, such as a shared, service provider network or even connect to another SPB-ISIS domain.

An SPB multi-access interface is configured on Backbone Edge Bridges (BEBs) that connect directly to a shared network instead of to Backbone Core Bridges (BCBs). Each BEB forms SPB-ISIS adjacencies over the shared network with all the other BEBs on the multi-access network interfaces.

Participating BEBs elect one of the multi-access network interfaces to serve as the Designated Intermediate System (DIS). Each BEB reports their adjacencies to the DIS. The DIS represents all of the multi-access links as a virtual SPB node (pseudo-node).

The following CLI commands are associated with this feature:

- New **p2p**, **multi-access**, and **priority** parameters added to the **spb isis interface** command.
- New **"Circ Type"** field added to **show spb isis interface** command output display.
- New **port** and **linkagg** parameters also added to the show **spb isis interface** command.

Prerequisite: Software releases prior to AOS Release 8.7R1 do not process pseudo-node LSPs. As a result, SPB nodes running such software may experience inconsistent connectivity to destinations beyond the shared Ethernet network segment. If such network reachability is desired, those SPB nodes must be upgraded to AOS Release 8.7R1. (CRAOS8X-21726)

IS-IS is link state protocol, which fundamentally requires every participating device in the topology to have the same view of the topology represented by the link state database and follow the same procedure to determine the shortest path to reach every other participating device in the network.

The SPB Over Shared Ethernet feature represents every shared link/network as a psuedonode. One of the nodes on the shared link is elected as a Designated IS (DIS) node which originates a pseudo-node LSP. This pseudo-node LSP needs to be flooded across the entire SPB network and all the devices in the SPB network (not just the devices directly connected to the shared network) need to understand this LSP to determine the shortest paths to other devices which travel through the shared network.

Advertisement and processing of such psuedonode LSPs is an enhancement to the standardized ISIS-SPB functionality which is limited to supporting only point-to-point links.

SAA SPB

SAA SPB support is extended to the OS6900-V72/C32 and OS6900-X48C6/T48C6 platforms.

The following CLI commands are associated with this feature:

- No new CLI

Quarantine Manger on SAP Port

Previously, Access Guardian supported Quarantine Manager and Remediation (QMR) only on UNP bridge ports. QMR support is now extended to UNP access ports (SAP ports). As a result, QMR is applied to users learned in both the VLAN and service domain. **Note**: Redirecting quarantined users for remediation is not supported for users learned on UNP access ports.

The following CLI commands are associated with this feature:

- No new CLI

mDNS on SAP Port

Apple's Bonjour protocol is built on multicast DNS, which is a Layer 2 non-routable protocol. Bonjour exchanges information through individual multicast DNS packets (mDNS) and DNS-based service discovery (DNS-SD). Bonjour packets are not routed, which limits their use to the current local area network. The mDNS relay functionality allows the Bonjour clients to see the services published across subnets.

The OmniSwitch implementation of this functionality previously supported mDNS traffic forwarded from a VLAN domain. The 8.7R1 release adds support for mDNS traffic forwarded from a Shortest Path Bridging (SPB) domain.

In a network where mDNS clients and servers are connected to edge switches that participate in an SPB domain, mDNS traffic is forwarded on an SPB service instance (I-SID) instead of a VLAN. An external loopback configuration is required on the switch where the mDNS relay function is performed. The mDNS relay is still provided in the VLAN domain, so the external loopback is required to pass mDNS traffic between an SPB SAP port and a VLAN port.

The following CLI commands are associated with this feature:

- No new CLI

Stellar AP Mode on SPB

Previously, the OmniSwitch detection and integration of OmniAccess Stellar APs was supported only on UNP bridge ports. This same functionality is now also supported on UNP access ports. When an OmniAccess Stellar AP is connected to:

- a UNP bridge port, clients are learned in the VLAN domain.
- a UNP access port, clients are learned in the service domain.

Similar to the built-in “DefaultWLANProfile” profile that is used to classify the AP MAC address, a new built-in “DefaultWLANAccessProfile” profile is used to classify the AP MAC address.

- The “DefaultWLANAccessProfile” profile is mapped to a VLAN into which the AP device is classified. This establishes a VLAN-port association (VPA) between the UNP port and profile VLAN on which the AP MAC address is learned and forwarded on the VLAN domain.
- The “DefaultWLANAccessProfile” profile is mapped to SPB service parameters that are used to create a dynamic SPB SAP on which the AP MAC address is learned and forwarded on the SPB service domain.

The following CLI commands are associated with this feature:

- No new CLI

Appmon Support on SPB

Application Monitoring support is extended to the SPB service domain; hence Appmon configuration is allowed on UNP access ports that will classify traffic into UNP profiles that are mapped to SPB service parameters.

The following CLI commands are associated with this feature:

- No new CLI

MACsec Support on OS6860N

MACsec feature support is extended to OmniSwitch 6860N. OS6860N only supports MACsec mode ‘dynamic’, 'static' mode is not supported. Key types supported are "aes-gcm-128", "aes-cmac-128", and "aes-cmac-256". Key type “aes-gcm-256” is currently not supported in this release.

- Supports MACsec dynamic mode only.
- OS6860N-U28 - Supports MACsec on SFP (1-24), SFP+ (25-28) and SFP28 (31-34) ports.
- OS6860N-P48Z - Supports MACsec on SFP28 (51-54) ports.
- OS6860N-P48M - Supports MACsec on expansion modules only.
- MACsec is not supported on any 4X10G splitter transceivers.

Modified CLI command

- security key-chain gen-random-key
- security key
- show interfaces capability

DHCP / UDP Related Features

Support for RFC 8106 - IPv6 Router Advertisement Options for DNS Configuration

AOS supports configuration of up to three DNS name server for IPv6 addresses. It is required to advertise the DNS name server IPV6 addresses in its router advertisement options. OmniSwitch allows to configure DNS advertisement by allowing to enable or disable DNS Search List (DNSSL) and Recursive DNS Server (RDNSS) router advertisement.

The following CLI commands are associated with this feature:

- The ipv6 interface CLI command is updated with configuration parameters **ra-send-dnssl** and **ra-send-rdnss** to configure the information in the router advertisement.

- The configuration status of the router advertisement is displayed in **show ipv6 interface** output.

DHCPv6 Snooping / ISFv6 Support on 9900

Support added for OmniSwitch 9900.

The following CLI commands are associated with this feature:

- No new CLI.

Layer 3 / Multicast Related Features

IPv4/v6 BGP

The route server clients must accept UPDATE messages where the leftmost AS in the AS_PATH attribute is not equal to the AS number of the route server that sent the UPDATE message. The OmniSwitch can be configured to check for the first AS in the ASPATH list while processing UPDATE messages from BGP neighbor. The switch can be explicitly configured for IPv4 and IPv6 address type.

The following CLI commands are associated with this feature:

- {ip | ipv6} bgp neighbor {ipv4_address | ipv6_address} check-first-as

Security / Device Profiling Related Features

IoT Device Profiling - IPv6 Support

Starting with 8.7R1, IPv6 is supported in Device Profiling. The Device Profiling for IPV6 packets is done using the DHCP-Fingerprinting, DNS-Fingerprinting and HTTP-Fingerprinting as it is done for the IPV4 packets.

The following CLI commands are associated with this feature:

- device-profile admin-state
- device-profile port linkagg
- device-profile device-type
- device-profile update-signature
- device-profile update-signature from
- device-profile auto-unp-assignment
- show device-profile config
- show device-profile summary
- show device-profile catalog
- show device-profile signatures from
- show device-profile signatures

Update to 802.1X 2010

This feature provides a new command to configure EAPoL version V1 or V3 globally on the switch for 802.1x authentication of users on UNP port. The default version would remain as V1.

The following CLI commands are associated with this feature:

- unp 802.1x eapol-version

IoT Device Profiling - Full Solution with OV and Cloud-based IoT Signature Engine

The required infrastructure for IoT Device Profiling full solution with OV and cloud-based IoT signature engine is present in 8.6.R1 & 8.6.R2 release. The enforcement is now implemented from OmniVista.

The following CLI commands are associated with this feature:

- No new CLI

Separate File for Appmon Configuration

In the previous release, ‘show config snapshot’ command when used to view the AppMon configuration. output would go up to 2800+ lines as it would display per application level configuration. This would get difficult in troubleshooting at customer end as AppMon supports around 2800 applications in the latest AppMon signature kit.

To resolve this, a new command app-mon separate-config-file is introduced, which will reduce per application level AppMon configuration displayed in the “show configuration snapshot” as well as in “vcboot.cfg”. When this command is used, per application configuration is moved to a separate file called appmon_vcboot.cfg from vcboot.cfg on write memory.

A new parameter app-snapshot is added to ‘show app-mon config’ command, which will display per application level AppMon configuration.The following CLI commands are associated with this feature:

The following CLI commands are associated with this feature:

- app-mon separate-config-file
- show app-mon config [app-snapshot]

PoE Related Features

Perpetual PoE

Perpetual PoE allows the switch to provide uninterrupted power to connected power device (PD) even when the switch is rebooting or reloading, such as on a soft reset. This feature uses the same FPGA and PoE controller changes as described in the Fast PoE feature description.

The following CLI commands are associated with this feature:

- lanpower ppoe {enable | disable}

Guidelines:

- The following FPGA/CPLD upgrades are required:
  - OS6860 models (See table.)
  - OS6865 models (See table.)
- The power to the PD devices will be interrupted if the PoE controller(MCU) firmware itself is being upgraded.

Fast PoE

Fast PoE can be used to provide PoE power within a few seconds after powering on the chassis. Prior to this feature PoE power is not provided until the chassis has completed its bootup. With Fast PoE the default state of the PoE subsystem is set to enabled in the FPGA image and the PoE configuration is stored in the controller EEPROM. This allows the chassis to immediately provide PoE power to any connected devices immediately after being powered on without waiting for the chassis to complete its bootup. Fast PoE requires an FPGA/CPLD upgrade.

The following CLI commands are associated with this feature:

- lanpower fpoe {enable | disable}

Guidelines:

  - OS6860 models (See table.)
  - OS6865 models (See table.)
- Factory default switches that don't have any PoE configuration must have an initial PoE configuration completed.
- The PoE configuration cannot be modified until the switch is up and the PoE module is completely initialized.
- LLDP-based PoE devices will not function as expected until the switch has completed its bootup and the switch is in a state to respond to LLDP requests.

LLDP Extension for 802.3bt

AOS supports the LLDP power via MDI TLV extension to support the additional capabilities offered by 802.3bt Type 3 and Type 4 PSEs and PDs on the OS6560 and OS6860N.

The following CLI commands are associated with this feature:

- No new CLI

802.3bt Support on OS6860N

IEEE 802.3bt support is being added to the OmniSwitch 6860N. IEEE 802.3bt adds support for Type 3 and Type 4 PoE devices and an additional 4 classes (class 5 to class 8), which can support up to 95 watts of power over 4-pairs of the ethernet cable.

The following CLI commands are associated with this feature:

- lanpower slot 802.3bt {enable | disable}

QoS Related Features

Application Monitoring - Application Attribute Extraction

In previous releases, AppMon supported detection of application signatures at a macro level.

With this enhancement, AppMon provides the capability to extract pre-defined attributes of a given application for debugging and monitoring purpose. The interface information for an application attribute flow can be viewed.

The new command does not allow any configuration but can be used to view the attribute records for a specific application. Currently, this command can be used to monitor only IEC104 application.

The following CLI commands are associated with this feature:

- app-mon data

GOOSE Messaging Prioritization

AOS provides priority for different types of messages as per the IEC 61850. As per the requirement Generic Object-Oriented Substation Event (GOOSE) messages and other associated message packets part of IEC 61850 getting switched via AOS Switches must be applied with specific QOS priority.

GOOSE messages allow for the broadcast of multicast messages across the Local Area Network (LAN). GOOSE messages are exchanged between Intelligent Electronic Devices (IEDs) present in the electrical sub-station networks.

To support this requirement, OmniSwitch allows to configure IEC 61850 message priority. The iec message-type message priority string CLI command allows to configure the priority.

The configured priority rule can be removed using the iec message-type string flush CLI command.

The following CLI commands are associated with this feature:

- iec message-type *message* priority *string*
- iec message-type *string* flush
- iec show

QSP-5 Support for OS6900-X72

Support for QoS Qset Profile (QSP) 5 added to OmniSwitch 6900-X72 and OmniSwitch 6860/6865. QSP 5 is a Weighted Round Robin (WRR) profile. In addition, custom profile support was also added to the OmniSwitch 6860/6865.

