Release Notes - Rev. A

OmniSwitch 6360, 6465, 6560, 6860(E), 6860N, 6865, 6900, 6900-V72/C32, 6900-X48C6/T48C6/X48C4E, 9900

Release 8.7R2

These release notes accompany release 8.7R2. 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 OS6900-V48C8 is currently not supported in AOS Release 8.7R2. It is referenced in the 8.7R2 user guides and the release notes. Support will be added in a future release.

Alcatel-Lucent Enterprise

Contents

Contents 2

Related Documentation 3

System Requirements 4

[IMPORTANT] *MUST READ*: AOS Release 8.7R2 Prerequisites and Deployment Information 9

Licensed Features 12

ALE Secure Diversified Code 12

New / Updated Hardware Support 13

New Software Features and Enhancements 16

Open Problem Reports and Feature Exceptions 28

Hot-Swap/Redundancy Feature Guidelines 31

Technical Support 34

Appendix A: Feature Matrix 35

Appendix B: SPB L3 VPN-Lite Service-based (Inline Routing) / External Loopback Support / BVLAN Guidelines 41

Appendix C: General Upgrade Requirements and Best Practices 44

Appendix D: Standard Upgrade - OmniSwitch Standalone or Virtual Chassis 49

Appendix E: ISSU – OmniSwitch Chassis or Virtual Chassis 51

Appendix F: FPGA / U-boot Upgrade Procedure 54

Appendix G: OS6900-V72/C32 Flash Cleanup Procedure / FEC Disable 56

Appendix H: Fixed Problem Reports 57

Appendix I: Installing/Removing Packages 72

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 6360 Hardware User Guide
- 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
OS6360	1GB	1GB
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/X48C4E	8GB	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 6360 – AOS Release 8.7.252.R02 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6360-10	8.7.149.R02	8.7. 149.R02	0.11	0.11
OS6360-P10	8.7.149.R02	8.7. 149.R02	0.11	0.11
OS6360-24	8.7.149.R02	8.7. 149.R02	0.15	0.15
OS6360-P24	8.7.149.R02	8.7. 149.R02	0.15	0.15
OS6360-P24X	8.7.149.R02	8.7. 149.R02	0.12	0.12

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6360-PH24	8.7.149.R02	8.7. 149.R02	0.12	0.12
OS6360-48	8.7.149.R02	8.7. 149.R02	0.15	0.15
OS6360-P48	8.7.149.R02	8.7. 149.R02	0.15	0.15
OS6360-P48X	8.7.149.R02	8.7. 149.R02	0.12	0.12

OmniSwitch 6465 – AOS Release 8.7.252.R02 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6465-P6	8.5.83.R01	8.7.2.R02[2]	0.10	0.10
OS6465-P12	8.5.83.R01	8.7.2.R02[2]	0.10	0.10
OS6465-P28	8.5.89.R02	8.7.2.R02[2]	0.5	0.7[1]
OS6465T-12	8.6.117.R01	8.7.2.R02[2]	0.4	0.4
OS6465T-P12	8.6.117.R01	8.7.2.R02[2]	0.4	0.4

1. FPGA version 0.7 is optional to address issue CRAOS8X-12042.
2. U-boot 8.7.2.R02 is optional to address UBIFS error issues CRAOS8X-4813/13440.

OmniSwitch 6560 – AOS Release 8.7.252.R02 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6560-24Z24	8.5.22.R01	8.7.2.R02[3]	0.7	0.8[5]
OS6560-P24Z24	8.4.1.23.R02	8.7.2.R02[3]	0.6	0.7[1] 0.8[5]
OS6560-24Z8	8.5.22.R01	8.7.2.R02[3]	0.7	0.8[5]
OS6560-P24Z8	8.4.1.23.R02	8.7.2.R02[3]	0.6	0.7[1] 0.8[5]
OS6560-24X4	8.5.89.R02	8.7.2.R02[4]	0.4	0.4
OS6560-P24X4	8.5.89.R02	8.7.2.R02[4]	0.4	0.4
OS6560-P48Z16 (903954-90)	8.4.1.23.R02	8.7.2.R02[3]	0.6	0.7[1] 0.8[5]
OS6560-P48Z16 (904044-90)	8.5.97.R04	8.7.2.R02[3]	0.3	0.6[2] 0.7[6]
OS6560-48X4	8.5.97.R04	8.7.2.R02[4]	0.4	0.7[2] 0.8[6]
OS6560-P48X4	8.5.97.R04	8.7.2.R02[4]	0.4	0.7[2] 0.8[6]
OS6560-X10	8.5.97.R04	8.7.2.R02[4]	0.5	0.8[2]

1. FPGA version 0.7 is optional to address issue CRAOS8X-7207.
2. FPGA versions are optional to address issue CRAOS8X-16452.

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
3. U-boot 8.7.2.R02 is optional to address eUSB issue CRAOS8X-13819. 4. U-boot 8.7.2.R02 is optional to address UBIFS error issues CRAOS8X-4813/13440. 5. FPGA version 0.8 is optional to address issue CRAOS8X-22857. 6. FPGA versions 0.7 and 0.8 are optional to support 1588v2.				

OmniSwitch 6860(E) – AOS Release 8.7.252.R02 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6860/OS6860E (except U28/P24Z8)	8.1.1.70.R01	8.1.1.70.R01	0.9	0.10[1]
OS6860E-U28	8.1.1.70.R01	8.7.74.R01	0.2	0.2
OS6860E-P24Z8	8.4.1.17.R01	8.4.1.17.R01	0.5	0.7[1]
1. FPGA versions 7 and 10 are optional on the PoE models for the fast and perpetual PoE feature support.				

OmniSwitch 6860N – AOS Release 8.7.252.R02 (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 8.7.252.R02 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6865-P16X	8.3.1.125.R01	8.7.2.R02[2]	0.20	0.25[1]
OS6865-U12X	8.4.1.17.R01	8.7.2.R02[2]	0.23	0.25[1]
OS6865-U28X	8.4.1.17.R01	8.7.2.R02[2]	0.11	0.14[1]
1. FPGA versions 0.25 and 0.14 are optional for the fast and perpetual PoE feature support. 2. U-boot 8.7.2.R02 is optional to address eUSB issue CRAOS8X-13819. **Note**: CRAOS8X-4150 for the OS6865-U28X was fixed with FPGA version 0.12 and higher.				

OmniSwitch 6900-X20/X40 – AOS Release 8.7.252.R02 (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

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
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 8.7.252.R02 (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 8.7.252.R02 (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 8.7.252.R02 (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[1]
1. FPGA version 0.1.11 and U-boot version 8.6.189.R02 are optional to address CRAOS8X-11118.				

OmniSwitch 6900-V72/C32 – AOS Release 8.7.252.R02 (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	2018.11.00.02	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/X48C4E- AOS Release 8.7.252.R02 (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

Hardware	Minimum ONIE	Current ONIE	Minimum CPLD	Current CPLD
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
OS6900-X48C4E	2019.05.00.10	2019.05.00.10	CPLD 1 – 0x3 CPLD 2 - 0x2 CPLD 3 – 0x3	CPLD 1 – 0x3 CPLD 2 - 0x2 CPLD 3 – 0x3
Note: These models use the **Yos.img** image file.				

OmniSwitch 9900 – AOS Release 8.7.252.R02 (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	8.6.261.R01	1.0	2.9.0	0.8
OS99-XNI-P24Z8	8.5.76.R04	8.6.261.R01	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 8.7R2 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.
AOS Release 8.7R2
There are new default user password polices being implemented in 8.7R2. This change does not affect existing users. - cannot-contain-username: enable - min-uppercase: 1 - min-lowercase: 1 - min-digit: 1 - min-nonalpha: 1
The OmniSwitch 6360 does not contain a real-time clock. - It is recommended to use NTP to ensure time synchronization on OS6360s. - When the switch is reset, the switch will boot up from an approximation of the last known good time. - When the switch is powered off it cannot detect the time left in the powered off state. When it boots up it will have the same time as when the switch was last powered off.
The default FEC setting for 25G fiber ports was changed from FC-FEC to RS-FEC. In a mixed release environment the FEC setting for switches running previous AOS versions should be changed to avoid connectivity issues.

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						
	OS6360	OS6465	OS6560	OS6860	OS6860N	OS6900	OS9900
Licensed Features							
MACsec (OS-SW-MACSEC)	N/A	Yes	Yes	Yes	Yes	Yes[3]	Yes
10G support (OS6560-SW-PERF)	N/A	N/A	Yes[1]	N/A	N/A	N/A	N/A
10G support (OS6360-SW-PERF)	Yes[2]	N/A	N/A	N/A	N/A	N/A	N/A
1. Performance software license is optional allowing ports 25/26 (OS6560-24X4/P24X4) and ports 49/50 (OS6560-48X4/P48X4) to operate at 10G speed. Ports support 1G by default. 2. Performance software license is optional allowing the 2 RJ45/SFP+ combo ports (25/26) of the OS6360-PH24 model to operate at 10G speed. Ports support 1G by default. 3. MACsec is supported on the OS6900-X48C4E.							

ALE Secure Diversified Code

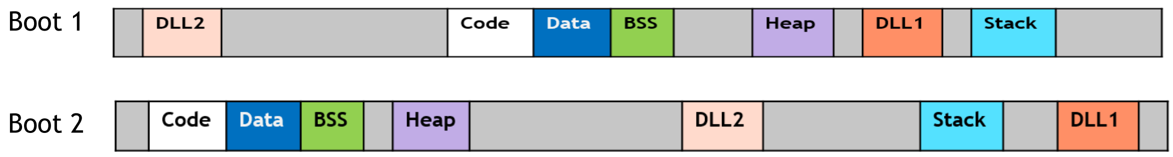
Alcatel-Lucent Enterprise provides network equipment that is hardened in conjunction with an independent 3rd party organization. ALE secure diversified code promotes security and assurance at the network device level using independent verification and validation of source code and software diversification 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 and Guidelines

The following new hardware is being introduced in this release.

Note: The OS6360 models support a VC of up to 4 units.

OS6360-10
Fixed-configuration chassis in a 1U form factor with:

- 10 x 10/100/1000Base-T non-PoE ports
- 2 x SFP ports
- Internal 30W AC power supply
- Fanless

OS6360-P10
Fixed-configuration chassis in a 1U form factor with:

- 8 x 10/100/1000Base-T PoE (802.3at) ports
- 2 x 10/100/1000Base-T non-PoE ports
- 2 x SFP ports
- Internal 165W AC power supply
- Fanless

OS6360-24
Fixed-configuration chassis in a 1U form factor with:

- 24 x 10/100/1000Base-T non-PoE ports
- 2 x RJ45/SFP combo ports
- 2 x SFP+ software configurable ports:
  - 2 x SFP uplinks
  - 2 x SFP+ uplink or VFL ports
- Internal 65W AC power supply
- Fanless

OS6360-P24
Fixed-configuration chassis in a 1U form factor with:

- 24 x 10/100/1000Base-T PoE (802.3at) ports
- 2 x RJ45/SFP combo ports
- 2 x SFP+ software configurable ports:
  - 2 x SFP uplinks
  - 2 x SFP+ uplink or VFL ports
- Internal 260W AC power supply
- Fanless

OS6360-P24X
Fixed-configuration chassis in a 1U form factor with:

- 24 x 10/100/1000Base-T PoE (802.3at) ports
- 2 x RJ45/SFP+ combo ports
- 2 x SFP+ software configurable ports:
  - 2 x SFP uplinks
  - 2 x SFP+ uplink or VFL ports
- Internal 550W AC power supply

OS6360-PH24
Fixed-configuration chassis in a 1U form factor with:

- 24 x 24 x 10/100/1000Base-T PoE (802.3at) ports
- 2 x RJ45/SFP+ combo ports (Upgradeable to 10G)
- 2 x SFP+ software configurable ports:
  - 2 x SFP uplinks
  - 2 x SFP+ uplink or VFL ports
- Internal 550W AC power supply

OS6360-48
Fixed-configuration chassis in a 1U form factor with:

- 48 x 10/100/1000Base-T non-PoE ports
- 2 x RJ45/SFP combo ports
- 2 x SFP+ software configurable ports:
    - 2 x SFP uplinks
    - 2 x SFP+ uplink or VFL ports
- Internal 120W AC power supply

OS6360-P48
Fixed-configuration chassis in a 1U form factor with:

- 48 x 10/100/1000Base-T PoE (802.3at) ports
- 2 x RJ45/SFP combo ports
- 2 x SFP+ software configurable ports:
    - 2 x SFP uplinks
    - 2 x SFP+ uplink or VFL ports
- Internal 550W AC power supply

OS6360-P48X
Fixed-configuration chassis in a 1U form factor with:

- 46 x 10/100/1000Base-T PoE (802.3at) ports
- 2 x 10/100/1000/2.5G PoE (802.3bt) ports
- 2 x RJ45/SFP+ combo ports
- 2 x SFP+ software configurable ports:
    - 2 x SFP uplinks
    - 2 x SFP+ uplink or VFL ports
- Internal 950W AC power supply

OS6900-V48C8 (Future Availability)
Fixed configuration chassis in a 1U form factor with:

- 48 x SFP28 ports
- 8 x QSFP28 ports
- 2 x SFP+ ports (Currently not functional)
- USB port
- RJ-45 console port
- EMP port
- Front-to-rear or rear-to-front cooling
- AC or DC power supply
- **Note**: The OS6900-V48C8 doesn't support a mix of 1G/10G and 25G speeds on the 4-port groups of ports 1-48 listed below. Mixing 1G and 10G speeds is supported.

the same color-coded ports must operate at the same speed				the same color-coded ports must operate at the same speed				the same color-coded ports must operate at the same speed				the same color-coded ports must operate at the same speed			
1	4	7	10	13	16	19	22	25	28	31	34	37	40	43	46
2	5	8	11	14	17	20	23	26	29	32	35	38	41	44	47
3	6	9	12	15	18	21	24	27	30	33	36	39	42	45	48

Front Panel Ports 1-48 Representation

OS6900-X48C4E
Fixed configuration MACsec chassis in a 1U form factor with:

- 40 x SFP+ ports
- 8 x SFP28 ports
- 4 x 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 OS6900-X48C4E model does not support a VC configuration.
Note: The OS6900-X48C4E doesn't support a mix of 1G/10G and 25G speeds on the 4-port groups of ports 41-48. Ports within a port group must all run at either 1G/10G speed or 25G speed. Mixing 1G and 10G speeds is supported.

  - Port Group 1 (41,42,43,44)
  - Port Group 2 (45,46,47,48)

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

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.

Transceivers and Guidelines
The following transceiver support and guidelines have been added in the release. Please refer to the Transceivers and Hardware Guides for additional information.

- 1G transceiver support has been added on the SFP28 (25G) ports of the following models:
  - OS6900-X48C4E, OS6860N and uplink module (OS68-VNI-U4).

  Note: The SFP-1G-T, SFP-GIG-T and the SFP Dual speed (SFP-DUAL-*) transceivers are not supported on the SFP28 ports.

Additional Transceiver Guidelines:

- The SFP-GIG-T and SFP-1G-T transceivers are not supported on the OS6900-X48C6. Use the SFP-10G-T for 1G copper support.
- The OS6900-X48C6 is limited to 38 SFP-10G-T transceivers per chassis.
- SFP Dual speed transceivers (SFP-DUAL-*) are not supported on the OS6900-X48C6/T48C6/X48C4E.
- SFP dual speed transceivers (SFP-DUAL-*) are not supported on the SFP28 (25G) ports on 6860N.
- Splitter functionality (4X10/4X25) is currently not supported on the OS6900-X48C6/T48C6/X48C4E.
- Splitter functionality (4X10/4X25) is currently not supported on the OS686N.

Additional Hardware Guidelines:

- The OS6860N-U28 doesn't support a mix of 1G/10G and 25G speeds on the 4-port group of ports 31-34. Ports within the port group must all run at either 1G/10G speed or 25G speed. Mixing 1G and 10G speeds is supported.
- The OS6860N-P48Z doesn't support a mix of 1G/10G and 25G speeds on the 4-port group of ports 51-54. Ports within the port group must all run at either 1G/10G speed or 25G speed. Mixing 1G and 10G speeds is supported.
- The OS68-VNI-U4 doesn't support a mix of 1G/10G and 25G speeds. Ports must all run at either 1G/10G speed or 25G speed. Mixing 1G and 10G speeds is supported.
- The OS6900-V72 doesn't support a mix of 10G and 25G speeds on the 4-port groups of ports 1-48. Ports within a port group must all run at either 10G speed or 25G speed.

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.

8.7R2 New Feature/Enhancements Summary

Feature	Platform
Management / NMS Related Features	
OVSDB Enhancement	6900- X72, Q32, V72/C32
Banner and User Account Enhancement	6360, 6465, 6560, 6860, 6860N, 6865, 6900 (all), 9900
Large Table Data Performance Improvement	6360, 6465, 6560, 6860, 6860N, 6865, 6900 (all), 9900
Webview 2.0 as Default	6360, 6465, 6560, 6860, 6860N, 6865, 6900 (all), 9900
Service / Access port / UNP Related Features	
Service Inline Routing - Native, single pass, without loopback	6860N, 6900- X48C6/T48C6
Transparent Circuit SPB Service PTOP No MAC Learning	6860, 6860N, 6865, 6900, 9900
Enhancement to SPB Inband Management IP Reachability	6860, 6860N, 6865, 6900, 9900
Layer 3 / Multicast Related Features	
Allow iBGP to OSPF Redistribution	6860, 6860N, 6865, 6900 (all), 9900
PIM Multicast Enhancements for Packed Register Messages	6860, 6860N, 6865, 6900 (all), 9900
Additional Features	
MRP - Media Redundancy Protocol	6465, 6865
LLDP Extension for 802.3bt	6465, 6865
Hot-swap for 6860N Modules	6860N
Explicit Congestion Notification (ECN) Support (RoCEv2)	6900-V72/C32
Multi-destination Ports for Remote Mirroring	6465
JITC Enhancements	6360, 6465, 6560, 6860, 6860N, 6865, 6900 (all), 9900
Parity Features	
1588v2	6560
Private VLAN	6860N, 6900-X48C6/T48C6/X48C4E
Application Monitoring (Appmon/DPI)	6860N
Link Fault Propogation	6860N
VLAN Stacking	6860N
Link OAM	6860N
L2CP Statistics	6860N
SAA, SAA-SPB	6560, 6860N
L2 GRE	6860N, 6900-X48C6/T48C6/X48C4E
Auto Fabric	6860N
Time Domain Reflectometry (TDR)	6865
Quarantine Manager Support on Vlan Domain	6465, 6560, 6860N, 6900 (all), 9900
RFP Over SPB	6860, 6865

Feature	Platform
EA Features	
OS9900 remote NI syslog (UDP and TLS)	9900
Hybrid NNI mode with VLAN Stacking and 802.1Q VLANs on the same NNI port	6465
ERP - SPB Interworking for Convergence	6860, 6860N, 6865, 6900 (all), 9900
Microservice Marketplace	6360, 6465, 6560, 6860, 6860N, 6865, 6900 (all), 9900
Introduction to Statistical Jitter in SAA	6360, 6465, 6560, 6860, 6860N, 6865, 6900 (all)
DHCP Options 2 and 12	6360, 6465, 6560, 6860, 6860N, 6865, 6900 (all), 9900
OAM PDU Support for EVC MEF OAM on per-CVLAN\SVLAN basis	6465, 6865
UNP Parity Features	6860, 6860N, 6865, 6900 (all), 9900
Increase Authentication Server Down Re-Auth Time	6465, 6560, 6860, 6860N, 6900 (all), 9900
DHCPv6 Guard Configuration Using VLAN Range Option	6560, 6860, 6860N, 6865, 6900 (all), 9900
USB Ethernet Dongle for OOB Management	6360, 6465, 6560, 6860, 6865
Support for Additional Tag-values Under UNP-profile Mapped to Services (SPB/VXLAN/L2GRE)	6860, 6860N, 6865, 6900 (all), 9900
Allow Uboot Shell Access after Authenticating with Password	6465
Webview Localization (French)	6360, 6465, 6560, 6860, 6860N, 6865, 6900 (all), 9900

Management / NMS Related Features

OVSDB Enhancmcnt

In this release, OVSDB is supported on VC of 2 or more configuration on OS6900-X72/Q32/V72/C32. Nuage ACL to AOS ACL is supported for ingress traffic. For egress traffic, the following classification is supported:

- Source IP IPv4
- Source IP IPv6

Ingress policies are applied through the UNP policy list, egress policies are applied directly through the QoS ACL framework

The following CLI commands are associated with this feature:

Old Command	New Command (8.7.R02)
pkgmgr commit	write memory
pkgmgr list	show pkgmgr
appmgr list	show appmgr
appmgr start aos-ovsdb ovsdb-server	appmgr start aos-ovsdb ovsdb-app
appmgr start aos-ovsdb ovsdb-client	
appmgr stop aos-ovsdb ovsdb-client	appmgr stop aos-ovsdb ovsdb-app

Banner and User Account Enhancement

The user custom configuration file can be backed up and restored. The configuration file is backed up in the /flash directory of the OmniSwitch.

The following CLI commands are associated with this feature:

- configuration {backup | restore}

Large Table Data Performance Improvement

In order to improve on the performance of large SNMP table queries OmniVista can now use CLI commands within the REST API framework and process the JSON output. The REST Client must login into the OmniSwitch web server with a user that has read privileges on the switch and the OmniSwitch must have HTTPS access enabled.

The following CLI commands are associated with this feature:

- ip service https enable

Webview 2.0 as Default

Webview 2.0 is now the default web interface beginning in 8.7R2.

The following CLI commands are associated with this feature:

- No new CLI

Service / Access port / UNP Related Features

Service Inline Routing - Native, single pass, without loopback

Service-based in-line routing (single pass) support extended to the OmniSwitch 6860N and OmniSwitch 6900-X48C6/T48C6 models. Similar to the OmniSwitch 9900, service-based in-line routing is configured on these models by assigning an SPB service to an IP interface.

By default, the OmniSwitch 6800N and OmniSwitch 6900-X48C6/T48C6 operate in what is referred to as a "Basic" mode in which service-based in-line routing is supported. While in the Basic mode, the availability of switch resources is reduced in order to provide the in-line routing support. When the Basic mode is disabled, the availability of switch resources is increased but in-line routing is no longer supported.

The following CLI commands are associated with this feature:

- service l3vpn (enables or disables service-based in-line routing support).
- show service l3vpn

Transparent Circuit SPB Service PTOP No MAC Learning

The OmniSwitch implementation of Shortest Path Bridging provides customers at various sites with a multipoint-to-multipoint (E-LAN) connectivity solution. When an SPB backbone service instance (I-SID) is created on a BEB, SDP tunnels are automatically created with other BEBs on which the same I-SID is configured. This results in a full mesh of connectivity between the BEBs that provides any-to-any connectivity for the service traffic on the I-SID. However, as the number of users increases, so does the number of MAC addresses that are dynamically learned to minimize the amount of traffic flooding in the network.

To help reduce the use of system resources and prevent MAC address explosion, an SPB service can be configured as a pseudo-wire type of service; a single point-to-point (E-LINE) connection between two SAP attachment points. The attachment points to customer edge (CE) devices can be between two local SAPs associated with the same service or between two SAPs across the SPB network.

An SPB pseudo-wire service reduces the number of customer MAC addresses learned and simplifies the flow of user traffic, as follows:

- Packets are transparently forwarded (MAC addresses are not learned) between two local SAPs.
- Packets from one SAP are encapsulated and transparently forwarded out of the SPB service network port.
- The encapsulation is removed from packets received from the SPB network port and are transparently forwarded out of the SAP.
- MAC address learning is automatically disabled, since there is no forwarding decision to be made. Packets entering one SAP attachment point will simply egress the other SAP attachment point of the pseudo-wire unchanged.
- Flooding and replication is not necessary since only two virtual ports are involved (SAP to SAP for a local service or SAP to a network port for the same service across the SPB backbone)

A new Layer 2 profile ("pw-def-access-profile") has been added for service access ports. When a service access port is configured with the "def-access-profile" (the default) and then assigned to an SPB pseudo-wire SAP, the Layer 2 profile for that port automatically changes to "pw-def-access-profile". The actions for this profile are set to tunnel for all Layer 2 control protocols, except for 802.1ad (LACP) which is set to peer. This reduces configuration steps in that a new Layer 2 profile for pseudo-wire SAP ports doesn't have to be manually created and assigned to a pseudo-wire SAP.

The following CLI commands are associated with this feature:

- New service pseudo-wire command.
- "Option" field of the show service command updated to display "Pseudo-wire" as a type of service.
- "PW-Enb" field added to **show service ports** command to indicate if the Pseudo-wire functionality is enabled for the SPB service.

- The “pw-def-access-profile” Layer 2 profile can be assigned to a service access port with the service access l2profile command.

- The “pw-def-access-profile” is included in the show service l2profile command display as one of the available default Layer 2 profiles.

Enhancement to SPB Inband Managemennt IP Reachability

Previously, SPB in-band management required configuring static routes on each of the SPB nodes. The static route would point an IP control BVLAN interface to a default L3 gateway outside of the SPB network to reach remote management stations. This process can be cumbersome and involves accessing each SPB node to configure the necessary static routes.

To help simplify this process, management network routes can now be redistributed into ISIS-SPB at one or more SPB Backbone Edge Bridges (BEBs) that connect to a management station. ISIS-SPB then advertises the management network routes, along with the locally configured IP Looback0 address and IP BVLAN address, to all SPB nodes in the network.