The following CLI commands are associated with this feature:

- No new CLI.

Virtual Chassis Related Features

VC for OS6900-X48C6/T48C6

Up to six (6) OS6900-X48C6 and OS6900-T48C6 chassis can be mixed in a Virtual Chassis.

The following CLI commands are associated with this feature:

- No new CLI

Mixed VC for OS6900-X48C6/T48C6 and OS6900-V72/C32

Up to six (6) OS6900-V72/C32 and OS6900-X48C6/T48C6 chassis can be mixed in a Virtual Chassis.

Note: With this mixed VC configuration only SPB L3 using external loopback is supported.

The following CLI commands are associated with this feature:

- No new CLI

Additional Features

Hardware Loopback

The hardware loopback test feature allows a user to measure the quality of service provided by the Ethernet service provider and help debug any forwarding related issues. Support for this functionality is extended to the OmniSwitch 6465. In addition, a SAP ID can be specified when configuring an outward loopback test on the OmniSwitch 6465.

The following CLI commands are associated with this feature:

- New sap parameter for the loopback-test command.
- New “SapId” field added to the show loopback-test command output display.

L2CP Statistics

Support for L2 Control Protocol tunneling frame statistics extended to the OmniSwitch 6860/6865 for UNI and NNI ports, but not for UNI profiles.

The following CLI commands are associated with this feature:

- No new CLI.

MAC Forced Forwarding / Dynamic Proxy ARP

Support for this feature has been added for the OS6465 in this release.

The following CLI commands are associated with this feature:

- No new CLI

Support for Jumbo EAP Frames

Access Guardian supports 802.1x authentication of users using EAP frame size up to 1696 bytes only. In networks or supplicants where jumbo frames are enabled EAP frame sizes may exceed this supported size and get dropped causing authentication failure.

In 8.7 R1, the 802.1x-authentication support is extended for Jumbo EAP or EAPOL frames, which means now EAP frames above 1696 is supported in AOS without EAP fragmentation. The maximum EAP fragment size allowed with respect to maximum RADIUS packet size is 4096 bytes.

The following CLI commands are associated with this feature:

- No new CLI

Link Fault Propogation

Support for this feature has been added for the OS6900-X72 and OS6900-V72/C32 in this release.

The following CLI commands are associated with this feature:

- No new CLI

JITC Enhancements

IPsec over IPv4

IPsec support for IPV4 added. IPsec support for HMAC-SHA2 family algorithms HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512 for authentication.

SNMP / ASA User Algorithms

The following algorithms have been added for SNMP and Authenticated Switch Access:

- Support added for SHA384, SHA224+AES, SHA256+AES, SHA384+AES algorithms.

LDAP over IPv6 support added

LDAP over IPv6 has been added in this release.

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-21090	In the rare case where an OS6456/6560 fails to mount the flash at bootup, the switch may still reach ready state impacting flash access and functionality.	There is no known workaround at this time.
CRAOS8X-22239	The configuration related to slot 1 (OS6860N-P48M) is not seen with "show configuration snapshot lanpower" output .	There is no known workaround at this time.
CRAOS8X-10059	Toggling admin state of bulk of VLANs (disable/enable) very quickly may cause VPA state of the VLANs to be incorrectly stuck in blocking state instead of forwarding.	Allow few seconds in between toggling admin state (disable/enable) of bulk of VLANs.
CRAOS8X-11850	Frequent addition and deletion of 64 vrfs could lead to memory exhaustion leading to kernel warning memory of 80% limiting to only 50 VRFs.	There is no known workaround at this time.
CRAOS8X-17305/20765	In dual CMM OS9900 chassis with auto fabric enabled some linkagg ports may not be displayed correctly on CMMB after takeover.	After auto fabric detects the configuration, doing a write-memory and CMMB reload before VC-takeover, will correctly synchronize CMMB database. If traffic issues are seen, reconfigure the linkagg ports should recover the issues.
CRAOS8X-17485	For 6860N, there is a limitation where ERP multicast packets are counted as multicast as well as unicast packets in "show interface counters". Ideally these should be counted as Multicast packkets only.	There is no other functional impact or packet drop because of this issue.
CRAOS8X-18633	When outport or bidirectional mirroring is configured along with rpmir vlan, then the CPU generated packets going out of mirror source port that are mirrored to destination port dont have RPMIR VLAN tag.	CPU mirroring is disabled on 6860N, 6900-T48C6/X48C6 models when RPMIR is configured.
CRAOS8X-19018	OS6900: After enable/disable the saa process. The " Last Time	There is no known workaround at this time.

	result" displays failed instead of success.	
CRAOS8X-20920	MTU counters are not displayed for max-frame-size 1522 & 9220 in "show interfaces accounting" output.	There is no known workaround at this time.

Hardware / Transceivers

CR	Description	Workaround
CRAOS8X-20744	On an OS6560 10G ports there may sometimes be and extra toggle when the port links up.	There is no known workaround at this time.
CRAOS8X-21496/21484	On the ports below an extra flap or two may be observed during link toggle. The LED may glow momentarily during SFP/link toggles. - 6560-P48Z16 (ports 49 – 52) - 6560-P48X4 (ports 49 – 52) - 6560-X10 (ports 1 – 8)	There is no known workaround at this time.
CRAOS8X-21805	On OS6560 10G ports there is a delay of up to 4 seconds during linkup.	There is no known workaround at this time.
CRAOS8X-21818	For 6860N-U28, when using DUAL-BX-D/U transceiver, if the port is configured for 100M speed and remote end is continuously toggled between 1G and 100M, at some point, the switch displays port link up at 100M while the remote end is at 1G.	There is no known workaround at this time.
CRAOS8X-21833	On an OS6860N-U28 when using the DUAL-MM-N transceiver, if the port is configured for 100M speed, the switch displays the port link up at 1G.	There is no known workaround at this time.
CRAOS8X-21980	On an OS6560, with 7m DAC cable, sometimes either link may not come up or CRC errors or link flaps may be seen.	There is no known workaround at this time.
CRAOS8X-22130	PoE is not working after unlike PS swap (600w/900w) and reload with fast/perpetual PoE enabled.	See Fast/Perpetual PoE P/S Swap instructions.

CRAOS8X-22810	On an OS6900-X48C6 with an SFP-10G-T transceiver connected at 1G, the remote side remains UP when the SFP-10G-T is administratively disabled.	There is no known workaround at this time.
CRAOS8X-21690	With the GPON SFP ONT (3FE46541AA) during boot-up, admin enable/disable or link insertion/deletion the micro-controller of the transceiver resets multiple times causing a delay in operational status.	There is no known workaround at this time.
CRAOS8X-18548	With the GPON SFP ONT (3FE46541AA) an error similar to the one below is seen when the interface is toggled causing a delay in operational status: *[256395.939542] i2c i2c-0: mv64xxx_i2c_fsm: Ctlr Error -- state: 0x4, status: 0x0, addr: 0x51, flags: 0x1*	There is no known workaround at this time.
CRAOS8X-18549	The GPON SFP ONT (3FE46541AA) is not detected for more than 1 minute after insertion.	There is no known workaround at this time.
CRAOS8X-19657	The GPON SFP ONT (3FE46541AA) connected interface toggles multiple times upon hot insertion and removal.	There is no known workaround at this time.
CRAOS8X-18552	The GPON SFP ONT (3FE46541AA) LED & interface are shown as UP once the remote end is disconnected.	There is no known workaround at this time.

Layer 3 / DHCP

PR	Description	Workaround
CRAOS8X-18718	Static ARP/Dynamic ARP is getting removed after there is congestion on a OS6860N.	There is no known workaround at this time.
CRAOS8X-11084	Packet drop seen in BFD config when VRRP VLAN interface is toggled.	There is no known workaround at this time.

Layer 2 / Multicast

PR	Description	Workaround
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.

MACsec

PR	Description	Workaround
CRAOS8X-10420	Between a OS6860N and an OS6860, when MACsec is enabled without encryption, the data packets are dropped. This is an interoperability issue between the two platforms.	Use MACsec with encryption between an OS6860N and an OS6860, this configuration works properly and is the recommended operational mode for MACsec.
CRAOS8X-19890	When dynamic MACsec is enabled on the SPB-SAP or Eservices-UNI ports, the MKA/1X packets are blocked/dropped by the SAP/UNI ports preventing the MACsec secure channel/association from being established.	There is no known workaround at this time.

QoS

PR	Description	Workaround
CRAOS8X-4424	With color-only policy action configuration, egress queue is not honoring the color marking. Packet drop is observed and expected traffic rate is not achieved.	There is no known workaround at this time.

Service Related

PR	Description	Workaround
CRAOS8X-4124	Traffic is not tunneled over L2GRE service when sending traffic from Edge to GTTS via another Edge switch where SAP/loopback port on GTTS is configured as static linkagg.	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-12513	When 2048 IGMP groups were sent over SPB service, only 1025 IGMP groups were received with 1024 SAPs per service configured on the edge switch. Seen with large amount of SAPs (>1K) configured on same port.	Distribute the SAPs across different ports.
CRAOS8X-20761	The 'show service spb *num* counters' command output does not display any ingress/egress statistics, zeros are always displayed.	There is no known workaround at this time.

UNP

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-14911	OS6860, OS6865, OS6900 - UNP user learning fails when the RADIUS unp-profile-precedence is set to tunnel-private-group-id. Sometimes when mac addresses are flushed they do not get removed from hardware and user learning fails.	Introducing a 2-3 seconds delay before sending user learning packets resolves the issue

Virtual Chassis

PR	Description	Workaround
CRAOS8X-10498	"qos port 1/1/3 maximum ingress-bandwidth 80M" doesn't work after vc-takeover and reload. 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>".
CRAOS8X-19992	OS6860: Upon VC takeover with L2 controlled PDU's traffic, lldpNi Agent ERR , intfNi Msec ERR, stpNi BINt ERR are seen.	There is no known workaround at this time.

CRAOS8X-20092	On a 6860N VFL ports are showing as splitter ports in 'show interfaces ddm actual' CLI.	There is no known workaround at this time.
CRAOS8X-20212	SPB IS-IS configuration get removed after VC-takeover with auto-fabric process.	There is no known workaround at this time.

Hot-Swap/Redundancy Feature Guidelines

Hot-Swap Feature Guidelines

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

- 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	Not Supported
OS68-XNI-U4	Not Supported
OS68-VNI-U4	Not Supported
OS68-QNI-U2	Not Supported
• Expansion modules must be inserted prior to bootup. • Runtime removal and insertion of the same or different expansion modules is not supported.	

OS6860N-P48M Hot-Swap/Insertion Compatibility

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.

VC Hot-Swap / Removal Guidelines

Elements of a VC are hot-swappable. They can also be removed from, or added to, a VC without disrupting other elements in the VC. Observe the following important guidelines:

- Hot-swapping an element of a VC is only supported when replaced with the same model element (i.e. an OS6900-X20 must be replaced with an OS6900-X20).
- Replacing an element with a different model element requires a VC reboot.

Fast/Perpetual PoE Unlike Power Supply Swapping

When swapping unlike power supplies on an OS6860N-P48M follow the procedure below to ensure continued PoE functionality when fast or perpetual PoE is enabled.

1. Disable fpoe and ppoe (Only needs to be executed if lanpower is started).
2. Save and synchronize the configuration.
3. Swap the power supplies.
4. Reload chassis.
5. Start lanpower.
6. Enable fpoe and ppoe as required.
7. Save and synchronize the configuration.

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: businessportal.al-enterprise.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 following is in addition to the information found in the **/flash/foss/Legal_Notice.txt** file.

```
FOSS Name : FOSS Version : Name of Applicable License : Pointer to file containing License Text

libatomic           : 1.0.0      : GPLv3+ & GPLv3+      : /flash/foss/gpl-3.0.txt +
                                   with exceptions &      /flash/foss/gpl-2.0.txt +
                                   GPLv2+ with exceptions /flash/foss/lgpl-2.1.txt +
                                   & LGPLv2+ & BSD        /flash/foss/bsd1.txt
openvswitch         : 2.12.0     : Apache License 2.0   : /flash/foss/Apache-License-2.0.txt
```

Appendix A: Feature Matrix

The following is a feature matrix for AOS Release 8.7R1.