When an SPB node receives the advertised management network information, the network route and Loopback0 address are injected into the management VRF as SPB management (SPB-MGMT) routes with the IP BVLAN address as the gateway. In turn, the SPB node advertises its own Loopback0 address to the gateway IP BVLAN address. Now, both the gateway BEB and the SPB node know how to reach each other.

The following CLI commands are associated with this feature enhancement:

- New **spb-mgmt** parameter has been added to the following commands:

  - ip route-pref
  - ip redist
  - show ip router database

- **spb-mgmt** has been included in the following show command output displays:

  - show ip routes
  - show ip route pref
  - show ip redist (when configured)

Layer 3 / Multicast Related Features

Allow iBGP to OSPF Redistribution

This feature supports redistribution of iBGP routes into OSPF protocol. Care should be taken when redistributing iBGP routes (from the same AS) into OSPF to avoid routing loops.

The following CLI commands are associated with this feature:

- vrf <vrfName>] [no] ip ospf redist-bgp-internal
- show ip ospf

PIM Multicast Enhancements for Packed Register Messages

In PIM-SM networks, PIM Null Register messages are sent periodically from the first hop router to the RP to signal the presence of Multicast sources in the network and to keep the (S,G) state alive as long as the source is active. Likewise, Register Stop messages are sent from the RP to stop the sending of the register encapsulated messages. These messages currently include information about a single multicast source and group. In large networks with a lot of sources, this can amount to a lot of PIM Control packets which ultimately may be dropped due to control plane processing overhead or CPU queue rate-limiting. The packing of these Null Registers and Register stops has been added to reduce the possibility of losing these packets.

The following CLI commands are associated with this feature:

- ip[v6] pim register-packing {enable | disable | force-enable}
- ip[v6] pim register-mtu <num>
- ip[v6] pim register-delay <num>

Additional Features

MRP - Media Redundancy Protocol

Media Redundancy Protocol (MRP) is an IEC standard that specifies a recovery protocol for use in high availability ring topology networks used in industrial automation networks. It is described in the IEC 62439-2. This protocol is designed to react to a single link or switch failure in the network and provide deterministic recovery time, which is important in ensuring real time data communication needs of industrial networks. During the failure of a connection, the media redundancy reconfigures the network so that the nodes can be accessed again through a substitute path.

MRP is packaged into a Debian package that can be installed or uninstalled from AOS switches. It will not be a part of standard AOS image. No license is required. Currently, MRP is supported by standalone switches or VC of 1.

Note: MRP interconnect is not supported in this release.

The following CLI commands are associated with this feature:

- mrp
- mrp domain
- show mrp
- show mrp domain
- show mrp port
- clear mrp
- clear mrp port

LLDP Extension for 802.3bt

AOS supports Power via MDI extension (29 Bytes) TLV to support type 3 and type 4 PD for IEEE802.3bt and the Power via MDI measurements (28 byte) TLV to support IEEE802.3bt.
The following CLI commands are associated with this feature:

- lanpower firmware-upgrade <filename> (OS6865)
- lanpower 802.3bt

The OS6865 requires a PoE firmware upgrade to version 3.52 for 802.3bt support. The file can be downloaded from the service & support website. Note the following:

- The binary file must be placed in the /flash directory of the Master.
- The lanpower service must be stopped on all chassis that are being upgraded.
- Once started, console messages will be displayed during the update procedure which may take up to 10 minutes.
- The chassis being upgraded should have minimal traffic flow during the upgrade.
- The chassis being upgraded should not be unplugged or distrubed during the upgrade.
- Command examples:

```
-> lanpower slot 1/1 firmware-upgrade 24035200_1000_030.s19

-> lanpower slot all firmware-upgrade 24035200_1000_030.s19
```

Hot-swap for OS6860N Modules

The OS6860N modules now support hot-swapping. See Hot-Swap/Redundancy Guidelines.

The following CLI commands are associated with this feature:

- No new CLI

Explicit Congestion Notification (ECN) Support

Enhanced Congestion Notification (ECN) is new improved mechanism for Responsive flows such as TCP/UDP, to proactively detect congestion in Network Devices and throttle sender rate of transmission to allow the congestion point to clear up, instead of ignoring the condition resulting into packet drops due to complete resource exhaustion as seen in regular TCP.

RoCEv2 uses IP Header ECN marking mechanism for congestion notification over UDP datagram for InfiniBand Header and data encapsulation. UDP Destination Port 4791 is reserved for RoCEv2.

This enhancement adds RoCEv2 support by implementing Explicit Congestion Notification (ECN) on the OS6900-V72/C32.The following CLI commands are associated with this feature:

- qos ecnp max-threshold
- qos ecnp min-threshold
- qos ecnp import
- qos qsp ecn-profile
- qos qsi port admin-state enable
- show qos ecnp [detail]

Multi-destination Ports for Remote Mirroring

RPMIR Loopback session allows to send the mirrored traffic from the source port to multiple destination associated to the source port. When the Loopback mode is enabled, the mirrored traffic sent to the Loopback port of RPMIR will be looped and sent to the same port as ingress packets. The ingress packets are Q-tagged with the RPMIR VLANID. The destination ports which is associated with RPMIR VLANID egresses out the mirrored RPMIR traffic, so that ingress mirrored packets are allowed.

The following CLI commands are associated with this feature:

- **port-mirroring source destination**, included the **loopback** option to configure RPMIR loopback session.

JITC Enhancements

IP OPTIONS FILTER

As per the STIG requirement perimeter router must be configured to block all packets with an IP option to prevent security attacks. Hence, the OmniSwitch is now configurable to drop packets with IP options.The following CLI commands are associated with this feature:

- ip dos type ip-options-filter admin-state {enable | disable}

- show ip dos config

Parity Features

1588v2 Precision Time Protocol End-to-End and Peer-to-Peer Transparent Clock is now supported on some OS6560 models.

- Supported on OS6560-48X4/P48X4/P48Z16 models only.

- Support on 1G and 10G ports only. Not supported on 2.5G ports.

- Not supported across Virtual Chassis.

- OS6560-48X4/P48X4 require FPGA 0.8.
- OS6560-P48Z16 (904044-90) requires FPGA 0.7.

Private VLAN is now supported on the OS6860N, OS6900-X48C6/T48C6, OS6900-X48C4E.

Application Monitoring (Appmon/DPI) is now supported on the OS6860N.

Link Fault Propogation is now supported on the the OS6860N

VLAN Stacking is now supported on the OS6860N.

Link OAM is now supported on the OS6860N.

L2CP Statistics is now supported on the OS6860N.

SAA, SAA-SPB is now supported on the OS6560 and OS6860N.

L2 GRE is now supported on the OS6860N and OS6900-X48C6/T48C6/X48C4E.

Auto Fabric is now supported on the OS6860N and OS6900-X48C6/T48C6/X48C4E.

Time Domain Reflectometry (TDR) is now supported on the OS6865.

Quarantine Manager Support on Vlan Domain is now supported on the OS6465, OS6560, OS6860N, OS6900 (all), and OS9900.

RFP Over SPB is now supported on the OS6860 and OS6865.

Early Availability Features

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.

OS9900 remote NI syslog (UDP and TLS)

In OmniSwitch 9900, only the CMM swlog is transferred to the external syslog server over TLS.

For full debug capability and usefulness of the syslog, the OS9900 is enhanced to transfer NI syslog(s) and HOST logs to the external server with UDP to remote syslog servers. This feature is already supported on other platforms.

The following CLI commands are associated with this feature:

- swlog host output socket { enable | disable}

- swlog ni slot <chassis/slot> output socket {enable|disable}

Hybrid NNI mode with VLAN Stacking and 802.1Q VLANs on the same NNI port

Any standard (non-service) VLAN can now be assigned to NNI ports as the default VLAN (untagged) or as an 802.1Q tagged VLAN .

This allows customers to configure 802.1q services, QinQ service, and untagged services using the same uplink NNI port.

There is no new CLI to support this feature, but the existing **vlan members untagged** and **vlan members tagged** commands can now be used to configure an untagged or tagged association with a VLAN Stacking NNI port.The following CLI commands are associated with this feature:

ERP - SPB Interworking for Convergence

Allows seamless connectivity between an access ERP ring and an SPBM aggregation network. The feature will allow ERP protected VLANs to be mapped dynamically and manually to a service on the SPBM network on the same SAP. This functionality is configured on a gateway switch that supports both ERP and SPBM.

This functionality is supported when there is more than one gateway switch between the access and backbone network for redundancy, as well as when there is a single gateway between the access and aggregation network. As a result, the following two types of topologies are supported:

- An access ERP ring connecting to an SPBM backbone.
- An ERP ring using an intermediate SPBM network as transport.The following CLI commands are associated with this feature:

The following CLI commands are associated with this feature:

- **access-untagged**, **access-tagged**, and **spb-remote-system** parameters added to the **erp-ring** command.

Microservice Marketplace

OmniVista (Enterprise or Cloud) has been identified as the marketplace for ALE microservices. OmniSwitch supports OmniVista to distribute and remotely install microservices. From 8.7R2, normal CLI and configure manager are used to sync the configuration between master and slave units in a VC. Starting from 8.7R2, the following “pkgmgr” CLI commands are changed:

- **pkgmgr/appmgr commit** is changed to **write memory**

- **pkgmgr lis**t is changed to **show pkgmgr**

- appmgr start has new **argument** keyword**.**

- appmgr list is replaced by **show appmgr.**

Introduction to Statistical Jitter in SAA

A new calculation of jitter values is implemented on each SAA probe. Each jitter that is calculated will be implemented as per a formula specified in RFC 1889, in the new “enhanced mode”.

Jitter is the variation in latency as measured in the variability over time of the packet latency across a network. A network with constant latency has no variation or jitter. By default, the inter-arrival jitter calculation is based on the round-trip time difference between two successive packets. The enhanced mode is to calculate inter-arrival jitter based on the formula specified in RFC 1889.

The following CLI commands are associated with this feature:

- saa jitter-calculation enhanced

- show saa

DHCP options 2 and 12

DHCP option 2 can be used to specify the time zone and DHCP option 12 can be used to specify the hostname. The automatic setting of the time zone from DHCP option 2 and 12 is supported through DHCP client IP interface, which can be either through user configured DHCP client IP interface or through Remote Config Load. Settings configured by the user will override the values obtained from DHCP.

The following CLI commands are associated with this feature:

- The **show system** command shows the current time zone that is effective.

- The **show ip interface dhcp-client** output is enhanced to reflect the time zone obtained through option 2 and option 12.

OAM PDU Support for EVC MEF OAM on per CVLAN\SVLAN Basis

Configuring Ethernet Virtual Circuits (EVC) MEGs or MEPs on per customer VLAN (CVLAN) in a SVLAN allows supporting connectivity and fault management on per CVLAN basis. The EVC MEG or MEP can be configured on the UNI-N of the provider bridge. The EVC MEG will assist the service provider to instantiate a MEP instance for each customer VLAN on the UNI-N port to perform OAM action for individual CVLAN traffic bound to the EVC.

The following CLI commands are associated with this feature:

- **ethoam endpoin**t; cvlan, ctag-priority, ctag-priority, and copy-outer-to-inner parameters added.

- **ethoam association** - allowed-cvlan-list parameter added.

- **show ethoam domain**

UNP Parity features

The following UNP Layer 3 functionality previously supported in the VLAN domain (on UNP bridge port) will now be supported in the service domain (on UNP access port):

- CP (Captive-Portal) /BYOD. Services: SPB, L2GRE.
- LTP (Location/Time Policy). Services: SPB, VXLAN, L2GRE.
- UNP User-Role. Services: SPB, VXLAN, L2GRE.
- UNP AP Mode. Services: SPB, VXLAN, L2GRE.
- UNP Kerberos Snooping. Services: SPB, VXLAN, L2GRE.

Increase Authentication Server Down Re-Auth Time

The authentication server down timer range is increased to 43200 seconds from 1000 seconds.The following CLI commands are associated with this feature:

- unp auth-server-down-timeout

DHCPv6 Guard Configuration using VLAN Range Option

Supports DHCPv6 guard VLAN and trusted port/linkage range configuration.

The following CLI commands are associated with this feature:

- ipv6 dhcp guard vlan
- ipv6 dhcp guard vlan trusted

USB-Ethernet Dongle for OOB Management

This feature allows for a USB-to-Ethernet interface for switches that lack on EMP port. This interface is treated just like EMP interface. All functions and CLI's related to EMP are applicable to USB-to-Ethernet dongle.

The following CLI commands are associated with this feature:

- ip interface emp

Support for additional tag-values under unp-profile mapped to services (spb/vxlan/l2gre)

When a device is dynamically assigned to a UNP profile that is mapped to service parameters, a service access point (SAP) is automatically created using the specified profile parameter values. Traffic from the device is then forwarded on the SAP.