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)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6	9900
Management Features									
AOS Micro Services (AMS)	8.6R1	8.6R1	8.6R1	8.7R1	8.6R1	8.6R1	8.6R1	8.7R1	8.6R1
Automatic Remote Configuration Download (RCL)	8.5R1	Y	Y	8.7R1	Y	Y	8.6R2	8.7R1	Y
Automatic/Intelligent Fabric	8.5R1	Y	Y	N	Y	Y	N	N	Y
Automatic VC	N	Y	Y	8.7R1	Y	Y	8.6R2	8.7R1	N
Bluetooth - USB Adapter with Bluetooth Technology	8.6R2	8.6R2	Y	8.7R1	8.6R2	8.7R1	8.6R2	N	N
Console Disable	8.6R2	8.6R2	8.6R2	8.7R1	8.6R2	8.6R2	8.6R2	8.7R1	8.6R2
Dying Gasp	Y	Y	Y	8.7R1	Y	N	N	N	N
Dying Gasp (EFM OAM / Link OAM)	8.6R1	8.6R1	8.6R1	8.7R1	8.6R1	N	N	N	N
EEE support	N	N	Y	8.7R1	Y	Y	N	N	N
Embedded Python Scripting / Event Manager	8.5R1	Y	Y	8.7R1	Y	Y	N	N	N
IP Managed Services	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Hitless Security Patch Upgrade	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1
In-Band Management over SPB	N	N	8.5R4	8.7R1	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4
ISSU	Y	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
NAPALM Support	8.5R1	8.5R1	8.5R1	8.7R1	8.5R1	8.5R1	N	N	N
NTP - Version 4.2.8.p11.	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4
OpenFlow	N	N	Y	N	N	Y	N	N	N
OV Cirrus – Zero touch provisioning	Y	Y	Y	8.7R1	Y	Y	N	N	N
OV Cirrus – Configurable NAS Address	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4
OV Cirrus – Default Admin Password Change	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4
OV Cirrus – Managed	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4
OVSDB	N	N	N	N	N	8.7R1 (X72/Q32)	8.7R1	N	N
Package Manager	8.6R2	8.6R2	8.6R2	8.7R1	8.6R2	8.6R2	8.6R2	8.7R1	8.6R2
Readable Event Log	8.6R1	8.6R1	8.6R1	8.7R1	8.6R1	8.6R1	8.6R1	8.7R1	8.6R1
Remote Chassis Detection (RCD)	N	N	8.6R2	8.7R1	N	Y	N	8.7R1	Y
SAA	8.5R1	N	Y	N	Y	Y	8.7R1	8.7R1	N
SAA SPB	N	N	Y	N	Y	Y	8.7R1	8.7R1	8.6R2
SAA UNP	Y	N	Y	N	Y	Y	N	N	N
SNMP v1/v2/v3	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
UDLD	8.5R1	Y	Y	8.7R1	Y	Y	N	N	EA
USB Disaster Recovery	8.5R1	Y	Y	8.7R1 (onie)	Y	Y	8.7R1 (onie)	8.7R1 (onie)	Y

Feature	6465	6560	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6	9900
USB Flash (AOS)	8.5R1	Y	Y	8.7R1	Y	Y	N	N	N
Virtual Chassis (VC)	8.5R2	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Virtual Chassis Split Protection (VCSP)	Y	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
VRF	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
VRF – IPv6	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
VRF – DHCP Client	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Web Services & CLI Scripting	8.5R1	Y	Y	8.7R1	Y	Y	8.7R1	8.7R1	Y
Layer 3 Feature Support									
ARP	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
BFD	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
BGP	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
DHCP Client / Server	8.6R1	Y	Y	8.7R1	Y	Y	8.5R4	8.7R1	Y
DHCP Relay	8.5R1	Y	Y	8.7R1	Y	Y	8.5R4	8.7R1	Y
DHCPv6 Server	N	N	Y	8.7R1	Y	Y	8.7R1	8.7R1	Y
DHCPv6 Relay	8.5R1	Y	Y	8.7R1	Y	Y	8.7R1	8.7R1	Y
DHCP Snooping / IP Source Filtering	8.5R4	Y	Y	8.7R1	Y	Y	8.6R2	8.7R1	Y
ECMP	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
IGMP v1/v2/v3	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
GRE	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.5R2
IP-IP tunneling	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.5R2
IPv6	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
IPv6 - DHCPv6 Snooping	8.6R1	8.6R1	8.5R3	8.7R1	8.5R4	N	8.6R2	8.7R1	8.7R1
IPv6 - Source filtering	N	8.6R1	8.5R3	8.7R1	8.5R4	N	8.6R2	8.7R1	8.7R1
IPv6 - DHCP Guard	EA	EA	EA	N	EA	N	N	N	N
IPv6 - DHCP Client Guard	EA	EA	EA	N	EA	N	N	N	N
IPv6 - RA Guard (RA filter)	N	8.5R2	Y	8.7R1	Y	Y	N	N	N
IPv6 - DHCP relay and Neighbor discovery proxy	8.5R1	Y	Y	8.7R1	Y	Y	N	N	Y
IP Multinetting	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
IPSec (IPv6)	N	N	Y	8.7R1	Y	Y	N	N	EA
ISIS IPv4/IPv6	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.5R2
M-ISIS	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.5R2
OSPFv2	N	8.5R2[1]	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
OSPFv3	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
RIP v1/v2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
RIPng	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y

Feature	6465	6560	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6	9900
UDP Relay (IPv4)	8.5R4	8.5R4	Y	8.7R1	Y	Y	8.5R4	8.7R1	8.5R4
UDP Relay (IPv6)	8.6R1	8.6R1	8.6R1	8.7R1	8.6R	8.6R1	8.6R1	8.7R1	8.6R1
VRRP v2	8.5R2	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
VRRP v3	8.5R2	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Server Load Balancing (SLB)	N	N	Y	N	Y	Y	N	N	N
Static routing	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Multicast Features									
DVMRP	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	N
IPv4 Multicast Switching	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Multicast *,G	Y	8.5R2	8.5R2	8.7R1	Y	Y	8.5R2	8.7R1	Y
IPv6 Multicast Switching	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
PIM-DM	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
PIM-SM	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
PIM-SSM	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
PIM-SSM Static Map	N	N	N	N	N	N	N	N	N
PIM-BiDir	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
PIM Message Packing	N	N	8.6R1	8.7R1	N	8.6R1	8.6R1	8.7R1	N
PIM - Anycast RP	N	N	8.6R2	8.7R1	8.6R2	8.6R2	8.6R2	8.7R1	8.6R2
Monitoring/Troubleshooting Features									
Ping and traceroute	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Policy based mirroring	N	N	Y	8.7R1	Y	Y	8.7R1	8.7R1	8.5R4
Port mirroring	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Port monitoring	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Port mirroring - remote	8.5R1	Y	Y	8.7R1	Y	Y	EA	N	EA
Port mirroring – remote over linkagg	N	N	Y	8.7R1	Y	Y	N	N	N
RMON	8.5R1	Y	Y	N	Y	Y	N	N	N
SFlow	8.5R1	Y	Y	8.7R1	Y	Y	8.7R1	8.7R1	Y
Switch logging / Syslog	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
TDR	N	N	Y	N	N	N	N	N	N
Layer 2 Feature Support									
802.1q	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
DHL	8.5R1	Y	Y	8.7R1	Y	N	N	N	N
ERP v2	8.5R1	8.5R2	Y	8.7R1	Y	Y	8.7R1	8.7R1	8.5R3
HAVLAN	EA	N	Y	N	Y	Y	8.6R2	8.7R1	EA

Feature	6465	6560	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6	9900
Link Aggregation (static and LACP)	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
LLDP (802.1ab)	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Loopback detection – Edge (Bridge)	8.5R1	Y	Y	8.7R1	Y	N	8.6R2	8.7R1	Y
Loopback detection – SAP (Access)	N	N	Y	8.7R1	Y	Y	8.6R2	8.7R1	EA
MAC Forced Forwarding / Dynamic Proxy ARP	8.7R1	N	8.6R1	N	8.6R1	N	N	N	N
Port mapping	Y	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	N
Private VLANs	N	N	Y	N	Y	Y	N	N	N
SIP Snooping	N	N	Y	N	N	N	N	N	N
Spanning Tree (1X1, RSTP, MSTP)	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Spanning Tree (PVST+, Loop Guard)	N	Y	Y	8.7R1	Y	Y	N	N	EA
MVRP	8.5R1	Y	Y	8.7R1	Y	Y	8.5R4	8.7R1	Y
SPB[2]	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
SPB - Over Shared Ethernet	N	N	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1
SPB – HW-based LSP flooding	N	N	N	N	N	N	N	N	8.5R4
QoS Feature Support									
802.1p / DSCP priority mapping	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
IPv4	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
IPv6	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Auto-Qos prioritization of NMS/IP Phone Traffic	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Auto-Qos – New MAC range	8.5R2	8.5R2	8.5R2	8.7R1	8.5R2	8.5R2	8.5R2	8.7R1	8.5R2
Groups - Port	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Groups - MAC	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Groups - Network	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Groups - Service	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Groups - Map	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Groups - Switch	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Ingress/Egress bandwidth limit	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Per port rate limiting	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	N
Policy Lists	8.5R1	Y	Y	8.7R1	Y	Y	8.7R1	8.7R1	Y
Policy Lists - Egress	N	N	Y	8.7R1	Y	Y	8.7R1	8.7R1	N
Policy based routing	N	N	Y	8.7R1	Y	Y	8.6R2	8.7R1	EA
Tri-color marking	N	N	Y	8.7R1	Y	Y	N	N	N
QSP Profiles 1	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
QSP Profiles 2/3/4	N	N	Y	QSP-2 only	Y	Y	QSP-2 only	QSP-2 only	N
QSP Profiles 5	8.5R1	Y	8.7R1	8.7R1	8.7R1	8.7R1 (X72)	N	N	Y

Feature	6465	6560	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6	9900
Custom QSP Profiles	Y	Y	Y	Y	Y	X72 only (EA)	Y	Y	Y
GOOSE Messaging Prioritization	8.7R1	N	N	N	8.7R1	N	N	**N**	**N**
Metro Ethernet Features									
CPE Test Head	8.6R1	N	N	N	N	N	N	N	N
Ethernet Loopback Test	N	N	8.6R1	8.7R1	8.6R1	N	N	N	N
Ethernet Services (VLAN Stacking)	8.5R1	N	Y	N	Y	Y	8.5R4	8.7R1	N
Ethernet OAM (ITU Y1731 and 802.1ag)	8.5R1	N	Y	8.7R1	Y	Y	8.7R1	8.7R1	EA
EFM OAM / Link OAM (802.3ah)	8.6R1	8.6R1	8.5R4	N	8.5R4	N	N	N	N
PPPoE Intermediate Agent	8.6R1	N	N	N	8.6R1	N	N	N	N
1588v2 End-to-End Transparent Clock	8.5R1	N	Y	N	Y	Y (X72/Q32)	N	N	N
1588v2 Peer-to-Peer Transparent Clock	8.6R1	N	N	N	N	N	N	N	N
1588v2 Across VC	N	N	N	N	N	8.5R2 (X72)	N	N	N
Access Guardian / Security Features									
802.1x Authentication	8.5R2	Y	Y	8.7R1	Y	Y	8.7R1	8.7R1	Y
Access Guardian – Bridge	8.5R1	Y	Y	8.7R1	Y	Y	8.6R1	8.7R1	Y
Access Guardian - Access	N	N	Y	8.7R1	Y	Y	8.5R4	8.7R1	Y
Application Fingerprinting	N	N	N	N	N	Y	N	N	N
Application Monitoring and Enforcement (Appmon)	N	N	Y	N	N	N	N	N	N
ARP Poisoning Protection	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
BYOD - COA Extension support for RADIUS	Y	Y	Y	8.7R1	Y	8.62	8.6R2	8.7R1	Y
BYOD - mDNS Snooping/Relay	Y	Y	Y	8.7R1	Y	8.62	8.6R2	8.7R1	Y
BYOD - UPNP/DLNA Relay	Y	Y	Y	8.7R1	Y	8.62	8.6R2	8.7R1	Y
BYOD - Switch Port location information pass-through in RADIUS requests	Y	Y	Y	8.7R1	Y	8.62	8.6R2	8.7R1	Y
Captive Portal	8.5R4	Y	Y	8.7R1	Y	8.62	8.6R2	8.7R1	Y
IoT Device Profiling	8.5R2	8.5R2	8.5R2	8.7R1	8.5R2	8.5R2	8.6R1	8.7R1	8.5R2
IoT Device Profiling (IPv6)	8.7R1	8.7R1	8.7R1	N	8.7R1	8.7R1	N	N	8.7R1
Directed Broadcasts – Control	8.5R2	8.5R2	8.5R2	8.7R1	8.5R2	8.5R2	8.7R1	8.7R1	Y
Interface Violation Recovery	8.5R1	Y	Y	8.7R1	Y	Y	8.7R1	8.7R1	Y
Kerberos Snooping	N	8.6R2	8.6R2	N	8.6R2	8.6R2	8.6R2	N	8.6R2
L2 GRE Tunnel Access (Edge) (bridge ports)	N	Y	Y	N	Y	8.6R1[3]	8.7R1	N	Y
L2 GRE Tunnel Access (Edge) (access ports)	N	N	8.6R1	N	8.6R1	8.6R1[3]	8.7R1	N	8.6R1
L2 GRE Tunnel Aggregation	N	N	Y	N	Y	Y[3]	8.7R1	N	Y
Learned Port Security (LPS)	8.5R1	Y	Y	8.7R1	Y	Y	8.5R4	8.7R1	Y
MACsec[4]	8.5R1	8.5R4	Y	8.7R1	N	N	N	N	8.5R2
MACsec MKA Support[4]	8.5R2	8.5R4	8.5R2	8.7R1	N	N	N	N	8.5R2