A SAP is comprised of the UNP access port on which device traffic is received, a VLAN tag value for the SAP encapsulation, and a service instance. The encapsulation (tag value) identifies the traffic received on the UNP access port that the SAP will forward on the service instance that is associated with the SAP. The following tag value options were previously supported:

- 0 (zero) - The VLAN tag of the packet is used for the SAP encapsulation value.
- qtag - The outer VLAN ID tag is used for the SAP encapsulation to capture single-tagged traffic.
- outer_qtag:inner_qtag - An outer and inner VLAN ID tag is used for the SAP encapsulation to capture double-tagged traffic.

A new all tag value option is now supported and is used to capture all tagged and untagged packets that are not already classified into another SAP. This parameter is also configurable as the inner tag value to capture double-tagged packets with the specified outer VLAN ID and any inner VLAN ID (qtag:all). For example, "10:all" captures double-tagged packets with an outer VLAN ID of 10 and any inner VLAN ID.

The following CLI commands are associated with this feature:

- A new **all** encapsulation value option was added for the **tag-value** parameter of the **unp profile map service-type** command.The following CLI commands are associated with this feature:

Allow Uboot Shell Access after Authenticating with Password

OmniSwitch allows to secure the Uboot with the Uboot password authentication. When Uboot authentication is enabled, the Uboot shell can be accessed only after authenticating with the password. As of now Uboot authentication is supported only on OmniSwitch 6465. The password authentication is not enabled by default. It needs to be enabled by the administrator. The Uboot authentication can be enabled using the **uboot authentication** CLI command.

The following CLI commands are associated with this feature:

- uboot authentication {enable password *string* | disable}
- show uboot authentication

The string is the password. The password can be between 8 to 30 characters.

Note: In case of VC, the password must be reapplied on the new slave joining the VC.

Uboot Password Recovery

The uboot password cannot be modified at the uboot prompt. Only the admin user can modify or set the password using the uboot authentication command. If the user forgets the password, user can continue to normal AOS boot. The admin user can then modify or reset the uboot password.

Note: If the flash is corrupt and the uboot fails to start the AOS, the switch must be returned to the factory for repair. U-boot version 8.7.2.R02 is required.

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-26633	On an OS6360-PH24 the speed configuration is getting removed from the running config with reload of Master chassis where the config is related to Slave chassis. This issue is seen only on linkagg member ports and is observed only if combo ports are part of linkagg, no issues with fixed ports.	Reconfigure the speed on the member port.
CRAOS8X-26039	RTR:5367:PTP_P2P: ports going to toggling state with an error (ptpNi library(HAL_lib)) on console when P2P is enabled on port in OS6465 only.	1588 P2P not supported on 6465s. Documented in CLI guide
CRAOS8X-26103	Due to the timestamp variations across slots and the implmentation of SAA calculations in AOS, SAA eth-lb/dmm sessions fail if packet count is set for 1.	It is recommended to use a packet count of at least 5 for better results. This also applies to saa mac-ping.
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-19920	Between an OS6860N and an OS6860, when MACsec is enabled without encryption, the data packets are dropped. This is an interop issue between the OS6860N and the OS6860.	There is no known workaround. However, MACsec with encryption works properly and is the recommended operational mode for MACsec.

Hardware / Transceivers

CR	Description	Workaround
CRAOS8X-26236	On OS6900-X48C6/T48C6/X48C4E and OS6860N models fast hot-swaps of some transceivers can cause the switch not to detrect the transceiver.	It's recommended to wait approximately 10 seconds between removal and installation of transceiver.

CRAOS8X-24676	On an OS6900-X48C6/X48C4E "bcmd esm ERR" error messages are seen when inserting/removing an SFP-10G-T transceiver.	There is no known workaround at this time. This is a display issue only.
CRAOS8X-26489	On an 9900-XNI-U48, when an SFP-10G-SR is hot-swapped with an SFP-GIG-T transceiver, traffic continues to flow but LED remains off.	There is no known workaround at this time.

Layer 2 / Multicast

PR	Description	Workaround
CRAOS8X-26458	On an OS6465, multicast static neighbor and querier accepts linkagg ID's which are not present in the system.	There is no known workaround at this time.
CRAOS8X-25382	On an OS6860, an STP loop may be created for few seconds during MACsec interface toggle.	Leave the MACsec transmit-interval setting at the default value of 2 seconds.
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 pkts only.	There is no other functional impact or packet drop because of this issue.
CRAOS8X-7428	IPMS Proxy is not supported on a service.	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.
CRAOS8X-20826	On an OS6900, multicast packets are received on nack port after changing the active RP to different interface.	There is no known workaround at this time.

QoS

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-26247	On an OS6900-V72, ECN-STATS are not working with the 'show qos qsi linkagg 1 ecn-stats' command.	There is no known workaround at this time.
CRAOS8X-4424	With color-only policy action configuration, Egress queue are not honour the colour marking and packets drop is observed and expected traffic rate is not achieved.	There is no known workaround at this time.

Service Related

PR	Description	Workaround
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 SAPs across different ports.
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, hence no MACsec secure channel/association can be established.	There is no known workaround at this time.

Virtual Chassis

PR	Description	Workaround
CRAOS8X-914	Sometimes after a VC-takeover, one of the users that was learned in blocking on UNP access linkagg is getting flushed though the mac-aging timer has not expired.	There is no known workaround at this time.

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	
OS68-XNI-U4	OS68-XNI-U4
OS68-VNI-U4	OS68-VNI-U4
OS68-QNI-U2	OS68-QNI-U2
OS68-CNI-U1	OS68-CNI-U1

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: https://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
```

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

Appendix A: Feature Matrix

The following is a feature matrix for AOS Release 8.7R2.

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	6360	6465	6560	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6	6900-X48C4E	9900
Management Features											
AOS Micro Services (AMS)	8.7R2	8.6R1	8.6R1	8.6R1	8.7R1	8.6R1	8.6R1	8.6R1	8.7R1	8.7R2	8.6R1
Automatic Remote Configuration Download (RCL)	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.6R2	8.7R1	8.7R2	Y
Automatic/Intelligent Fabric	8.7R2	8.5R1	Y	Y	8.7R2	Y	Y	Y	Y	Y	Y
Automatic VC	8.7R2	N	Y	Y	8.7R1	Y	Y	8.6R2	8.7R1	8.7R2	N
Bluetooth - USB Adapter with Bluetooth Technology	8.7R2	8.6R2	8.6R2	Y	8.7R1	8.6R2	8.7R1	8.6R2	N	N	N
Console Disable	8.7R2	8.6R2	8.6R2	8.6R2	8.7R1	8.6R2	8.6R2	8.6R2	8.7R1	8.7R2	8.6R2
Dying Gasp	N	Y	Y	Y	8.7R1	Y	N	N	N	N	N
Dying Gasp (EFM OAM / Link OAM)	N	8.6R1	8.6R1	8.6R1	8.7R1	8.6R1	N	N	N	N	N
EEE support	N	N	N	Y	8.7R1	Y	Y	N	N	N	N
Embedded Python Scripting / Event Manager	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.7R2	8.7R2	8.7R2	N
IP Managed Services	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
Hitless Security Patch Upgrade	8.7R2	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R2	8.7R1
In-Band Management over SPB	N	N	N	8.5R4	8.7R1	8.5R4	8.5R4	8.5R4	8.7R1	8.7R2	8.5R4
ISSU	8.7R2	Y	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
NAPALM Support	8.7R2	8.5R1	8.5R1	8.5R1	8.7R1	8.5R1	8.5R1	8.7R2	8.7R2	8.7R2	N
NTP - Version 4.2.8.p11.	8.7R2	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.5R4	8.7R1	8.7R2	8.5R4
OpenFlow	N	N	N	Y	N	N	Y	N	N	N	N
OV Cirrus – Zero touch provisioning	8.7R2	Y	Y	Y	8.7R1	Y	Y	8.7R2	8.7R2	8.7R2	N
OV Cirrus – Configurable NAS Address	8.7R2	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.5R4	8.7R1	8.7R2	8.5R4
OV Cirrus – Default Admin Password Change	8.7R2	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.5R4	8.7R1	8.7R2	8.5R4
OV Cirrus – Managed	8.7R2	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.5R4	8.7R1	8.7R2	8.5R4
OVSDB	N	N	N	N	N	N	8.7R1 (X72/Q32)	8.7R1	N	N	N
Package Manager	8.7R2	8.6R2	8.6R2	8.6R2	8.7R1	8.6R2	8.6R2	8.6R2	8.7R1	8.7R2	8.6R2
Readable Event Log	8.7R2	8.6R1	8.6R1	8.6R1	8.7R1	8.6R1	8.6R1	8.6R1	8.7R1	8.7R2	8.6R1
Remote Chassis Detection (RCD)	N	N	N	8.6R2	8.7R1	N	Y	N	8.7R1	8.7R2	Y
SAA	8.7R2	8.5R1	8.7R2	Y	8.7R2	Y	Y	8.7R1	8.7R1	8.7R2	N
SAA SPB	N	N	N	Y	8.7R2	Y	Y	8.7R1	8.7R1	8.7R2	8.6R2
SAA UNP	N	Y	N	Y	N	Y	Y	N	N	N	N
SNMP v1/v2/v3	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
UDLD	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	N	N	N	EA
USB Disaster Recovery	8.7R2	8.5R1	Y	Y	8.7R1 (onie)	Y	Y	8.7R1 (onie)	8.7R1 (onie)	8.7R2 (onie)	Y

Feature	6360	6465	6560	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6	6900-X48C4E	9900
USB Flash (AOS)	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	N	N	N	N
Virtual Chassis (VC)	8.7R2	8.5R2	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
Virtual Chassis Split Protection (VCSP)	8.7R2	Y	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
VRF	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
VRF – IPv6	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
VRF – DHCP Client	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
Web Services & CLI Scripting	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.7R1	8.7R1	8.7R2	Y
Layer 3 Feature Support											
ARP	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
BFD	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
BGP	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
DHCP Client / Server	8.7R2	8.6R1	Y	Y	8.7R1	Y	Y	8.5R4	8.7R1	8.7R2	Y
DHCP Relay	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R4	8.7R1	8.7R2	Y
DHCPv6 Server	N	N	N	Y	8.7R1	Y	Y	8.7R1	8.7R1	8.7R2	Y
DHCPv6 Relay	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.7R1	8.7R1	8.7R2	Y
DHCP Snooping / IP Source Filtering	8.7R2	8.5R4	Y	Y	8.7R1	Y	Y	8.6R2	8.7R1	8.7R2	Y
ECMP	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
IGMP v1/v2/v3	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
GRE	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.5R2
IP-IP tunneling	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.5R2
IPv6	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
IPv6 - DHCPv6 Snooping	8.7R2	8.6R1	8.6R1	8.5R3	8.7R1	8.5R4	N	8.6R2	8.7R1	8.7R2	8.7R1
IPv6 - Source filtering	8.7R2	N	8.6R1	8.5R3	8.7R1	8.5R4	N	8.6R2	8.7R1	8.7R2	8.7R1
IPv6 - DHCP Guard	EA	EA	EA	EA	N	EA	N	N	N	N	N
IPv6 - DHCP Client Guard	EA	EA	EA	EA	N	EA	N	N	N	N	N
IPv6 - RA Guard (RA filter)	N	N	8.5R2	Y	8.7R1	Y	Y	N	N	N	N
IPv6 - DHCP relay and Neighbor discovery proxy	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	N	N	N	Y
IP Multinetting	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
IPSec (IPv6)	N	N	N	Y	8.7R1	Y	Y	N	N	N	EA
ISIS IPv4/IPv6	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.5R2
M-ISIS	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.5R2
OSPFv2	N	N	8.5R2[1]	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
OSPFv3	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
RIP v1/v2	N	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
RIPng	N	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y

Feature	6360	6465	6560	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6	6900-X48C4E	9900
UDP Relay (IPv4)	8.7R2	8.5R4	8.5R4	Y	8.7R1	Y	Y	8.5R4	8.7R1	8.7R2	8.5R4
UDP Relay (IPv6)	8.7R2	8.6R1	8.6R1	8.6R1	8.7R1	8.6R	8.6R1	8.6R1	8.7R1	8.7R2	8.6R1
VRRP v2	8.7R2	8.5R2	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
VRRP v3	8.7R2	8.5R2	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
Server Load Balancing (SLB)	N	N	N	Y	N	Y	Y	N	N	N	N
Static routing	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
Multicast Features											
DVMRP	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	N
IPv4 Multicast Switching	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
Multicast *,G	8.7R2	Y	8.5R2	8.5R2	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
IPv6 Multicast Switching	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
PIM-DM	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
PIM-SM	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
PIM-SSM	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R1	Y
PIM-SSM Static Map	N	N	N	N	N	N	N	N	N	N	N
PIM-BiDir	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
PIM Message Packing	N	N	N	8.6R1	8.7R1	N	8.6R1	8.6R1	8.7R1	8.7R2	N
PIM - Anycast RP	N	N	N	8.6R2	8.7R1	8.6R2	8.6R2	8.6R2	8.7R1	8.7R2	8.6R2
Monitoring/Troubleshooting Features											
Ping and traceroute	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
Policy based mirroring	N	N	N	Y	8.7R1	Y	Y	8.7R1	8.7R1	8.7R2	8.5R4
Port mirroring	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
Port monitoring	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
Port mirroring - remote	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	EA	N	N	EA
Port mirroring - remote over linkagg	N	N	N	Y	8.7R1	Y	Y	N	N	N	N
RMON	8.7R2	8.5R1	Y	Y	N	Y	Y	N	N	N	N
SFlow	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.7R1	8.7R1	8.7R2	Y
Switch logging / Syslog	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
TDR	N	N	N	Y	8.7R2	N	N	N	N	N	N
Layer 2 Feature Support											
802.1q	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
DHL	8.7R2	8.5R1	Y	Y	8.7R1	Y	N	N	N	N	N
ERP v2	N	8.5R1	8.5R2	Y	8.7R1	Y	Y	8.7R1	8.7R1	8.7R2	8.5R3
HAVLAN	N	EA	N	Y	N	Y	Y	8.6R2	8.7R1	8.7R2	EA

Feature	6360	6465	6560	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6	6900-X48C4E	9900
Link Aggregation (static and LACP)	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
LLDP (802.1ab)	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
Loopback detection - Edge (Bridge)	8.7R2	8.5R1	Y	Y	8.7R1	Y	N	8.6R2	8.7R1	8.7R2	Y
Loopback detection - SAP (Access)	N	N	N	Y	8.7R1	Y	Y	8.6R2	8.7R1	8.7R2	Y
MAC Forced Forwarding / Dynamic Proxy ARP	8.7R2	8.7R1	N	8.6R1	N	8.6R1	N	N	N	N	N
MRP	N	8.7R2	N	N	N	8.7R2	N	N	N	N	N
Port mapping	8.7R2	Y	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	N
Private VLANs (PVLAN)	N	N	N	Y	8.7R2	Y	Y	N	8.7R2	8.7R2	N
SIP Snooping	N	N	N	Y	N	N	N	N	N	N	N
Spanning Tree (1X1, RSTP, MSTP)	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
Spanning Tree (PVST+, Loop Guard)	8.7R2	N	Y	Y	8.7R1	Y	Y	N	N	N	EA
MVRP	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R4	8.7R1	8.7R2	Y
SPB[2]	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
SPB - Over Shared Ethernet	N	N	N	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R2	8.7R1
SPB - HW-based LSP flooding	N	N	N	N	N	N	N	N	N	N	8.5R4
QoS Feature Support											
802.1p / DSCP priority mapping	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
IPv4	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
IPv6	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
Auto-Qos prioritization of NMS/IP Phone Traffic	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
Auto-Qos - New MAC range	8.7R2	8.5R2	8.5R2	8.5R2	8.7R1	8.5R2	8.5R2	8.5R2	8.7R1	8.7R2	8.5R2
Groups - Port	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
Groups - MAC	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
Groups - Network	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
Groups - Service	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
Groups - Map	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
Groups - Switch	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
Ingress/Egress bandwidth limit	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
Per port rate limiting	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	N
Policy Lists	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.7R1	8.7R1	8.7R2	Y
Policy Lists - Egress	N	N	N	Y	8.7R1	Y	Y	8.7R1	8.7R1	8.7R2	N
Policy based routing	N	N	N	Y	8.7R1	Y	Y	8.6R2	8.7R1	8.7R2	EA
Tri-color marking	N	N	N	Y	8.7R1	Y	Y	N	N	N	N
QSP Profiles 1	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
QSP Profiles 2/3/4	N	N	N	Y	QSP-2 only	Y	Y	QSP-2 only	QSP-2 only	QSP-2 only	N

Feature	6360	6465	6560	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6	6900-X48C4E	9900
QSP Profiles 5	8.7R2	8.5R1	Y	8.7R1	8.7R1	8.7R1	8.7R1 (X72)	N	N	N	Y
Custom QSP Profiles	8.7R2	Y	Y	Y	Y	Y	X72 only (EA)	Y	Y	Y	Y
GOOSE Messaging Prioritization	N	8.7R1	N	N	N	8.7R1	N	N	**N**	**N**	**N**
Metro Ethernet Features											
CPE Test Head	N	8.6R1	N	N	N	N	N	N	N	N	N
Ethernet Loopback Test	N	N	N	8.6R1	8.7R1	8.6R1	N	N	N	N	N
Ethernet Services (VLAN Stacking)	N	8.5R1	N	Y	8.7R2	Y	Y	8.5R4	8.7R1	8.7R2	N
Ethernet OAM (ITU Y1731 and 802.1ag)	N	8.5R1	N	Y	8.7R1	Y	Y	8.7R1	8.7R1	8.7R2	EA
EFM OAM / Link OAM (802.3ah)	N	8.6R1	8.6R1	8.5R4	8.7R2	8.5R4	N	N	N	8.7R2	N
PPPoE Intermediate Agent	N	8.6R1	N	N	N	8.6R1	N	N	N	N	N
1588v2 End-to-End Transparent Clock	N	8.5R1	8.7R2	Y	N	Y	Y (X72/Q32)	N	N	N	N
1588v2 Peer-to-Peer Transparent Clock	N	N	8.7R2	N	N	N	N	N	N	N	N
1588v2 Across VC	N	N	N	N	N	N	8.5R2 (X72)	N	N	N	N
Access Guardian / Security Features											
802.1x Authentication	8.7R2	8.5R2	Y	Y	8.7R1	Y	Y	8.7R1	8.7R1	8.7R2	Y
Access Guardian – Bridge	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.6R1	8.7R1	8.7R2	Y
Access Guardian - Access	N	N	N	Y	8.7R1	Y	Y	8.5R4	8.7R1	8.7R2	Y
Application Fingerprinting	N	N	N	N	N	N	Y	N	N	N	N
Application Monitoring and Enforcement (Appmon)	N	N	N	Y	8.7R2	N	N	N	N	N	N
ARP Poisoning Protection	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	Y
BYOD - COA Extension support for RADIUS	8.7R2	Y	Y	Y	8.7R1	Y	8.62	8.6R2	8.7R1	8.7R2	Y
BYOD - mDNS Snooping/Relay	8.7R2	Y	Y	Y	8.7R1	Y	8.62	8.6R2	8.7R1	8.7R2	Y
BYOD - UPNP/DLNA Relay	8.7R2	Y	Y	Y	8.7R1	Y	8.62	8.6R2	8.7R1	8.7R2	Y
BYOD - Switch Port location information pass-through in RADIUS requests	8.7R2	Y	Y	Y	8.7R1	Y	8.62	8.6R2	8.7R1	8.7R2	Y
Captive Portal	8.7R2	8.5R4	Y	Y	8.7R1	Y	8.62	8.6R2	8.7R1	8.7R2	Y
IoT Device Profiling	8.7R2	8.5R2	8.5R2	8.5R2	8.7R1	8.5R2	8.5R2	8.6R1	8.7R1	8.7R2	8.5R2
IoT Device Profiling (IPv6)	8.7R2	8.7R1	8.7R1	8.7R1	N	8.7R1	8.7R1	N	N	N	8.7R1
Directed Broadcasts – Control	8.7R2	8.5R2	8.5R2	8.5R2	8.7R1	8.5R2	8.5R2	8.7R1	8.7R1	8.7R2	Y
Interface Violation Recovery	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.7R1	8.7R1	8.7R2	Y
Kerberos Snooping	8.7R2	N	8.6R2	8.6R2	N	8.6R2	8.6R2	8.6R2	N	N	8.6R2
L2 GRE Tunnel Access (Edge) (bridge ports)	N	N	Y	Y	8.7R2	Y	8.6R1[3]	8.7R1	8.7R2	8.7R2	Y
L2 GRE Tunnel Access (Edge) (access ports)	N	N	N	8.6R1	8.7R2	8.6R1	8.6R1	8.7R1	8.7R2	8.7R2	8.6R1
L2 GRE Tunnel Aggregation	N	N	N	Y	8.7R2	Y	Y[3]	8.7R1	8.7R2	8.7R2	Y
Learned Port Security (LPS)	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R4	8.7R1	8.7R2	Y
MACsec[4]	N	8.5R1	8.5R4	Y	8.7R1	N	N	N	N	X48C4E	8.5R2

Feature	**6360**	**6465**	**6560**	**6860(E)**	**6860N**	**6865**	**6900**	**6900-V72/C32**	**6900-X48C6/T48C6**	**6900-X48C4E**	**9900**
MACsec MKA Support[4]	N	8.5R2	8.5R4	8.5R2	8.7R1	N	N	N	N	X48C4E	8.5R2
Quarantine Manager	N	8.7R2	8.7R2	Y	8.7R2	Y	8.7R2	8.7R2	8.7R2	8.7R2	8.7R2
RADIUS - RFC-2868 Support	8.7R2	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.5R4	8.7R1	8.7R2	8.5R4
Role-based Authentication for Routed Domains	N	N	N	8.5R4	8.7R1	8.5R4	8.5R4	8.6R1	8.7R1	8.7R2	8.5R4
Storm Control (flood-limit)	N	N	N	Y	8.7R1	Y	Y	Y	8.7R1	8.7R2	N
Storm Control (Unknown unicast with action trap/shutdown)	N	N	N	Y	Y	Y	Y	N	N	N	N
TACACS+ Client	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.6R1	8.7R1	8.7R2	Y
TACACS+ command based authorization	8.7R2	N	N	Y	8.7R1	Y	Y	8.7R2	8.7R2	8.7R2	N
PoE Features											
802.3af and 802.3at	8.7R2	8.5R1	Y	Y	8.7R1	Y	N	N	N	N	Y
802.3bt	8.7R2	N	8.6R2	N	8.7R1	N	N	N	N	N	N
Auto Negotiation of PoE Class-power upper limit	8.7R2	8.5R1	Y	Y	8.7R1	Y	N	N	N	N	Y
Display of detected power class	8.7R2	8.5R1	Y	Y	8.7R1	Y	N	N	N	N	Y
LLDP/802.3at power management TLV	8.7R2	8.5R1	Y	Y	8.7R1	Y	N	N	N	N	Y
HPOE support	8.7R2 (95W)	8.5R1 (60W)	Y (95W)	Y (60W)	8.7R1 (95W)	Y (75W)	N	N	N	N	Y (75W)
Time Of Day Support	8.7R2	8.5R1	Y	Y		Y	N	N	N	N	Y
Perpetual PoE	8.7R2	N	N	Y	Y	Y	N	N	N	N	N
Fast PoE	8.7R2	N	N	Y	Y	Y	N	N	N	N	N
Data Center Features (License May Be Required)											
CEE DCBX Version 1.01	N	N	N	N	N	N	Y	N			N
Data Center Bridging (DCBX/ETS/PFC)	N	N	N	N	N	N	Y	N	N	N	N
EVB	N	N	N	N	N	N	N	N	N	N	N
FCoE / FC Gateway	N	N	N	N	N	N	Y	N	N	N	N
VXLAN[5]	N	N	N	N	N	N	Q32/X72	8.5R3	N	N	N
VM/VXLAN Snooping	N	N	N	N	N	N	Y	N	N	N	N
FIP Snooping	N	N	N	N	N	N	Y	N	N	N	N

Notes:
1. OS6560 supports stub area only.
2. See protocol support table in Appendix B.
3. Not supported on 6900-T20/T40/X20/X40.
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)	OmniSwitch 6900-T48C6/X48C6	OmniSwitch 6860N
IPv4 Protocols				
Static Routing	Y	8.6R2	8.7R2	8.7R2
RIP v1/v2	Y	8.6R2	8.7R2	8.7R2
OSPF	Y	8.6R2	8.7R2	8.7R2
BGP	Y	8.6R2	8.7R2	8.7R2
VRRP	Y	8.7R1	8.7R2	8.7R2
IS-IS	N	N	N	N
PIM-SM/DM	8.5R3	8.6R2	N	N
DHCP Relay	8.5R3	8.6R2	8.7R2	8.7R2
UDP Relay	8.5R4	8.6R2	8.7R2	8.7R2
DVMRP	N	N	N	N
BFD	8.7R2	8.7R2	8.7R2	8.7R2
IGMP Snooping	Y	8.6R2	8.7R2	8.7R2
IP Multicast Headend Mode	Y	8.6R2	8.7R2	8.7R2
IP Multicast Tandem Mode	8.5R4	8.6R2	N	N
IPv6 Protocols				
Static Routing	8.5R4	8.6R2	8.7R2	8.7R2
RIPng	8.5R4	8.6R2	8.7R2	8.7R2
OSPFv3	8.5R4	8.6R2	8.7R2	8.7R2
BGP	8.5R4	8.6R2	8.7R2	8.7R2
VRRPv3	8.5R4	8.7R1	8.7R2	8.7R2
IS-IS	N	N	N	N
PIM-SM/DM	8.5R4	8.6R2	N	N
DHCP Relay	8.6R1	8.7R2	8.7R2	8.7R2
UDP Relay	8.6R1	8.7R2	8.7R2	8.7R2
BFD	8.7R2	8.7R2	8.7R2	8.7R2
IPv6 MLD Snooping	Y	8.7R2	8.7R2	8.7R2
IPv6 Multicast Headend Mode	Y	8.7R2	8.7R2	8.7R2
IPv6 Multicast Tandem Mode	8.5R4	8.7R2	N	N

Note: Inline routing support for the OS6900-X48C4E is an EA feature in 8.7R2.

External Loopback Support							
	OmniSwitch 9900	OmniSwitch 6860/6865	OmniSwitch 6860N	OmniSwitch 6900	OmniSwitch 6900-V72/ C32	OmniSwitch 6900-X48C6/ T48C6	OmniSwitch 6900-X48C4E
IPv4 Protocols							
Static Routing	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2
RIP v1/v2	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2
OSPF	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2
BGP	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2
VRRP	8.6R1	8.5R4	8.7R1	Y	8.7R1	8.7R2	8.7R2
IS-IS	Y	Y	Y	Y	Y	Y	8.7R2
PIM-SM/DM	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2
DHCP Relay	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.7R1	8.7R2
UDP Relay	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.7R1	8.7R2
DVMRP	N	N	N	N	N	N	N
BFD	Y	Y	Y	Y	Y	Y	8.7R2
IGMP Snooping	8.5R4	Y	8.7R1	Y	8.6R1	8.7R1	8.7R2
IP Multicast Headend Mode	8.5R4	Y	8.7R1	Y	8.6R1	8.7R1	8.7R2
IP Multicast Tandem Mode	8.5R4	Y	8.7R1	Y	8.6R1	N	N
IPv6 Protocols							
Static Routing	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2
RIPng	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2
OSPFv3	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2
BGP	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2
VRRPv3	8.5R4	8.5R4	8.7R1	Y	8.7R1	8.7R2	8.7R2
IS-IS	Y	Y	Y	Y	Y	Y	8.7R2
PIM-SM/DM	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.7R1	8.7R2
DHCP Relay	8.6R1	8.6R1	8.7R1	8.6R1	8.6R1	8.7R1	8.7R2
UDP Relay	8.6R1	8.6R1	8.7R1	8.6R1	8.6R1	8.7R1	8.7R2
BFD	Y	Y	Y	Y	Y	Y	8.7R2
IPv6 MLD Snooping	8.5R4	Y	8.7R1	Y	Y	8.7R2	8.7R2
IPv6 Multicast Headend Mode	8.5R4	Y	8.7R1	Y	Y	8.7R2	8.7R2
IPv6 Multicast Tandem Mode	8.5R4	Y	8.7R1	Y	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 8.7R2 (GA)
OS6465	8.6.289.R01 (GA) 8.6.299.R01 (MR) 8.6.189.R02 (GA) 8.6.196.R02 (MR) 8.6.203.R02 (reGA) 8.7.277.R01 (GA) 8.7.280.R01 (MR) 8.7.354.R01 (GA)
OS6560	8.6.289.R01 (GA) 8.6.299.R01 (MR) 8.6.189.R02 (GA) 8.6.196.R02 (MR) 8.6.203.R02 (reGA) 8.7.354.R01 (GA)
OS6860(E)	8.6.289.R01 (GA) 8.6.299.R01 (MR) 8.6.189.R02 (GA) 8.6.196.R02 (MR) 8.6.203.R02 (reGA) 8.7.277.R01 (GA) 8.7.280.R01 (MR) 8.7.354.R01 (GA)
OS6860N	8.7.277.R01 (GA) 8.7.280.R01 (MR) 8.7.354.R01 (GA)
OS6865	8.6.289.R01 (GA) 8.6.299.R01 (MR) 8.6.189.R02 (GA) 8.6.196.R02 (MR) 8.6.203.R02 (reGA) 8.7.277.R01 (GA) 8.7.280.R01 (MR) 8.7.354.R01 (GA)
OS6900	8.6.289.R01 (GA) 8.6.299.R01 (MR) 8.6.189.R02 (GA) 8.6.196.R02 (MR) 8.6.203.R02 (reGA) 8.7.277.R01 (GA) 8.7.280.R01 (MR) 8.7.354.R01 (GA)
OS6900-V72/C32	8.6.289.R01 (GA) 8.6.299.R01 (MR) 8.6.189.R02 (GA) 8.6.196.R02 (MR)

	8.6.203.R02 (reGA) 8.7.277.R01 (GA) 8.7.280.R01 (MR) 8.7.354.R01 (GA) See Appendix G when upgrading an OS6900-V72/C32.
OS6900-X48C6/T48C6	8.7.277.R01 (GA) 8.7.280.R01 (MR) 8.7.354.R01 (GA)
OS9900	8.6.289.R01 (GA) 8.6.299.R01 (MR) 8.6.197.R02 (GA) 8.6.203.R02 (reGA) 8.7.354.R01 (GA)

8.7R2 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
  - Refer to Appendix F for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6560 – Nos.img
  - Refer to Appendix F for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6860 – Uos.img
  - Refer to Appendix F for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6860N – Uosn.img
- OS6865 – Uos.img
  - Refer to Appendix F for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6900 **-** Tos.img
  - Refer to Appendix F for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- 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           8.7.252.R02             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
  - Refer to Appendix F for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6560 – Nos.img
  - Refer to Appendix F for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6860 – Uos.img
  - Refer to Appendix F for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6860N – Uosn.img
- OS6865 – Uos.img
  - Refer to Appendix F for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6900 **-** Tos.img
  - Refer to Appendix F for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6900-V72/C32 – Yos.img. See Appendix G.
- OS6900-X48C6/T48C6 – Yos.img.
- OS9900 – Mos.img, Mhost.img, Meni.img
- ISSU Version File - issu_version
- imgsha256sum (not required) –This file is only required when running in Common Criteria mode. Please refer to the Common Criteria Operational Guidance Document for additional information.

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

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

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

3. Clean up existing ISSU directories

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

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

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