Feature	6465	6560	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6	9900
Quarantine Manager	N	N	Y	N	Y	N	N	N	N
RADIUS - RFC-2868 Support	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4
Role-based Authentication for Routed Domains	N	N	8.5R4	8.7R1	8.5R4	8.5R4	8.6R1	8.7R1	8.5R4
Storm Control	N	Y	Y	8.7R1	Y	Y	N	8.7R1	N
TACACS+ Client	8.5R1	Y	Y	8.7R1	Y	Y	8.6R1	8.7R1	Y
TACACS+ command based authorization	N	N	Y	8.7R1	Y	Y	N	N	N
PoE Features									
802.3af and 802.3at	8.5R1	Y	Y	8.7R1	Y	N	N	N	Y
802.3bt	N	8.6R2	N	8.7R1	N	N	N	N	N
Auto Negotiation of PoE Class-power upper limit	8.5R1	Y	Y	8.7R1	Y	N	N	N	Y
Display of detected power class	8.5R1	Y	Y	8.7R1	Y	N	N	N	Y
LLDP/802.3at power management TLV	8.5R1	Y	Y	8.7R1	Y	N	N	N	Y
HPOE support	8.5R1 (60W)	Y (95W)	Y (60W)	8.7R1 (95W)	Y (75W)	N	N	N	Y (75W)
Time Of Day Support	8.5R1	Y	Y		Y	N	N	N	Y
Perpetual PoE	N	N	Y	Y	Y	N	N	N	N
Fast PoE	N	N	Y	Y	Y	N	N	N	N
Data Center Features (License May Be Required)									
CEE DCBX Version 1.01	N	N	N	N	N	Y	N		N
Data Center Bridging (DCBX/ETS/PFC)	N	N	N	N	N	Y	N	N	N
EVB	N	N	N	N	N	N	N	N	N
FCoE / FC Gateway	N	N	N	N	N	Y	N	N	N
VXLAN[5]	N	N	N	N	N	Q32/X72	8.5R3	N	N
VM/VXLAN Snooping	N	N	N	N	N	Y	N	N	N
FIP Snooping	N	N	N	N	N	Y	N	N	N

Notes:
1. OS6560 supports stub area only.
2. See protocol support table in Appendix B.
3. Supported on OS6900-Q32/X72 models.
4. Site license required beginning in 8.6R1.
5. L2 head-end only on OS6900-V72/C32.

Appendix B: SPB L3 VPN-Lite Service-based (Inline Routing) / External Loopback Support / BVLAN Guidelines

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

Inline Routing Support		
	OmniSwitch 9900	OmniSwitch 6900-V72/C32 (Front panel port)
IPv4 Protocols		
Static Routing	Y	8.6R2
RIP v1/v2	Y	8.6R2
OSPF	Y	8.6R2
BGP	Y	8.6R2
VRRP	Y	8.7R1
IS-IS	N	N
PIM-SM/DM	8.5R3	8.6R2
DHCP Relay	8.5R3	8.6R2
UDP Relay	8.5R4	8.6R2
DVMRP	N	N
BFD	N	N
IGMP Snooping	Y	8.6R2
IP Multicast Headend Mode	Y	8.6R2
IP Multicast Tandem Mode	8.5R4	8.6R2
IPv6 Protocols		
Static Routing	8.5R4	8.6R2
RIPng	8.5R4	8.6R2
OSPFv3	8.5R4	8.6R2
BGP	8.5R4	8.6R2
VRRPv3	8.5R4	8.7R1
IS-IS	N	N
PIM-SM/DM	8.5R4	8.6R2
DHCP Relay	8.6R1	N
UDP Relay	8.6R1	N
BFD	N	N
IPv6 MLD Snooping	Y	N
IPv6 Multicast Headend Mode	Y	N
IPv6 Multicast Tandem Mode	8.5R4	N

External Loopback Support						
	OmniSwitch 9900	OmniSwitch 6860/6865	OmniSwitch 6860N	OmniSwitch 6900	OmniSwitch 6900-V72/C32	OmniSwitch 6900-X48C6/T48C6
IPv4 Protocols						
Static Routing	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1
RIP v1/v2	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1
OSPF	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1
BGP	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1
VRRP	8.6R1	8.5R4	8.7R1	Y	8.7R1	N
IS-IS	N	N	N	N	N	N
PIM-SM/DM	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1
DHCP Relay	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.7R1
UDP Relay	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.7R1
DVMRP	N	N	N	N	N	N
BFD	N	N	N	N	N	N
IGMP Snooping	8.5R4	Y	8.7R1	Y	8.6R1	8.7R1
IP Multicast Headend Mode	8.5R4	Y	8.7R1	Y	8.6R1	8.7R1
IP Multicast Tandem Mode	8.5R4	Y	8.7R1	Y	8.6R1	8.7R1
IPv6 Protocols						
Static Routing	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1
RIPng	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1
OSPFv3	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1
BGP	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1
VRRPv3	8.5R4	8.5R4	8.7R1	Y	8.7R1	N
IS-IS	N	N	N	N	N	N
PIM-SM/DM	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.7R1
DHCP Relay	8.6R1	8.6R1	8.7R1	8.6R1	8.6R1	8.7R1
UDP Relay	8.6R1	8.6R1	8.7R1	8.6R1	8.6R1	8.7R1
BFD	N	N	N	N	N	N
IPv6 MLD Snooping	8.5R4	Y	8.7R1	Y	N	N
IPv6 Multicast Headend Mode	8.5R4	Y	8.7R1	Y	N	N
IPv6 Multicast Tandem Mode	8.5R4	Y	8.7R1	Y	N	N

SPB BVLAN Scalability and Convergence Guidelines

If services are distributed across more than 4 BVLANs in the network it is recommended to consolidate them among just 4 BVLANs. This will reduce the scale of address updates that will happen in the control plane and also help improve network scalability, stability and convergence. Modifying the service BVLAN association is currently not supported. The service will need to be deleted and recreated on the new BVLAN, therefore it's suggested that the consolidation be done during a maintenance window to prevent network disruption.

In most SPB networks this is not a local operation on a single switch. The BVLAN is configured on all the switches in the network. A check must be performed to see if any service has been attached to the BVLAN. The check does not have to be on a local switch, the service attachment to the BVLAN can be on any switch in the network.

1. This will indicate that this is an active BVLAN.
2. Even if the service is not local to a node the node can act as a transit node for the active BVLAN. For this reason the BVLAN cannot be deleted from the network.

To determine if a BVLAN is active use the following command. If there is a service associated with the BVLAN then **In Use** will show as **Yes**. This is a network wide view so even if the services are active on a remote node, this local node will show that the BLVAN is active even if the services are not configured on the local node.

```
OS6860-> show spb isis bvlans
SPB ISIS BVLANS:
                                                                    Services  Num    Tandem
Root Bridge
BVLAN   ECT-algorithm     In Use  mapped    ISIDS  Multicast  (Name : MAC Address)
-------+-----------------+-------+---------+------+----------+-------------------------------
---------
  4000  00-80-c2-01       YES     YES           5  SGMODE
  4001  00-80-c2-02       NO      NO            0  SGMODE
```

After the services have been consolidated the idle BVLANs can be deleted across the entire network. Deleting idle BVLANs will have no effect on the existing network.

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 8.7R1 (GA)
OS6465	8.5.196.R04 (GA) 8.6.289.R01 (GA) 8.6.299.R01 (MR) 8.6.189.R02 (GA) 8.6.203.R02 (reGA) 8.7.277.R01 (GA) 8.7.280.R01 (MR)
OS6560	8.5.196.R04 (GA) 8.6.289.R01 (GA) 8.6.299.R01 (MR) 8.6.189.R02 (GA) 8.6.203.R02 (reGA)
OS6860(E)	8.5.196.R04 (GA) 8.6.289.R01 (GA) 8.6.299.R01 (MR) 8.6.189.R02 (GA) 8.6.203.R02 (reGA) 8.7.277.R01 (GA) 8.7.280.R01 (MR)
OS6860N	8.7.277.R01 (GA) 8.7.280.R01 (MR)
OS6865	8.5.196.R04 (GA) 8.6.289.R01 (GA) 8.6.299.R01 (MR) 8.6.189.R02 (GA) 8.6.203.R02 (reGA) 8.7.277.R01 (GA) 8.7.280.R01 (MR)
OS6900	8.5.196.R04 (GA) 8.6.289.R01 (GA) 8.6.299.R01 (MR) 8.6.189.R02 (GA) 8.6.203.R02 (reGA) 8.7.277.R01 (GA) 8.7.280.R01 (MR)
OS6900-V72/C32	8.5.196.R04 (GA) 8.6.289.R01 (GA) 8.6.299.R01 (MR) 8.6.189.R02 (GA) 8.6.203.R02 (reGA) 8.7.277.R01 (GA) 8.7.280.R01 (MR) See Appendix G when upgrading an OS6900-V72/C32.

OS6900-X48C6/T48C6	8.7.277.R01 (GA) 8.7.280.R01 (MR)
OS9900	8.5.196.R04 (GA) 8.6.289.R01 (GA) 8.6.299.R01 (MR) 8.6.189.R02 (GA) 8.6.203.R02 (reGA)

8.7R1 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 U-Boot 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 8.6.289.R01 GA, July 14, 2019.,
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:  MON AUG 12 2019 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
    - If upgrading an OS6465-P28, upgrading the FPGA to version 0.7 is required to address CRAOS8x-12042.
    - AOS must be upgraded prior to upgrading the FPGA. See Appendix F.
- OS6560 – Nos.img
    - If upgrading an OS6560-P48Z16 (904044-90), OS6560-48X4, OS6560-P48X4, OS6560-X10, upgrading the FPGA may be required to address CRAOS8X-16452.
    - AOS must be upgraded prior to upgrading the FPGA. See Appendix F.
- OS6860 – Uos.img
    - Upgrading the FPGA is required for fast and perpetual feature support only.
- OS6865 – Uos.img
    - If upgrading an OS6865-U28X, upgrading the FPGA to version 0.12 may be required to address CRAOS8X-4150. See Appendix F.
    - Upgrading the FPGA is required for fast and perpetual feature support only.
    - AOS must be upgraded prior to upgrading the FPGA. See Appendix F.
- OS6900 - Tos.img
    - If upgrading an OS6900-X72, upgrading the FPGA to version 0.1.11 is required to address CRAOS8X-11118. See Appendix F.
    - If upgrading an OS6900-X72, upgrading the u-boot/miniboot to version 8.6.189.R02 is required to address CRAOS8X-11118. See Appendix F.
- OS6900-V72/C32 – Yos.img. See Appendix G.
- 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           8.7.354.R01             239607692 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:

- OS6465 – Nos.img
    - If upgrading an OS6465-P28, upgrading the FPGA to version 0.7 is required to address CRAOS8x-12042.
    - AOS must be upgraded prior to upgrading the FPGA. See Appendix F.
- OS6560 – Nos.img
    - If upgrading an OS6560-P48Z16 (904044-90), OS6560-48X4, OS6560-P48X4, OS6560-X10, upgrading the FPGA may be required to address CRAOS8X-16452.
    - AOS must be upgraded prior to upgrading the FPGA. See Appendix F.
- OS6860 – Uos.img
    - Upgrading the FPGA is required for fast and perpetual feature support only.
- OS6865 – Uos.img
    - If upgrading an OS6865-U28X, upgrading the FPGA to version 0.12 may be required to address CRAOS8X-4150. See Appendix F.
    - Upgrading the FPGA is required for fast and perpetual feature support only.
    - AOS must be upgraded prior to upgrading the FPGA. See Appendix F.
- OS6900 - Tos.img
    - If upgrading an OS6900-X72, upgrading the FPGA to version 0.1.11 is required to address CRAOS8X-11118. See Appendix F.
    - If upgrading an OS6900-X72, upgrading the u-boot/miniboot to version 8.6.189.R02 is required to address CRAOS8X-11118. See Appendix F.
- OS6900-V72/C32 – Yos.img. See Appendix G.