```
OS6900-> ssh 127.10.2.65
Password:switch
```

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

```
6900-> rm –r /flash/issu_dir
```

6. Log out of the Slave chassis:

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

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

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

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

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

9. Upgrade the image files using ISSU:

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

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

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

This indicates that the ISSU is completed

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

Allow the upgrade to complete. DO NOT modify the configuration files during the software upgrade. It normally takes between 5 and 20 minutes to complete the ISSU upgrade. Wait for the System ready or [L8] state which gets displayed in the ssh/telnet/console session before performing any write-memory or configuration changes.

```
6900-> debug show virtual-chassis topology
Local Chassis: 1
Oper                                       Config   Oper                      System
```

```
Chas  Role         Status              Chas ID  Pri   Group  MAC-Address        Ready
-----+------------+-------------------+--------+-----+------+------------------+-------
1     Master        Running             1        100   19     e8:e7:32:b9:19:0b  Yes
2     Slave         Running             2        99    19     e8:e7:32:b9:19:43  Yes
```

10. Verify the Software Upgrade

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

```
OS6900-> show microcode
/flash/working
Package           Release                 Size      Description
-----------------+------------------------+--------+-----------------------------------
Tos.img           8.7.252.R02              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	Description	Switch does not shutdown after crossing danger threshold temperature.
	FPGA Version	0.7
	Platforms	OS6465-P28
CRAOS8X-7207	Description	Chassis reboots twice to join a VC.
	FPGA Version	0.7
	Platforms	OS6560-P24Z24,P24Z8,P48Z16 (903954-90)
CRAOS8X-4150	Description	VC LED status behavior.
	U-boot Version	0.12
	Platforms	OS6865-U28X
8.7R1 Release		
CRAOS8X-16452	Description	Port remains UP when only SFP is connected.
	FPGA Version	- 0.6 (OS6560-P48Z16 (904044-90)) - 0.7 (OS6560-48X4, OS6560-P48X4) - 0.8 (OS6560-X10)
	Platforms	OS6560-P48Z16 (904044-90), OS6560-48X4, OS6560-P48X4, OS6560-X10
CRAOS8X-11118	Description	1000BaseT SFP interface up before system ready
	U-boot/FPGA Version	- U-boot version 8.6.R02.189 - FPGA version 0.1.11
	Platforms	OS6900-X72
Fast/Perpetual PoE	Description	Fast and Perpetual PoE Support
	FPGA Version	0.7 (OS6860E-P24Z8) 0.10 0.14 (OS6865-U28X) 0.25 (OS6865-P16X/U12X)
	Platforms	OS6860/OS6865
8.7R2 Release		
CRAOS8X-4813/13440)	Description	Uboot unable to mount NAND flash with UBIFS errors
	U-boot Version	8.7.2.R02
	Platforms	6465(T), 6560-24X4/P24X4/48X4/P48X4/X10
CRAOS8X-13819	Description	Uboot unable to mount eUSB flash
	U-boot Version	8.7.2.R02
	Platforms	6560-24Z24/P24Z24/24Z8/P24Z8/P48Z16(903954-90/904044-90), 6865
CRAOS8X-22857	Description	OS6560-P24Z24 reloads continuously with pmds
	FPGA Version	0.8
	Platforms	6560-24Z24/P24Z24/24Z8/P24Z8/P48Z16 (903954-90)
1588v2 Support	Description	1588v2 Support
	FPGA Version	0.7 (OS6560-P48Z16 (904044-90)) 0.8 (OS6560-48X4/P48X4)
	Platforms	OS6560-48X4/P48X4/P48Z16(904044-90)

U-boot Password Authentication	Description	U-boot password support (Early Availability)
	U-boot Version	8.7.2.R02
	Platforms	OS6465

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_7277
- U-boot.8.7.R02.2.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_7277
Parse /flash/fpga_kit_7277
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.8.7.R02.2.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 8.6R01 - 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 8.7.252.R02 release.

CR/PR NUMBER	Description
Case: 00515437 CRAOS8X-24521	**Summary:** On 6560 VC, under **show license-info** 10G license is showing installed only on the master chassis but not the slave chassis. **Explanation:** It is a display issue, as the related interfaces are operating at 10G speed. This issue is fixed as from AOS 8.7R02 GA. 🔒 Click for Additional Information
Case: 00470907 CRAOS8X-20742	**Summary:** Slow upload speed when transfer the file from PC to switch via SFTP, FTP. **Explanation:** Average upload speed is 200-250KB/s. The issue is noticed when the IP interface in "no forward" status Workaround - Configure the IP interface in "forward" status in order to resolve the issue 🔒 Click for Additional Information
Case: 00491454 CRAOS8X-22236	**Summary:** OS6900/OS6860 Unable to authenticate via radius user**.** **Explanation:** The switch could ping with radius server with server name. However, the "radcli" could not resolve the radius server host name. 🔒 Click for Additional Information
Case: 00493654 00516325 CRAOS8X-22235	**Summary:** OS6860 SNMP traps "last field of OID duplicated" **Explanation:** Consider the OID of “chassisTrapsObjectType 1.3.6.1.4.1.6486.801.1.1.1.3.1.1.13.9.0”, however when sending the trap to NMS it will be like 1.3.6.1.4.1.6486.801.1.1.1.3.1.1.13.9.9.0. 🔒 Click for Additional Information
Case: 00508200 CRAOS8X-24125	**Summary:** Radius Health check does not take into account the ip service source-ip interface **Explanation:** When sending the Radius Access-Request when doing Health-Check, the switch does not check the ip service source-ip interface set for Radius, as a consequence the request is not received by Radius Server and aaa authentications are not proceeded 🔒 Click for Additional Information
Case: 00522779 CRAOS8X-25557	**Summary:** OS6465 logs lpCmm growing quickly **Explanation:** Lanpower is generating lot of logs as below: LanCmm ERR: lpCmmGetNiMaxPower 4997:lpVcCmmUtilInfoFind fails LanCmmUtl INFO: lpVcCmmUtilInfoFind 513 lpVcCmmInfo Not Found

	🔒 Click for Additional Information
Case: 00478366 CRAOS8X-20792	**Summary:** Blackhole route configuration is lost after the reload **Explanation:** This behavior is seen because the blackhole route is added to the inactive static route queue after reload. This causes the route removal from the config. 🔒 Click for Additional Information
Case: 00474945 CRAOS8X-20335	**Summary:** Timeout is notice in the OS6560 while querying the MIB "lldpRemManAddrTable" (OID 1.0.8802.1.1.2.1.4.2) **Explanation:** Timeout is seen due to the incorrect decoding of the OID values in the BER. LLDP frame contains BER encoded OID values in management address tlv. The Encoded values are used directly in lldpcmm without decoding the OID values which causes the timeout issue. 🔒 Click for Additional Information
Case: 00531024 CRAOS8X-26437	**Summary:**. "pmApiGetLAGIdForPP" entry in the swlogs **Explanation:** This entry is seen due to incorrect registeration in port manager. 🔒 Click for Additional Information
Case: 00504102 CRAOS8X-24078	**Summary:** Access-request is not triggered from switch after the upgrade from 8.6 R02 to any 8.7 R01 microcode. **Explanation:** SSH auth using radius server is not getting success due to the access-request is not egressing from the switch. Attributes are returning from the server when doing the test radius server. But, when trying to authenticate the switch, login fail will occur. This is due to the incorrect server type is seen in radcli data structure 🔒 Click for Additional Information
Case: 00506973 CRAOS8X-23554	**Summary:** Configuration of L2-Profile on UNP Ports does not appear in "show configuration snapshot" **Explanation:** Configuring l2-profile is not displaying per port and sub range of ports because of snapshot issue for UNP ports. 🔒 Click for Additional Information
Case: 00511707 CRAOS8X-24188	**Summary:** 32 characters not supported in ip dhcp relay interface if_name **Explanation:** This is due to the extra characters appended at the end of if_name, when interface name is configured of length 32. "12" is appended at the end of if_name in the above example. 🔒 Click for Additional Information
Case:	**Summary:**

00478154 CRAOS8X-20673	"PL error" logs seen in the swlogs. **Explanation:** The entry is due to invalid values in pd->dst_asic field of pd header.This PL error log doesn't indicate an impacting error and is internally used. Click for Additional Information
Case: 00496695 CRAOS8X-22495	**Summary:** CVLAN double tagged packet egress via UNI port **Explanation:** This behavior seen because of the stale translate profile remained in the hardware. **Click for Additional Information**
Case: 00504720 CRAOS8X-23154	**Summary:** show configuration snapshot returns ERROR: Unable to retrieve PVLAN snapshot. **Explanation:** When PVLAN has more than 100 line of configuration MIP overflow occurs. This cause the command “show configuration snapshot” to returns error. Click for Additional Information
Case: 00510850 CRAOS8X-23895	**Summary:** In console after loading new AOS image files and booting up as 8.7.354 R01. tcamni main ERR message error is seen. **Explanation:** This error occurs when checking of expansion module in the switch. As per hardware guide it is seen that there is no expansion slot support for OS6900-V72 model. Fix is given to reduce severity of the error logs which gets printed in console during expansion slot check is reduced in in OS6900-V72 as it has no expansion slot. Click for Additional Information
Case: 00487318 00495612 00501948 00501938 CRAOS8X-21531	**Summary:** XNI-U48 of OS9900 Not Passing Traffic on 8 Ports of one ASIC. **Explanation:** Toggling of some ports in XNI-U48 at a very high rate caused the interruption handler of the ASIC to get frozen. Click for Additional Information
Case: 00473460 CRAOS8X-20076	**Summary:** After upgrading OV to 4.5R1, extraneous “lpCmm LanCmm” messages appear in OS900 swlogs. **Explanation:** The lpCmm LanCmm Mip/Utl messages in the swlog are related to LanPower. OS9900 chassis supports PoE, but the NIs used in this chassis are not P series and don’t support PoE, therefore, the lanpower related configuration are not possible. Hence, when there is no lanpower configuration and SNMP getnext action is performed from SNMP server (like OV2500, OVCirrus etc) these logs will be printed in swlogs.

	🔒 Click for Additional Information
Case: 00487352 CRAOS8X-21499	**Summary:** UNP user classified with vlan-tag on a profile assigned to another vlan, shows a profile source as: MAC OUI Rule UNP - Tag Mismatch - Block. **Explanation:** Tag Mismatch – block" is displayed when tag value is not matched and user gets classified in proper profile due to trust-tag enabled. It is a display problem. 🔒 Click for Additional Information
Case: 00515056 CRAOS8X-24469	**Summary:** OS6900-X72 slave chassis 1 has 20x linkagg ports not coming Up after reboot/reload. **Explanation:** On VC-2 OS6900-X72 reboot/or reload of slave chassis will cause some linkagg ports not to come up, due to a timing issue in the HW ports programming steps of the initialization/bootup. Another reload of the slave chassis will make the ports to come up. 🔒 Click for Additional Information
Case: 00518452 CRAOS8X-24918	**Summary:** OS6860 having multiple UNP access ports with Aps connected to it , show constant memory increase on slave chassis. **Explanation:** Memory dynamically allocated during dynamic SAP/Service add/deletion was not freed on slave chassis only. Reloading the whole VC will lower the memory usage on slave chassis. 🔒 Click for Additional Information
Case: 00519261 CRAOS8X-25031	**Summary:** VC of OS6860 showed a memory usage increase on all chassis. **Explanation:** Intense Port flapping have triggered a memory usage increase of rmon task, shared on all chassis. Fixing the port flapping only will not solve the problem. Reloading the whole VC will clear this memory usage. 🔒 Click for Additional Information
Case: 00521375 CRAOS8X-22525	**Summary:** VC of OS6860 showed a memory usage increase on one chassis. **Explanation:** Intense Port flappings have triggered a memory usage increase of lbdni task, on the chassis where the flapping occurred. Fixing the port flapping only will not solve the problem. Reloading the chassis will clear this memory usage. 🔒 Click for Additional Information
Case: 00511701 CRAOS8X-24020	**Summary:** SPB adjacency on NNI ports is down **Explanation:**

	When the SPB ports are configured to be the NNI ports as well, the ISIS Hello packets are not trapped to CPU. This is the reason SPB adjacency is not formed. This issue is seen specifically in 8.7.354 R01 🔒 Click for Additional Information
Case: 00492186 CRAOS8X-22177	**Summary:** NTP reachability value not correct in the CLI/SNMP show output **Explanation:** The reachability field in NTP show command was stuck at 0 even if the NTP server is reachable, as per RFC this value should be 377. 🔒 Click for Additional Information
Case: 00464149 CRAOS8X-18501	**Summary:** Some unexpected behavior with the priv-mask feature in enhanced Mode. **Explanation:** The read-write access will be allowed only for http/https access types. For other access types console, telnet and ssh only read-only access is allowed. 🔒 Click for Additional Information
Case: 00505742 CRAOS8X-23647	**Summary:** Once Windows PC turned On, MAC authentication is successful however once 802.1x Auth is triggered from PC the redirection is not happening hence the user is blocked in a UNP profil for MAC auth. **Explanation:** AS the redirection from MAC authentication to 802.1x authentication because of URL link of redirction sent back in the MAC authentication response. Fix is merged in 8.7R02. 🔒 Click for Additional Information
Case: 00505572 CRAOS8X-23287	**Summary:** “Not updating the Vpa state” log is shown in swlog and syslog after a power maintenance window **Explanation:** As master rebooted and a linkagg connected but down when it rebooted as slave was trying to update the VPA of the link down (standby firewall). This synchronization of the VPA state “Not updating the Vpa state” is fixed in 8.7R02 GA. 🔒 Click for Additional Information
Case: 00473846 CRAOS8X-20200	**Summary:** OS6860 - Incorrect SNMP output for untagged VLANs **Explanation:** The MIB OID "dot1qVlanCurrentUntagPorts" returns an incorrect bitmap indexing (off by 24 bits), while "dot1qVlanCurrentEgressPorts" is returns the correct index value for the SNMP walk output. The fix is available in 8.7R02. 🔒 Click for Additional Information
Case: 00512469 CRAOS8X-24557	**Summary:** OS6900: Continuous error and warn alerts

	Explanation: "qosGetPlInfoFromModidDport 129" error messages constantly generated in OS6900 switch Fix is available in AOS 8.7R02. 🔒 Click for Additional Information
Case: 00450337 CRAOS8X-17551	**Summary:** How SNMP traps for DDM Output Power processed? **Explanation:** Digital Diagnostics Monitoring allows the switch to monitor the status of a transceiver by reading the information contained on the transceiver's EEPROM. Every time the Output Power (Rx) crosses the Alarm High to Warning High, AOS 8.X sends a trap notification. When the status falls back to the threshold limit of Alarm High from Warning High, no trap notification will be sent. Code changes done to clear DDM violation when the real-time value falls within the threshold limit and to send trap even for the scenario like AH -- WH -- AH. 🔒 Click for Additional Information
Case: 00474782 CRAOS8X-20502	**Summary:** OS6465: PoE Input Voltage dropped below AT lower Threshold 52V **Explanation:** The following PoE logs were generated every 20 seconds on the OS6465 switch that uses ALE recommended power supply. swlogd lpNi LanNi INFO: lpProcessPowerSupplyVoltage 2994:PoE Input Voltage dropped below AT lower Threshold 52V(voltage: 471) The severity level will be changed to debug1 from AOS 8.7.R02. 🔒 Click for Additional Information
Case: 00466533 CRAOS8X-15567	**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. The issue is fixed from AOS 8.7 R01. 🔒 Click for Additional Information
Case: 00504424 CRAOS8X-24891	**Summary:** OS6860 - ip dhcp relay getting enabled after the switch reboot. **Explanation:** When disabling IP DHCP relay in the switch 6860, after reboot it is not reflecting in the switch config (vcboot.cfg). Found the DHCP relay is still enabled. The issue is fixed from AOS 8.7.R02 GA. 🔒 Click for Additional Information
Case: 00506094 CRAOS8X-23295	**Summary:** OS6860E-P24 switch does not display the FAN information. **Explanation:**

	After the upgrade to AOS 8.7R01, the OS6860E-P24 switch does not display the FAN information. The switch display the output as "This product has no fans". This issue is not seen in the OS6860-24, OS6860-48 and OS6860E-P48 switches. 🔒 Click for Additional Information
Case: 00507112 CRAOS8X-23410	**Summary:** Lanpower "power-policy" command repeated in the switch configuration. **Explanation:** configChangeStatus value and show running-directory Whenever the "power-policy" was mapped to any of the lanpower port, the Lanpower "power-policy" command would be repeated in the switch configuration. 🔒 Click for Additional Information
Case: 00507648 00507815 00508326 CRAOS8X-23525	**Summary:** After the upgrade to 8.7.354R01, UNP user table in the switch intermittently display only the IPV4 or IPV6 address of End devices. **Explanation:** Current working behavior is, the IP information in the packet which comes first for user authentication to the switch is displayed in the UNP user output. If the End device support both IPV4 and IPV6 address and the switch software receives an IPV6 packet for authentication, then the "show unp user" displays the IPV6 information. Like vice, if the software receives an IPV4 packet, then the IPV4 information would be displayed. Until 8.6R02, the user table in the switch displayed only the IPV4 address of the End device, even when the user support IPV6 address. Fix provided is to give priority to IPV4 address, if the End device supports both IPV4 and IPV6 address. 🔒 Click for Additional Information
Case: 00507996 CRAOS8X-23539	**Summary:** Lanpower power-policy configuration could be removed even when it is mapped to several Lanpower port. **Explanation:** OS6560 switch allow the user to remove the power-policy configuration, even when it is mapped in different lanpower configuration. Fix provided is to restrict the removal of power-policy, if the policy is mapped to several lanpower port. 🔒 Click for Additional Information
Case: 00507995 CRAOS8X-23538	**Summary:** No option to delete individual ports from lanpower port groups. **Explanation:** If lanpower power-policy is applied to a group of lanpower ports, then there is no option to remove individual lanpower ports from the configuration. Support for deletion of individual ports from lanpower port groups is added in 8.7R02 🔒 Click for Additional Information
Case: 00511798 CRAOS8X-24013	**Summary:** Lanpower power-policy config does not work on Friday.