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
```

- 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           8.7.354.R01              239607692 Alcatel-Lucent OS
```

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 / U-boot Upgrade Procedure

The following CRs or features can be addressed by performing an FPGA/CPLD or U-boot upgrade on the respective models.

CR / Feature	Summary
CRAOS8X-12042	OS6465-P28 - Switch does not shutdown after crossing danger threshold temperature. (FPGA version 0.7)
CRAOS8X-7207	OS6560-P24Z24,P24Z8,P48Z16 (903954-90) - Chassis reboots twice to join a VC. (FPGA version 0.7)
CRAOS8X-4150	OS6865-U28X - OS6865-U28X VC LED status behavior. (FPGA version 0.12)
Fast/Perpetual PoE	OS6860/OS6865 Fast and Perpetual PoE (8.7R1)
CRAOS8X-11118	OS6900-X72 - 1000BaseT SFP interface up before system ready (8.7R1) - (U-boot version 8.6.R02.189) - (FPGA version 0.1.11)
CRAOS8X-16452	OS6560-P48Z16 (904044-90), OS6560-48X4, OS6560-P48X4, OS6560-X10 - Port remains UP when only SFP is connected.

Note: AOS must be upgraded prior to performing an FPGA/CPLD or U-boot upgrade.

1. Download and extract the upgrade archive from the Service & Support website. In addition to the AOS images, the archive will also contain an FPGA upgrade kit and U-boot file, for example.

- CPLD File - fpga_kit_7023
- U-boot.8.6.R02.189.tar.gz

2. FTP (Binary) the files 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, for example:

```
-> update fpga-cpld cmm all file fpga_kit_7023
Parse /flash/fpga_kit_7023
fpga file: OS6900-X72_CPLD_V01B_20191204.vme
Please wait...
fpga file: OS6900-X72_CPLD_V01B_20191204.vme
update chassis 1
Starting CMM ALL FPGA Upgrade
CMM 1/1
Successfully updated
Reload required to activate new firmware.
```

4. If required, a u-boot upgrade can then be performed, for example:

```
-> update uboot cmm all file /flash/u-boot.8.6.R02.189.tar.gz
Starting CMM ALL UBOOT Upgrade
Please wait...
CMM 1/1
u-boot-ppc_2040.bin: OK
U-boot successfully updated
Successfully updated
```

5. Once complete, a reboot is required.

Appendix G: OS6900-V72/C32 Flash Cleanup Procedure / FEC Disable

Prior to performing a standard or ISSU upgrade on an OS6900-V72/C32 it's required to perform a cleanup of some files in the flash memory. This procedure must be performed when upgrading from the releases listed below. A script file has been created that will automatically perform the file cleanup on a VC or standalone chassis. It must be run from the maintenance shell prior to upgrading.

Additionally, the script will prompt the user to confirm if an ISSU upgrade is being performed. If an ISSU upgrade is being performed the script will create an additional file (*issu_no_fec_vfl_pre_86R2*) in the **/flash** directory on both chassis in the VC. This file will prevent (Forward Error Correction) FEC from being automatically enabled after the upgrade on any 10G/40G VFLs, which is the default setting beginning in 8.6R2. This prevents a FEC mismatch between the Master and Slave chassis (enabled on Slave chassis / disabled on the Master chassis) during the ISSU upgrade.

- Standard Upgrade
  - If upgrading from AOS Release 8.5R02, 8.5R03, or 8.5R04 - Script file will perform flash cleanup.
  - If upgrading from AOS Release 8.6R01 or later - Script file not needed.
- ISSU Upgrade
  - If upgrading from AOS Release 8.5R04 - Script file will perform flash cleanup and FEC disable.
  - If upgrading from AOS Release 8.6R01 - Script file will perform FEC disable.
- Script file name: ***pre_update_script.sh*** (Available from service & support website)
  - **Note**: An error, "**/mnt/chassis*: No such file or directory**", may be displayed when running the script on a standalone chassis. This error has no affect on the upgrade.

1. FTP the script file to the **/flash** directory on the Master chassis of the VC or standalone chassis.
2. OS6900-> su
3. YUKON #-> cd /flash
4. YUKON #-> sh pre_update_script.sh
5. YUKON #-> exit
6. OS6900->
7. You may now proceed to performing a standard or ISSU upgrade.
8. If performing an ISSU upgrade, perform the following after the upgrade is complete:

   - Delete the *issu_no_fec_vfl_pre_86R2* file from the **/flash** directory.
   - Enable FEC on the VFL ports using the '**interfaces *chassis*/*slot*/*port* fec auto**' command. Enable FEC on a pair-by-pair basis.

Appendix H: Fixed Problem Reports

The following problem reports were closed in the 8.7.277.R01 release.

CR	Description
Case: **00483135** *CRAOS8X-17251*	**Summary:** VC-takeover caused UNP users to go into No Static Service Resource / Block State. **Explanation:** UNP users could not get a new SAP entry created as stale SAP entries were still present, caused by a SAP information not synchronized between the new master chassis and the former master chassis. Click for Additional Information
Case: **00477035** *CRAOS8X-20414*	**Summary:** Swlogs AGCMM display too many information at INFO level, related to mac address added or removed. **Explanation:** Those AGCMM information can fill up the swlogs completely on networks using heavily UNP users. These information should be displayed at DEBUG3 level, not INFO level. Click for Additional Information
Case: **00454134** **00442385** *CRAOS8X-16250*	**Summary:** 6900-V72: SPB L3 routes lost due to memory exhaustion. **Explanation:** SPB L3 routes are lost with the swlog error message "swlogd isis_spb_0 ERROR ALRM: SPB-ISIS task is out of memory". Issue is resolved by reloading the switch. Click for Additional Information
Case: **00446640** *CRAOS8X-16700*	**Summary:** OS6560 running in AOS 8.6.R01 reboots generating PMD when PVST+ port connected to Cisco device. **Explanation:** Switch crashed as it received PVST+ TCN BPDU from Cisco. In current code, this BPDU should be dropped as PVST+ is enabled. While dropping PVST+ BPDU an exception occurred as Vlan TLV field was not present, causing switch to crash and generates PMD stpNi task. This issue is fixed in AOS 8.7.R01. Click for Additional Information
Case: **00451171** *CRAOS8X-17699*	**Summary:** OS6560-24X4/P24X4 Port 1/1/25 and 1/1/26 link status down. **Explanation:** In OS6560-24X4 switch, Port 1/1/25 & 1/1/26 Auto-negotiation is enabled at Switch global CLI(ESM level) but it is disabled at hardware level and changed the INBAND auto-negotiation enabled by default. Click for Additional Information
Case: **00457943** *CRAOS8X-17893*	**Summary:** OSPF checksum calculation mismatch/error in OS9900 switch running AOS 8.6.R01. **Explanation:** When OSPF packet transmitted across interface, Transmitting node will generate packet along with checksum and the receiving end will correlate incoming packet checksum with

	checksum generated at receiving node. There is mismatch reported on packet from transmitting node. Click for Additional Information
Case: **00444765** **00453364** **00473075** *CRAOS8X-16452*	**Summary:** 6560: 10G interface remains UP when only SFP is connected. **Explanation**: 10G interface status remains UP and LED is ON when only an SFP, without any fiber cable, is connected to the interface. As the port remains UP, the mac-addresses learnt on the port are not immediately flushed. This creates connectivity issues. Click for Additional Information
Case: **00432146** *CRAOS8X-15564*	**Summary:** OS6900: Packet loss is seen when gratuitous ARP packet is received on SAP port of hair-pin loop. **Explanation:** Invalid ARP entry is created when a gratuitous ARP is received on a SAP port. This happens when there is a hair-pin loop and a default vlan is mapped on the hair-pin linkagg and the vlan linkagg. Click for Additional Information
Case: **00454134** *CRAOS8X-17258*	**Summary:** 6900-V72: SPB L3 routes lost due to memory exhaustion. **Explanation:** SPB L3 routes are lost with the swlog error message "swlogd isis_spb_0 ERROR ALRM: SPB-ISIS task is out of memory". Issue is resolved by reloading the switch. Click for Additional Information
Case: **00444456** CRAOS8X-16465	**Summary:** Cannot configure a port as SAP service access port if an IP interface exists for the default VLAN of the port. **Explanation:** A switch port cannot be configured as SAP service access port if an IP interface exists for the default VLAN mapped on the port. Following error messages is printed: ERROR: A vlan with IP interface attached to this port is not supported! (NETWORK PORT: 0x1). Click for Additional Information
Case: **00474955** CRAOS8X-20567	**Summary:** OS6560: DHL configuration having a space in the DHL name is lost upon reload. **Explanation**: OS6560: DHL configuration having a space in the DHL name is accepted and saved without the quotation marks. The configuration is lost upon reload. Click for Additional Information
Case: **00469503** CRAOS8X-19568	**Summary**: AP-225 connected with two ports to the same OS6860-P48switch does not power up. **Explanation**: The OS6860 switch detects the AP as legacy device when both the ports are connected to the same switch. Lanpower-capacitor detection needs to be enabled in order to power up the AP. Click for Additional Information

Case: **00441096** CRAOS8X-16685	**Summary:** The Polycom IP-Phone connected to OS6860 switch reboots continuously due to EAP-ID mismatch. **Explanation:** The OS6860 switch increments EAP-ID in EAP success packet which is detected as mismatch by Polycom IP-Phone and it rejects the same. Hence the IP-Phone reboots. Click for Additional Information
Case: **00448033** **00477752** CRAOS8X-16808	**Summary:** The write-memory fails on OS6860 switch after upgrade to 8.6 R02. **Explanation:** The issue is seen as the vlan manager (VM) snapshot stops responding due to excessive configuration in vlan manager. The workaround is to optimize the vlan configuration by using the vlan range commands and using the default description for vlans. Click for Additional Information
Case: **00429279** CRAOS8X-15153	**Summary:** OS9900 XNI-U48 rebooted after upgrade to AOS 8.6.R01. **Explanation:** OS9900-XNI-U48 NI crashed after the switch is upgraded to 8.6.289 R01 generating the PMD. From the PMD the suspended task is stpNi. Click for Additional Information
Case: **00449934** **00476852** CRAOS8X-17029	**Summary:** OS9900 drops the packets when only one port is available in SAP linkagg. **Explanation:** When the switch is configured with SPB inline routing, where routes ingress and egress packets use same SAP port, the egress packets are dropped. Click for Additional Information
Case: **00441765** CRAOS8X-16227	**Summary:** LLDP statistics show constant growing number of TLV discards and LLDPU errors for All LLDP frames received from the port connected to a STELLAR AP 1221. There is no warning/error messages present in the swlogs. **Explanation:** The LLDP packets received from this AP contained mismatching auto negotiation/Status flags and caused increases of TLV discards and LLDPU errors. This was seen on OS6860 running 86R01, with AP 1221 running 3.0.7.26 build. Click for Additional Information
Case: **00467838** CRAOS8X-19116	**Summary:** OS6860: 10MB and 100MB links showing Error frames (exact same amount of packets than the Tx Frame losses). **Explanation:** Error frames calculation was incorrect and was counting TX frame losses as error frames for the lower speed interfaces. Issue was seen on 86R02. Click for Additional Information
Case: **00386473** CRAOS8X-10615	**Summary:** OS6900 memory consumption more than 100%. **Explanation:**

	Switch health displays memory more than 100% during high memory state and this is a display issue. Click for Additional Information
Case: **00431225** CRAOS8X-15486	**Summary:** DHCP IPSF configuration not completely visible in the OS6860 switch. **Explanation:** In the VC of OS6860 switch with more than 5 NIs in the VC, the master switch displays the DHCP IPSF configuration of first 5 NIs only. This is a display issue, since IPSF configuration is applied properly on all the NIs in the VC. Click for Additional Information
Case: **00464070** CRAOS8X-18462	**Summary:** Power-Rule configured in the OS6560 switch does not work as expected. **Explanation:** Power-Rule configured to Power ON and OFF the PD devices at a particular time is always delayed. The delay interval is always random and there is no workaround for this issue. Click for Additional Information
Case: **00439333** CRAOS8X-16237	**Summary:** DHCP-Decline packets are dropped by the OS6860 switch. **Explanation:** If DHCP snooping feature is enabled in the OS6860 switch, it drops the DHCP-Decline packet from the End device. DHCP-Decline is a “client to server” packet and it should not dropped by the DHCP snooping in the untrusted port. Disabling the DHCP snooping feature is the only workaround. Click for Additional Information
Case: **00438147** **00456826** **00473115** **00455366** **00447253** **00473607** CRAOS8X-16020	**Summary:** lpNi LanNi and LanXtr ERR are continuously generated in the swlogs of OS6860&OS6860E switches. **Explanation:** When frequent I2C packets are sent to PoE controller and the I2C processing is bit slow, the buffer list in OS6860/OS6860E switch would get full. If the buffer list is full then the switch would generate these error messages. There is no functional impact, and the PD device would still continue to get lanpower from switch. Click for Additional Information
Case: **00442690** **00448287** CRAOS8X-16284	**Summary:** OS6465 frequently generating "lpNi LanXtr" and "intfNi Drv" INFO logs. **Explanation:** OS6465 switch periodically sends a command to the controller to get the power supply voltage and hence the "lpNi LanXtr" messages are printed with the power supply information. "intfNi Drv" messages are triggered whenever PoE Port status is read from the PoE controller. There is no functional impact in the switch due to this event. Click for Additional Information
Case: **00443661** **00468900** CRAOS8X-16344	**Summary:** "LanCmm ERR" continuously generated in the switch logs. **Explanation:** When the chassis with the PoE configuration suddenly removed from the VC, the chassis info would still be available in the lpVcCmmInfoMap until the next reboot. When the lpCmm tries

	to send messages to slots, it would check all the chassis-ID in lpVcCmmInfoMap and if corresponding chassis is not physically available, the lpCmm would throw this error messages. Reload of complete Virtual Chassis would stop the switch to genenrate this error and there is no potential issue due to this error. Click for Additional Information
Case: **00419763** CRAOS8X-13812	**Summary**: Missing data when using the timestamp operand in the "show log swlog command". **Explanation**: When using the timestamp operand in the "show log swlog" command there are instances where not all of the data is displayed. This can lead to incorrect diagnosis / conclusions when troubleshooting an issue. Click for Additional Information
Case: **00411071** CRAOS8X-13167	**Summary**: Packet loss with dynamic MAC Sec on OS6465 after the key rotation. **Explanation**: There is a traffic loss spiked noticed after each 4th key rotation. Click for Additional Information
Case: **00440835** CRAOS8X-16200	**Summary**: Upgrade from OV Cirrus to AOS 8.x Virtual Chassis fails. **Explanation**: When upgrade is performed from OV Cirrus, a new directory cloud is created on switch and used as new running-directory. However, in case of Virtual Chassis, the vcsetup.cfg is not copied on slaves. From AOS 8.7.R01 and for future upgrade, the current running-directory will be used. Click for Additional Information
Case: **00440283** CRAOS8X-16128	**Summary**: Upgrade from OV Cirrus to OS6560 and OS6465 resulting of low flash. **Explanation**: When upgrade is performed from OV Cirrus, a new directory cloud is created on switch and used as new running-directory. However for the access switches like OS6560 and OS6465 that do not have much space in flash, this operation results in flash becoming full. From AOS 8.7.R01 and for future upgrade, the current running-directory will be used. Click for Additional Information
Case: **00449271** CRAOS8X-16811	**Summary**: IoT Enforcement done by OV 4.5R01 does not work on AOS 8.x switches when connecting supplicant devices. **Explanation**: When enforcement is performed from OV (switch receives the new UNP profile by SNMP set), the switch is sending an EAP failure packet to supplicant resulting of re-authentication. Click for Additional Information
Case: **00455303** CRAOS8X-17948	**Summary**: Dynamic MAC Sec not operational on OS6465 Ports 1/1/23-24 after port toggling. **Explanation**: Issue specific to PHY 1548P that locks MAC Sec when port link state moved from UP to DOWN.

	Click for Additional Information
Case: **00451278** CRAOS8X-16934	**Summary:** "No licenses in install map" error observed on console port when applied MAC Sec license. **Explanation:** The file license.dat contains invalid license (wrong length). Click for Additional Information
Case: **00434293** CRAOS8X-15698	**Summary:** IoT Profiling does not work for Alcatel IPTouch if auto-phone qos is enabled. **Explanation:** Issue specific to OS6860 and OS6900, by default the auto-phone qos is enabled and fingerprint is not sent to OmniVista when connecting an IPTouch on UNP Port. Click for Additional Information
Case: **00451056** CRAOS8X-17006	**Summary:** MAC Sec does not establish (operational status down) and no secure association created **Explanation:** On swlogs is noticed error "CP is entering in state ABANDON" when we expect transmitting. Click for Additional Information
Case: **00435119** CRAOS8X-15779	**Summary:** From OV Cirrus, if we apply a SNMP User v3 password with suffix"*" into the SNMP Management template, switch is not manageable. **Explanation:** Switch appears DOWN on OV Cirrus Managed Devices page because of SNMP authentication timeout. Click for Additional Information
Case: **00440659** CRAOS8X-16189	**Summary:** OS6560 as mDNS edge switch does not forward traffic into L2GRE Tunneling. **Explanation:** OS6560 is not tunneling mDNS packets because TCAM rules are disabled. Click for Additional Information
Case: **00466169** **00476023** *CRAOS8X-18923*	**Summary:** Persistent high memory seen on OS6560-24X4 switch due to continuous link flap. **Explanation:** CSPD task register itself to link-flap event. For every link-flap event, it allocates some memory and does not free it. The leak is small but if the link-flap happens many times, the leak become bigger. As a workaround, reboot of the switch helps to release the memory. Click for Additional Information
Case: **00448426** *CRAOS8X-16769*	**Summary:** Documentation update is required in Network and CLI guide for QoS port maximum depth default value & egress/ingress bandwidth. **Explanation:** Changes done under "qos port" CLI and corresponding show outputs. Click for Additional Information
Case: **00441623** *CRAOS8X-16326*	**Summary:** In OS6560, QoS is unable to find the host part from the mask configured in the policy condition source ip and traffic was denied instead of allow.

	Explanation: There are two rule structures maintained. One will be in Hardware level and the other will be in software level. In the issue scenario, "Accept" rule is missing in software level, but the "Deny" rule is present. This is the reason, the accept rule which has high precedence is not taking effect over deny which has low precedence. Reported problem has been fixed. 🔒 Click for Additional Information
Case: **00427579** *CRAOS8X-14933*	**Summary:** OS9900/OS6560 dropping non-zero Sender IP in ARP unicast/broadcast packets in Qos DENY rule under SRC network group of 0.0.0.0 mask /8 **Explanation**: ARP is treated as an L3 packet which is expected and Sender IP of the ARP should be checked to check the Qos policy source network group for matches. However, as the ARP packet do not have the IP header, software assumes the source IP address as 0.0.0.0 though the Sender IP of ARP are non-zero. As a workaround, to configure explicit ARP allow in the Qos with precedence more than Qos DENY rule. 🔒 Click for Additional Information
Case: **00450525** *CRAOS8X-17923*	**Summary:** 6860E has “Authentication failure: Temporarily out of resources, please try again” for both MAC and 802.1x supplicant authentication. **Explanation**: This is due to the configuration changes done in the " AAA radius-server" command to first enter the key wrongly under host part of the command and then followed by the correction of the key in the same command. Reported issue has been fixed. 🔒 Click for Additional Information
Case: **00407627** *CRAOS8X-12403*	**Summary:** "Pending changes" field is missing in "show qos config" command output. **Explanation**: This output explains the status if the Qos is applied after configured. It is added as follows in the 8.7.R01: Under ->show qos config, cli command, QoS Configuration Admin = enable, **Pending changes = none** 🔒 Click for Additional Information
Case: **00452640** *CRAOS8X-17233*	**Summary:** CPU utilization is at 50% for OSPF task in OS6560-P24X24. **Explanation**: The switch enters in the select process in OSPF repeatedly due to socket issues between IPCMM and OSPF. As the switch keeps entering in select process in loop for OSPF again and again, the CPU spikes. 🔒 Click for Additional Information
Case: **00401386** **00409716** *CRAOS8X-12591*	**Summary:** Dump file is created after applying the content of the script file during Automatic Remote Configuration Download process. **Explanation**: “Reload working no rollback timeout” and “write memory” in the script file in instructions.alu file when executed, the PMD files are created.

	These commands are not to be executed via the script file as per the switch management guide as well. Correction has been done to throw error and avoid the dump file creation if these commands are executed via the script file. Click for Additional Information
Case: **00445674** *CRAOS8X--17741*	**Summary:** Description for hash-control MIB to be updated for the MIB: "alaCapManHashControlCommands". **Explanation**: Corrected the MIB description as follows: Click for Additional Information
Case: **00462882** **00471235** *CRAOS8X-15875*	**Summary:** After any SSH login to the switch lots of SSH messages are appeared in the swlog. **Explanation:** In AOS 8.6.R02, ssh has been upgraded to openssh7.7p1 and this is the reason that all these logs are displayed mistakenly in the switch logs. These messages will be suppressed in 87.R01 Click for Additional Information
Case: **00462198** *CRAOS8X-18177*	**Summary:** After OS9900 executes CMM takeover, linkaggs no longer work. **Explanation:** This issue is due to communication issue between CMM and NI. where the NI received corrupted packets from the CMM, causing the linkagg on the NI to crash and fail to re-initialize. This issue will be fixed in 8.7.R01. The new firmware will allow the linkagg to recover and be reinitialized. Click for Additional Information
Case: **00408139** **00451040** **00415801** **00448690** **00453084** **00427009** *CRAOS8X-14598*	**Summary:** With only the SFP-10G-SR transceiver module connected to port of OS6560-P48X4, without any cable, port operational status is up. Traffic counter is increasing and port flapping is observed. **Explanation:** RECEIVE FAULT bit is set on PMA_PMD (register 8, device 1). After clearing this register (device 1 register 8), able to see the port functioning properly, while previously it use to flap every 10 seconds. Click for Additional Information
Case: **00457281** **00436286** **00463574** *CRAOS8X-15887*	**Summary:** The "lpNi LanNi INFO: Port 17 FAULT State change 1b to 1c desc: Port is off: Non-802.3AF/AT powered device (Non-standard PD connected)" message is seen continuously in the logs. **Explanation:** This log message will be moved to debug3 level as from AOS 8.7R01. Click for Additional Information
Case: **00443527** *CRAOS8X-16437*	**Summary:** Core switch rebooted due to invalid SIP packet. **Explanation:** Crash occurred due to an invalid SIP packet. Address of SIP transaction points to invalid address. So from SIP transaction, trying to dereference any value leads to crash.

	Click for Additional Information
Case: **00461094** *CRAOS8X-17031*	**Summary:** Log message "linkAggNi main ERR: [1:1] -> [la_ni_hw_lacp_frame_trt.cpp:598] pktdrv_xmit_writebuffer Failed port:1/1/27(26) ret:-1 errno:3 error" seen prior to OS6465 switch reboot. **Explanation:** Above error message is seen, as during the switch reboot, packet driver cannot transmit the packet to the allocated buffer, i.e TX DMA. The reboot itself occurred due to switch running out of memory from NTP task memory leak (issue fixed in 8.6 203.R02). Click for Additional Information
Case: **00467907** *CRAOS8X-19790*	**Summary:** Slave chassis does not inherit permanent Data Center (DC) license from the Master chassis and the Virtual Chassis (VC) is not formed. The Slave chassis is put into "Mis-Configured-License". **Explanation:** The Slave chassis will not inherit the permanent DC license from the master chassis, as the DC license is bound to a specific switch's serial number and the MAC address. In such a case, the slave is put into "Mis-Configured-License". All switches within a VC should have their own DC license. The switch management guide has been corrected. Click for Additional Information
Case: **00463784** *CRAOS8X-18855*	**Summary:** Minimum age password policy failing to work. For instance when setting the minimum age password policy to 1 day, as expected, the user was not able to change the password before the end of 1 day. After 1 day the user can change his password as expected. **Explanation:** With the fix, once the password minimum age is elapsed, the user can only modify the password once, after which, the password age is reset, & the user has to wait for the configured password minimum age to elapse again, before a password change is allowed again. Click for Additional Information
Case: **00476702** *CRAOS8X-20382*	**Summary:** OS6900-V72 switch rebooting frequently with IPRM pmd file generated. **Explanation:** The issue is due to pointer memory corruption while deleting export tree leaf node. Code changes have been made in AOS 8.7R01 to modify the way export tree leaf nodes are deleted. Click for Additional Information
Case: **00445117** *CRAOS8X-16445*	**Summary:** The switch is rebooting after receiving the SNMP OID for pause frame. **Explanation**: The LAG OID for pause frame is taken and added as missing OID or random number at the end: LAG OIDs "interface" start with 40000001. OIDs 40000001, 40000002 and 40000003 will not cause a reboot, even if the lag does not exist. However, any other OID will cause a reboot. Click for Additional Information
Case: **00444932**	**Summary:** OS6860: Re-authentication for MAC authenticated users.

CRAOS8X-16603	**Explanation:** The new command will be available in the release AOS 8.7.R01 to allow mac session timeout. From the CLI, the session timeout can be configured from 300 to 172800 seconds [default 43200]. Click for Additional Information
Case: **00450967** *CRAOS8X-17188*	**Summary:** TTL value of Echo Request can vary, however, the TTL value of Echo Reply should always be 64. TTL value of the ICMP Echo Reply is copied from the Echo Request packet **Explanation:** TTL value of the ICMP Reply will be always set to 64 Click for Additional Information
Case: **00461489** **00451595** **00465423** **00473404** **00465409** **00478048** **00453977** **00453998** **00449856** **00479320** *CRAOS8X-17830*	**Summary:** OS6860 memory spiked from 50 to 80 after the upgrade to 8.6.R02 **Explanation:** It is because of some enhancements in 8.6 R02 release, calculations are added for un-accounted memory areas. Click for Additional Information
Case: **00448782** *CRAOS8X-16930*	**Summary:** The Vc is splitting after upgrading from 8.5R04 to 8.6R02. **Explanation**: The switch qos condition used is altering with the qos cache and making the switch to drop/not take account of VC-ISIS packets to form the VC Click for Additional Information
Case: **00408611** *CRAOS8X-12487*	**Summary:** False Splitter cable message is displayed once fiber/DAC cable is connected. **Explanation:** The ports 1/1/1-48 of 6900V72 switch are not supporting splitter cables however if a normal cable is connected to the above range of ports a displayed message showing it as a splitter cable. Click for Additional Information
Case: **00408634** *CRAOS8X-12489*	**Summary:** Some display differences on show interface output. **Explanation:** The speed of linkagg member display is wrong, 25G configured speed is displayed instead of 10G when the 10G cables is used as well as one of the linkagg members is showing the autoneg enable instead of disable. Click for Additional Information
Case: **00458056** **00433949** *CRAOS8X-17470*	**Summary:** SNMP polls failing to complete and timing out. **Explanation:**

	SNMP polling timeouts which are not related to device reachability. This latency issue, along with the switch receiving many snmp get bulk request which query a non-existing object in a short interval, caused the snmpwalk to time out. Click for Additional Information
Case: **00462031** *CRAOS8X-18144*	**Summary:** Show commands are missing from swlog as well as tacacs accounting server. **Explanation:** Tacacs server as well as swlog files are not having the show/read commands typed into switch. Click for Additional Information
Case: **00475207** *CRAOS8X-20294*	**Summary:** Vlan configuration duplication post upgrade to 8.6.203.R02. **Explanation:** The configuration of existing vlan name and admin-state is duplicated many time after upgrade to 8.6.203R02. Click for Additional Information
Case: **00473155** *CRAOS8X-20036*	**Summary:** The result of SNMP OID of show qos qsi port stats is giving a rate value instead of counter value. **Explanation**: As per the SNMP MIB the value returned for the concerned OID should be counter and not a rate value. The CLI output is giving the right value, the change is aiming to provide a counter value once OID is polled like the CLI output result. Click for Additional Information
Case: **00436299** *CRAOS8X-15923*	**Summary:** One specific SPB service was impacted in SPB network. The servers belong to this service were completely down. **Explanation**: The communication between servers has been lost. BCB was learning mac-address details of both VMs. However the corresponding BEBs are not learning mac details of remote serves. A correction has been done in the multicast replication subsystem and issue has been fixed. Click for Additional Information
Case: **00474630** *CRAOS8X-20178*	**Summary:** 6900-V72: SPB BVLAN 4000 tag removed in UNI encapsulation in ethernet-service (cvlan all). **Explanation**: The problem was with encapsulating SPB traffic through OS6900-V72 in UNI-NNI (ethernet-service) configuration. The tag of bvlan 4000 is removed between UNI and NNI, A regular CVLAN tag was not getting affected, whereas only SPB control BVLAN which was configured as CVLAN ALL is getting removed where the control vlan 4000 for ISIS hello packet, the cvlan tag 4000 is removed. Issue has been identified as a bug and fix would be available from AOS 8.7 R01 GA. Click for Additional Information
Case: **00448838** *CRAOS8X-16757*	**Summary:** When inserting SFPs into the switch – LED for PS slot-2 lit orange for a very short time and on console, power supply related information was getting printed.

	Explanation: Issue has been identified as a bug and fix would be available from AOS 8.7 R01 GA. Click for Additional Information
Case: **00444802** **00451333** **00466551** *CRAOS8X-16886*	**Summary:** OS6560-P24X4 LACP negotiation issue on port 25/26 **Explanation**: AOS switch Model OS6560-P24X4 connected to another switch via linkagg with ports 1/1/25 and 1/1/26 (fiber switch ports). After performing an upgrade on OS6560-P24X4 from 86R01 to 86R02, LACP negotiation issue pop up with partner switch. Issue has been identified as related to DUAL MM SFP used on switch ports belongs to OS6560-P/24X4 and 48X4 model switches. Click for Additional Information
Case: **00429021** *CRAOS8X-15051*	**Summary:** UNP users were connected to all 4 units of the stack and are in same subnet, however users connected on Unit-4 were able to communicate only with user connected on unit-4 alone but not with rest of the users connected on 3 other units part of same VC. **Explanation**: Issue is identified as Mac entry flush at Hardware level in the VC. All other switches of the VC (1, 2 & 3) other than the unit (unit-4) where PC is directly connected to are flushing the PC's mac address in Hardware. The mac-address flush is happening due to timing issue by mac-aging on the switch with corresponding to UNP and is not updating the re-learned mac entry of the PC to other units in the VC. Click for Additional Information
Case: **00425790** *CRAOS8X-16121*	**Summary:** On OS6860E, configured port as UNP type access and classification based on phone's mac-oui. Once in every 30 sec, phone is not working and regains connectivity by itself. **Explanation**: Switch received tagged packet from phone with Vlan ID x, as per configuration the user moved to profile P1 under vlan x. Now the same user has sent LLDP frame as untagged, switch has moved the user from vlan x to vlan 1 and is still under profile P1. Hence traffic for voice vlan (vlan x) is not getting transmitted to phone. Code changes have been done so that LLDP frame should not be considered for reclassification if already mac-address from the same user exists on the respective UNP port. Click for Additional Information
Case: **00454259** *CRAOS8X-17509*	**Summary:** Checking the interface uptime/downtime details using MIB OIDs is not giving constant results though the port status is unchanged. **Explanation**: The value of the ifLastChange (1.3.6.1.2.1.2.2.1.9) is not static. The "last interface changed" outputs are changing while doing the snmpwalk. Observed problem has been identified as a bug and fix would be available in AOS 8.7 R01 GA. Click for Additional Information
Case: **00438864** *CRAOS8X-16054*	**Summary:** OV2500/NMS station was receiving multiple duplicate notifications from AOS switches whenever single link flap event occurs on a port which is part of Linkagg. **Explanation**:

	The OV2500/NMS station was receiving the duplicate notifications, the description of all the notifications about linkagg leave or join are the same. One SNMP trap for Link down/up event followed by 4 SNMP traps about linkagg leave/join has been observed. All these 4 traps are absolutely same and duplicate to each other in the same second of time. This is the reason OV2500 (NMS station) is displaying 4 linkagg leave/join traps for single link toggle event. Click for Additional Information
Case: **00341536** *CRAOS8X-6157*	**Summary:** No authentication is triggered when an ALE IP phone is connected on a UNP classification enabled port. **Explanation**: The issue is only with the IP phones MAC ranging from "00:80:9f:00:00:00 – 00:80:9f:ff:ff:ff and 00:13:fa:00:00:00 – 00:13:fa:ff:ff:ff". The rule "UNP Vlan STP blk" is not hit when default VLAN is disabled for IP phone MAC connected ports. **As a workaround, e**nable default VLAN on the port or qos no phones qos apply Click for Additional Information
Case: **00393014** *CRAOS8X-11118*	**Summary:** 1000Base-T SFP interface on OS6900-X72 comes up becomes up even before the reboot process is complete. **Explanation:** Port with 1000Base-T goes down when the switch starts rebooting. The port comes up 20 seconds after the switch reboot. Again after 5 minutes 20 seconds, the port goes down and will come up once the switch reaches L8 state. Click for Additional Information
Case: **00460036** *CRAOS8X-17883*	**Summary:** OS6465 switches do not shut down after crossing danger threshold temperature. **Explanation:** According to hardware specification, the switch should shutdown whenever the switch board temperature reaches the danger threshold. However, OS6465 switches continue to operate even after crossing the danger threshold temperature. Click for Additional Information
Case: **00456191** *CRAOS8X-17434*	**Summary:** Unable to perform SNMPwalk to MIB "alaQoSAppliedRuleTable" and the output of "show active policy rule" simultaneously. **Explanation:** If we run SNMPwalk to MIB "alaQoSAppliedRuleTable" and at the same time run the output of "show active policy rule", it will throw an error stating "Already have an active command on session 65535". Click for Additional Information
Case: **00460040** *CRAOS8X-17884*	**Summary:** OS6465-P6/P12 - Missing powersupply entry in the output, no traps while removing powersupply/power cord. **Explanation:** OS6465 running with two powersupplies configured manually, when one of the powersupply's cord is unplugged, the entry of the respective powersupply is removed from the "show powersupply" output. Also, there is no trap generated for the powersupply removal.

	Click for Additional Information
Case: **00464243** *CRAOS8X-19272*	**Summary:** Unique Local Private IPv6 prefixes do not get installed via eBGP node. **Explanation:** The Unique Local IPv6 prefix((starts with fd::) is picked up in the BGP routing table since the redistribution of local into bgp is configured on OS6900. However, it is not advertised to the EBGP neighbor switch. Click for Additional Information
Case: **00464282** *CRAOS8X-18687*	**Summary:** Support for show ipv6 bgp path neighbor commands. **Explanation:** The command extension for "Show ipv6 bgp path <neighbor-adv, neighbor-rcv>" is not available, while it is available in IPv4 BGP path command output. Click for Additional Information
Case: **00474397** *CRAOS8X-20235*	**Summary:** Max-frame-size set to 1518 or 1520 causes packet loss **Explanation:** Max-frame-size(MFS) set to 1518 or 1520 on OS6465 switches causes packet loss on ping packet size more than 1468 bytes. Click for Additional Information
Case: **00468914** **00452881** *CRAOS8X-18390*	**Summary:** OS6860: Unable to discover the switch on OV2500. **Explanation:** Intermittently OS6860 switch fails to be discovered on the OV2500. The AOS SNMP code used "strlen" function on a non-string buffer which causes the bug and made the switch intermittently not discovered by OV. The issue is fixed on AOS 8.7.R01 where the usage of strlen function is removed. Click for Additional Information
Case: **00431901** *CRAOS8X-15567*	**Summary:** How to change the user "admin" password during Automatic Remote Configuration Download process on AOS 8x **Explanation:** The user "admin" password can only be changed when the switch is logged in as an "admin" user. As a workaround, the userTable7 will be pushed to the switch with the help of a TFTP command in the script. Click for Additional Information
Case: **00460852** *CRAOS8X-17975*	**Summary:** Addition of collision information under “show interfaces" output. **Explanation:** With 10M Half-duplex connection, packets drop are not captured under “show interfaces” output. The following three collision parameters Single Collision, Excessive Collision, and Late Collision will be added into to "Show interfaces Chassis/Slot/Port" output from the AOS 8.7R01. Click for Additional Information
Case: **00443853**	**Summary:**

CRAOS8X-17612	Polycom IP phones are connected to the switch and configured as 802.1x client and causing the re-authentication. **Explanation:** Polycom IP phones are re-authenticating in every 30 seconds which is causing either call loss or one-way calls. Found EAP-START is being sent from Polycom to the device causing the re-authentication. Click for Additional Information
Case: **00451075** **00393169** *CRAOS8X-11468*	**Summary:** OV processing old traps when the switch uptime is high. **Explanation:** From the below debug log in OV side, it is visible that uptime of TRAP seqID:1 is 497 days while that if swgID:0 is 0 ticks. Due to this big difference in uptime between neighboring trap IDs, OV has cleared the trap replay database and as a result all the received traps were displayed once again. Click for Additional Information
Case: **00432045** *CRAOS8X-15589*	**Summary:** Buffer overflow is detected when "?" or "tab" is used with PIM commands inside the VRF instance. **Explanation:** Buffer leak is seen only when using too long session prompt name. Correction and resize has been done for session prompt in 8.7R1. Click for Additional Information
Case: **00431157** *CRAOS8X-15621*	**Summary:** TCAM NI error messages are seen when the interface is coming up. **Explanation:** The error comes only for the QOS condition with port ranges (tcp-port 20-21 or 80-81) for built-in network groups. Click for Additional Information
Case: **00420086** *CRAOS8X-14053*	**Summary:** The OS9900 (OS99-XNI-U48) and OS 6465 switches are connected in the linkagg by using two links. if one port is disabled from the linkagg shut down, it would shut down the 2nd port from the linkagg and will come up. **Explanation:** This issue is because of the XNI module in OS9900 with the CLI command "disable". The port was powered off and due to the power off of the PHY interface, it toggled the other port in the linkagg. The code change has been done to rest the interface instead of power off when the command "disable" used to shut down the interface. Click for Additional Information

The following problem reports were closed in the 8.7.354.R01 release.

Case: **00491780** *Internal CR:270453*	**Summary:** Clarification on swlog message " phy_glue_56375_54998es_phy_cmd_set" on OS6860N-P48M. **Explanation:**

	These logs are introduced for initial level of debugging (during development stage), and the purpose of these logs is to check the port enable/disable functionality at the PHY Level. These logs will be moved to Debug “level2”. Click for Additional Information
Case: **00480280** *CRAOS8X-20814*	**Summary:** 2x6900: mac-addresses dynamically learnt on the ERP port cannot be flushed. **Explanation:** The dynamic mac-addesses learnt on the ERP port are not timing out. The command to flush this mac-address or all mac-address is accepted, however, the mac-address is not flushed. Click for Additional Information
Case: **00422893** *CRAOS8X-14374*	**Summary:** Setting the interface flood-rate to default value of 997 causes the removal of the flood-rate status configuration. **Explanation:** If the interface flood-rate status is set to a non-default status and then the interface flood-rate value is set to default value of 997, the configuration for the interface flood-rate status is not displayed in the configuration snapshot. See the following example: Click for Additional Information
Case: **00482441** *CRAOS8X-20966*	**Summary:** Disabling auto-neg and changing the speed or duplex parameter causes the port to go down while the LED remain ON. **Explanation:** On OS6465-P12 switch, when auto-neg is disabled and the speed is set to 100 mbps or Duplex is set to HALF or FULL, the port status changes to DOWN, however, the LED remain ON. Click for Additional Information
Case: **00487069** *CRAOS8X-21451*	**Summary:** WATERMARK_HIGH In Zone Low Memory Dumping. **Explanation:** After the upgrade of OS6860 & OS6860E switches to 8.7.277.R01 GA, the switches started to reload randomly after logging the memory dump and PMD. PMD in the switch was generated due the 'aluSubagent' task been crashed. The aluSubagent memory leak is due to the issue with the net-snmp version 5.8, and this upgrade was done in 8.7.277.R01 GA. Click for Additional Information
Case: **00475640** *CRAOS8X-21374*	**Summary:** Port is not coming UP when using 100M SFP after a reload. **Explanation:** If the 100M SFP is used and the port will be UP and working however once the reload happen the port is not changing the status from DOWN to UP. Click for Additional Information
Case: **00450337** *CRAOS8X-17551*	**Summary:** How SNMP traps for DDM Output Power processed. **Explanation:**

	Every time the Output Power (Rx) crosses the Alarm High to Warning High AOS 8.X sends a trap notification. But when the status falls back to the threshold limit of Alarm High from Warning High, no trap notification will be sent. Click for Additional Information
Case: **00474782** *CRAOS8X-20502*	**Summary:** OS6465: PoE Input Voltage dropped below AT lower Threshold 52V(voltage: 472) log query. **Explanation:** Lanpower INFO logs are generated only on os6465-P12 for every 20 seconds. Swlog: swlogd lpNi LanNi INFO: lpProcessPowerSupplyVoltage 2994:PoE Input Voltage dropped below AT lower Threshold 52V(voltage: 471). Click for Additional Information
Case: **00466533** *CRAOS8X-19481*	**Summary:** OS6860E: Incorrect IP-address is sent as NAS-IP-Address during Radius Authentication. **Explanation:** When two IP interfaces have reachability with the secondary Radius server, the switch uses the IP-address other than the one that as configured as NAS-IP address. Click for Additional Information
Case: **00463122** *CRAOS8X-18594*	**Summary:** BFD feature working; however, the following error gets printed in the swlogs. 2020 Mar 30 03:41:50.222 TEST swlogd bfdni error ERR: : [pmApiGetPortState:2411] PMInit Not Done. **Explanation:** The error is coming when BFD-NI is not registered with port manager library. The issue fix will be available in 8.7.R02 Click for Additional Information
Case: **00472558** *CRAOS8X-20155*	**Summary:** The first attempt of the EAP TLS is getting failed (in progress) stats, from the CPPM perspective, TIMEOUT message in the access tracker. **Explanation:** Switch is sending EAP request identity packet in middle of EAP/TLS exchanges. Some clients are responding to those packets and that leads to mismatch eap response id for actual EAP/TLS request packet and authentication is getting pause for few seconds. Click for Additional Information
Case: **00479898** *CRAOS8X-20776*	**Summary:** When using the command "ssh strong-hmacs enable", the algorithm hmac-sha1 is still shown in the hmac list. ->ssh strong-ciphers enable ->ssh strong-hmacs enable. **Explanation:** The SSH strong-hmacs is not enabled, the switch uses the best hmac of "hmac-sha2-256" as default. HMAC-SHA1 will be removed from the Hmac list from the release AOS 8.7 R01 Click for Additional Information
Case: **00476819**	**Summary:** VRRPv3 packet with invalid checksum from ALE OS6860E.

CRAOS8X-20463	**Explanation:** VRRPv3 packet with invalid checksum are sent from OS6860E switch. The other switch in the VRRP pair ignores the advertisements with the faulty checksum. Impact is that both switches are acting as master. So the VRRP pair is not working as expected due to this issue. A fix to this issue is provided from AOS 8.7R01 MR-2. Click for Additional Information
Case: **00473604** *CRAOS8X-20141*	**Summary:** Vulnerability: Weak permission for Password, Shadow and Group Files (generic-passwd-shadow-group-file-permissions) in AOS Switches. **Explanation:** The vulnerability identified related to the Weak permission for Password, Shadow and Group Files and password hashes in /etc/passwd were fixed. Click for Additional Information
Case: **00470514** *CRAOS8X-19670*	**Summary:** OID "1.3.6.1.2.1.17.4.3.1." is not returning MAC address of all the ports on the switch. **Explanation:** OID "1.3.6.1.2.1.17.4.3.1." is not returning MAC address of all the ports on the switch. OID is only returning the MAC learned on one port. Issue is fixed on 8.7 R01. Click for Additional Information
Case: **00490698** **00488706** *CRAOS8X-21894*	**Summary:** IP Relay does not work after AOS upgrade from 8.5.R02 to 8.7.R01. **Explanation:** When a switch with deprecated IP Relay commands is upgraded to 8.7.R01, the deprecated IP Relay commands are automatically changed to new commands, however, the IP Relay functionality does not work. The issue is not seen when the configuration is saved and the switch reloaded for the second time. Also, dhcp statistics output showing zero values too has been fixed. Click for Additional Information

Appendix I: Installing/Removing Packages

The package manager provides a generic infrastructure to install AOS or non-AOS third party Debian packages and patches. The following packages are supported in 8.7R1. The package files are kept in the **flash/working/pkg** directory or can be downloaded from the Service & Support website.

Package	Package Description
WebView (package-webview-8.7.R01-354.deb)	WebView 2.0 Application
ams / ams-apps (ams-8.7.R01-354.deb/ams-apps-8.7R01-354.deb)	AOS Micro Services Application
OVSDB (aos-ovsdb-8.7.R01-354.deb)	OVSDB Application
Patch	OpenSSL Security Patch
NTPD	NTP upgrade
- A reboot is required after installing the OpenSSL security patch upgrade. - If a package is not commited it can result in image validation errors when trying to reload the switch. - If either the WebView or AMS packages were installed in a previous release they will have to be re-installed after upgrading to 8.7R01.	

Installing Packages

Verify the package prior to install. Then install and commit the package to complete the installation. For example:

```
-> pkgmgr verify package-webview-8.7.R01-####.deb
  Verifying MD5 checksum.. OK
-> pkgmgr install package-webview-8.7.R01-####.deb
-> pkgmgr commit
-> pkgmgr list

Legend: (+) indicates package is not saved across reboot
        (*) indicates packages will be installed or removed after reload
Name                Version           Status              Install Script
--------------+--------------------+------------------+---------------------------------
  ams           default               installed          default
  ams-apps      default               installed          default
  webview       8.7.R01-###           installed          /flash/working/pkg/webview/install.sh
```

Removing Packages

Find the name of the package to be removed using the **pkgmgr list** command, then remove and commit the package to complete the removal. Remove the Debian installation file. For example:

```
-> pkgmgr remove webview
Purging webview (8.7.R01-####)...
Removing package webview.. OK
Commit is required complete package webview removal

-> pkgmgr commit
Package(s) Committed

-> pkgmgr list
Legend: (+) indicates package is not saved across reboot
        (*) indicates packages will be installed or removed after reload
Name                Version           Status              Install Script
--------------+--------------------+------------------+---------------------------------
  ams           default               installed          default
  ams-apps      default               installed          default
  webview       7.X.X.R01-6868        removed            /flash/working/pkg/webview/install.sh
```

Remove the Debian package installation file. For example:

```
 -> rm /flash/working/pkg/package-webview-8.7.R01-####.deb
```

AOS Upgrade with Encrypted Passwords

AMS

The ams-broker.cfg configuration file for AMS contains plain text passwords. The passwords can be stored as encrypted beginning with the 8.7R1 release. Follow the steps below prior to upgrading to 8.7R1 to store encrypted passwords.

1. Remove *ams-broker.cfg* file present under path /flash/<running-directory>/pkg/ams/ prior to upgrading AOS.
2. This will remove the broker configuration which must be re-configured after the upgrade.
3. Remove this file from each VC node.
4. Upgrade the switch to the 8.7R1 release.
5. Once the switch comes up after the upgrade, the password present under/flash/<running-directory>/pkg/ams/ams-broker.cfg file will be encrypted.

IoT-Profiler

The ovbroker.cfg configuration file for AMS-APPS/IoT-Profiler contains plain text passwords. The passwords can be stored as encrypted beginning with the 8.7R1 release. Follow the steps below prior to upgrading to 8.7R1 to store encrypted passwords.

1. Remove the *install.sh* file present under path /flash/<running-directory>/pkg/ams-apps/ for AMS-APPS prior to upgrading AOS.
2. Remove this file from each VC node.
3. Upgrade the switch to the 8.7R1 release.
4. Once the switch comes up after the upgrade, the password present under/flash/<running-directory>/pkg/ams-apps/ovbroker.cfg file will be encrypted.