	Explanation: Lanpower in switch does not start on Friday, if the Lanpower power-policy configured from Monday to Friday. The lanpower in the switch works between Monday to Thursday; however, on Friday the lanpower in the switch does not start. 🔒 Click for Additional Information
Case: 00501333 CRAOS8X-22774	**Summary:** Vulnerability check for CVE 2020-12351 | 2020-12352 | 2020-24490. **Explanation:** BlueZ vulnerabilities: Improper input validation in BlueZ may allow an unauthenticated user to potentially enable the following via adjacent access Escalation of privilege | Information disclosure | Denial of service. 🔒 Click for Additional Information
Case: 00495286 CRAOS8X-22276	**Summary:** IoT devices on 6860s are not getting DHCP IP when the profile source is OV enforced UNP. MAC-learning and UNP output are inconsistent for these devices. **Explanation:** IoT devices are connected on UNP spb-access port to undergo 802.1x/MAC authentication with UPAM and no classification/rules are configured. Access-Guardian has cached the IoT MAC-address and OVE returned profile before the MAC is learnt on the table. Here, Access Guardian did not pause for L2-Engine until it gets the response from service manager task to create the entry for service ID, VP and VFI values leading to VP-0 and VFID-0 and thus no MAC-learning happens. Fix is given to make Access Guardian pause the L2-Engine for service manager to create the UNP servicing entry and then forward it to source-learning. 🔒 Click for Additional Information
Case: 00484564 CRAOS8X-21158	**Summary:** After hot swapping faulty with working power supply, airflow was detected incorrectly and powersupply was not operational in OS6900-X72. **Explanation:** The Chassis Supervision power manager did not set the error count to zero when the faulty power supply was detected. There was an error reading PS as error count value remained in non-zero when working power supply was hot swapped on the same power supply slot. The Chassis Supervision fan and temperature manager updated the airflow as unknown for the same reason. Fix is given to set the error count variable to zero if there are faulty power supply been detected. This way, the known working power supply will have correct power supply detection to be operational. 🔒 Click for Additional Information
Case: 00498706 CRAOS8X-22539	**Summary:** TCP timestamp response (generic-tcp-timestamp) detected in Rapid7 tool. **Explanation:** The remote host responded with a TCP timestamp. The TCP timestamp response can be used to approximate the remote host's uptime, potentially aiding in further attacks. Fix is given with a CLI command:

	Ip tcp time-stamp-response admin-state disable 🔒 Click for Additional Information
Case: 00488102 00524014 CRAOS8X-21658	**Summary:** Switch rebooted with pmd file after configuring port mirroring in 6900. **Explanation:** Fix is given to avoid the invalid memory access when configuring the port mirroring. 🔒 Click for Additional Information
Case: 00495291 CRAOS8X-22279	**Summary:** In OS9900, ERROR: Destination Port Group matching not currently supported, when configuring policy condition with “destination port group” command. **Explanation:** CLI guide has been corrected to inform the policy command with “destination port group” is supported only in 6860, 6865 and 6900. This command is not supported for OS9900. 🔒 Click for Additional Information
Case: 00473154 CRAOS8X-20106	**Summary:** QOS qsi stats not shown as the documentation **Explanation:** The stats of the Queue 8 is show in Queue 1 instead, 8.R01 will have the fix of the CLI display to honor the documentation. 🔒 Click for Additional Information
Case: 00488780 CRAOS8X-21726	**Summary:** SPB services are down after changing SPB ISIS to point to multipoint access in one link. **Explanation:** Existent SPB nodes running AOS less than build 8.7.R01 were not able to process the new LSP capability and triggered an LSP database corruption. Fix code with multi access connection type; the device with different code behind the multi-access will not lose connection. 🔒 Click for Additional Information
Case: 00476405 CRAOS8X-20600	**Summary:** For a specific VRRP instance, the switch will prevent from configuring an advertisement interval of less than 100 centi-seconds with <ip vrrp 1 interface vlan10_ip interval 90> for instance. **Explanation:** VRRPv2 works with seconds but inputs through the commands are given in centi-seconds. Also, a value of less than 1 second should not be accepted. Since 100 centi-seconds equals to 1 second, a value of less than 100 centi-seconds should not be accepted. Code changes have been made such that a value less than 100 centi-seconds is not accepted. Both the software fix & document correction has been done. 🔒 Click for Additional Information
Case: 00493020	**Summary:** Fixed port speed is not working fine on Multigig port

CRAOS8X-22215	**Explanation:** Setting the port speed fixed to 2.5 not working. 🔒 Click for Additional Information
Case: 00521069 CRAOS8X-25570	**Summary:** BFD multiplier configuration syntax changed and disappears after reboot. **Explanation:** The issue is fixed in AOS 8.7.R02 GA. 🔒 Click for Additional Information
Case: 00478972 CRAOS8X-20695	**Summary:** No swlog messages are printed when SPB ISIS adjacency status changes **Explanation:** When SPB ISIS adjacency status changes to Down, UP or INIT, no swlog messages are printed in the swlog. 🔒 Click for Additional Information
Case: 00468800 CRAOS8X-19452	**Summary:** OS9900: Enabling qos qsi stats caused high CPU utilization and NI crash **Explanation:** Enabling qos qsi stats on all ports of the NI caused high CPU utilization and NI crash 🔒 Click for Additional Information
Case: 00423730 CRAOS8X-14475	**Summary:** The maximum convergence time listed in the specification guide is 50 milliseconds. **Explanation:** However, more than 50 millisecond convergence is noticed whenever there is a link flap in a multi-ring topology, with common RPL node for two or more sub-rings. 🔒 Click for Additional Information
Case: 00475778 CRAOS8X-20293	**Summary:** OS6560: Logging a policy rule causes the switch to crash **Explanation:** Switch crash happens when a switch is rebooted with policy rule which is logged 🔒 Click for Additional Information
Case: 00487374 CRAOS8X-21616	**Summary:** DDM Traps not generated when the port status changes **Explanation:** DM traps are not sent when the DDM enabled interfaces are toggled on the remote end. 🔒 Click for Additional Information

Case: 00488189 CRAOS8X-21688	**Summary:** OS6900: Unexpected reload of the slave chassis with kernel panic log messages **Explanation:** The slave chassis reloads unexpectedly with "Kernel panic - not syncing: Fatal exception in interrupt" log messages 🔒 Click for Additional Information
Case: 00492471 CRAOS8X-22041	**Summary:** Interface ddm configuration is not saved in vcboot.cfg **Explanation:** Interface DDM configuration is not saved in the config, unless an admin-state of an interface is enabled after configuring DDM. 🔒 Click for Additional Information
Case: 00493323 CRAOS8X-22103	**Summary:** Unable to delete "linkagg lacp port actore system-id" if set once via CLI **Explanation:** Unable to delete "linkagg lacp port actore system-id" if set once via CLI 🔒 Click for Additional Information
Case: 00497175 CRAOS8X-22376	**Summary:** 802.1X authentication fails after switch reload, when instead of IP address, DNS name of the RADIUS server is configured **Explanation:** 802.1X authentication is implemented. In the aaa configuration, instead of using the radius server IP address, the FQDN name (DNS name) is used 🔒 Click for Additional Information
Case: 00501797 CRAOS8X-22945	**Summary:** OS6900-V72/C32: Service local VRRP disable command not supported **Explanation:** OS6900-V72/C32 configured as BEB removes VLAN tag of all packets destined to VRRP mac before sending the packets out on SAP port. This results in connectivity issues. 🔒 Click for Additional Information

Case: 00503117 CRAOS8X-22976	**Summary:** Link failure on sub-ring causes ERP convergence on the ERP Master ring. **Explanation:** Whenever there is link failure in ERP sub-ring, ERP convergence is seen in sub-ring as well as in Master ring. These also leads to mac flusing on Master ring. 🔒 Click for Additional Information
Case: 00503881 CRAOS8X-23031	**Summary:** 6860N: UNP user loses connectivity with the error code "No SPB Resource" **Explanation:** 6860N-For-single-user-multiple-UNP-user-contexts-are-created-resulting-in-No-SPB-Resource 🔒 Click for Additional Information
Case: 00505704 CRAOS8X-23435	**Summary:** Remote access to OS6465 Loopback0 IP does not work when MAC and ARP entry for default gateway are flushed **Explanation:** Remote access using Loopback0 interface does not work when MAC entry and ARP entry of the default gateway are flushed in OS6465 🔒 Click for Additional Information
Case: 00506008 CRAOS8X-23431	**Summary:** OS6900-X72 back-to-front fan tray type part name **Explanation:** What is the correct part name for back-to-front fan trap type in OS6900-X72? 🔒 Click for Additional Information
Case: 00506895 CRAOS8X-23391	**Summary:** OS6860N: LLDP updates are not sent on UNP service ports **Explanation:** LLDP updates are not sent on UNP service ports. Due to this the IP Phones do not receive the VLAN advertisement from the switch. This results in connectivity issue as the IP Phones do not QTAG the packets with the expected VLAN. 🔒 Click for Additional Information

Case: 00510346 00513326 CRAOS8X-23875	**Summary:** 6860N-P48Z: No ingress traffic and mac-learning on switch ports **Explanation:** After a few days, after reload, there is no mac-learning on some switch ports in the range 1/1/1-36. Interface counters are not incrementing even though the link is UP. 🔒 Click for Additional Information
Case: 00510880 CRAOS8X-23911	**Summary:** OS6860N: Layer 2 multicast frames with TTL value of 1 are discarded **Explanation:** Multicast frames switches in the same VLAN are discarded if the TTL value of the multicast frames is set to 1. 🔒 Click for Additional Information
Case: 00480280 00523246 CRAOS8X-20814	**Summary:** 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: 00451258 CRAOS8X-17094	**Summary:** ## Internal PoE devices connected with 4-pin (2-pair) cabling are not powered on several ports of OS6560-P48Z16. **Explanation:** PoE devices connected with 4-pin (2-pair) cabling are not powered on several ports of OS6560-P48Z16. 🔒 Click for Additional Information
Case: 00487520 CRAOS8X-24485	**Summary:** Connecting an OS6860N-P48Z to an OS6900-X72 with ALE SFP-GIG-SX not working. **Explanation:** The support for 1G fiber SFP on 25G uplinks of 6860N would be available from AOS 8.7 R02 GA. 🔒 Click for Additional Information
Case: 00521282 CRAOS8X-26155	**Summary:** When changing the NTP configuration the VC is crashing **Explanation:** The problem happened when config an NTP server using the existing IP address, which is already used by a configured FQDN NTP server. 🔒 Click for Additional Information
Case: 00518917 CRAOS8X-25025	**Summary:** Show configuration snapshot not working for OS6865.

	Explanation: Saving the configuration with write memory command and show configuration snapshot not working. ->show tech-support Please wait... ERROR: System is busy. Please try later. (1007) Found the issue to be due to calling event log by enabling the command ->swlog advanced enable. Fix would be available from AOS 8.7 R02 GA. 🔒 Click for Additional Information
Case: 00511468 CRAOS8X-24411	**Summary:** DHCP clients connected on switch which is acting as DHCP relay agent not getting the Ip-address lease from DHCP server. **Explanation:** The DHCP discover packet from client was getting dropped by switch port as it was configured as QOS USER PORT using below command: ->qos user-port shutdown bpdu dhcp-server By default user-port filter is enabled and is considering DHCP discover packet as ip-spoof and filtering the same. Issue fix in AOS 8.7 R02 GA. 🔒 Click for Additional Information
Case: 00499137 CRAOS8X-22573	**Summary:** The traffic from Access switch for specific vlan tag is not getting leaned on BEB switch via SAP port. **Explanation:** At Hardware level the switch considered the respective vlan ID as untagged though it was configured as Tagged as per the switch configuration. 🔒 Click for Additional Information
Case: 00495957 CRAOS8X-22489	**Summary:** The ping from Access switch configured as DHL to the firewall not working. **Explanation:** The access switch OS6560 is configured as Dual home Linkagg with 2 uplinks as DHL link A and Link B with port B as blocking. Reason for ping not working was due to ARP moment happening in OS6560 as the ARP is getting moved to DHL-Blocking port. Issue has been fixed in AOS 8.7 R02 GA. 🔒 Click for Additional Information
Case: 00501948 CRAOS8X-22965	**Summary:** MAC addresses are not learnt on the switch ports of OS9900. **Explanation:** Due to continuous toggling of switch port at a very high rate caused the interruption handler of this ASIC to get frozen. The continuous toggling should be taken care by correcting the L1 issue. Fix is given to avoid the ASIC getting operational impact due to continuous port toggling and learn the MAC-addresses successfully after L1 issue is resolved. 🔒 Click for Additional Information

Case: 00523788 00498115 CRAOS8X-22474	**Summary:** OS6860E-P24Z8 switch running with firmware 8.7.354.R01 GA, throwing errors non stop: 2021 Jan 31 18:24:45.747 6860E swlogd zcNi main ERR: : [pmApiGetPortState:2411] PMInit Not Done **Explanation:.** "PMInit Not Done" error gets printed when PmApiInitDone variable is NULL/0. PmApiInitDone variable is responsible for logging the error message. Code changes are made to register port manager library from AOS 8.7.R02 GA. 🔒 Click for Additional Information
Case: 00476940 CRAOS8X-21061	**Summary:** unp redirect allowed-name server6 ip-address command throwing error while adding 6th Subnet as server. **Explanation:.** Maximum number of UNP allowed server was 5 in 8x until 8.6.R01. Since 8.6.R02, it is reduced to 1 due to the new feature additions and unavailability of underlying QOS rules. Currently only one server can be added to the configuration from AOS 8,7 R02 GA. 🔒 Click for Additional Information
Case: 00535145 CRAOS8X-26692	**Summary:** OS6860N running AOS 8.7R01 - cloud-agent is not starting when switch is booting with zero configuration. **Explanation:** Connect a OS6860N chassis out of the box (zero config) and uplink to network in oder to receive DHCP Lease with option 43 to get OV 2500 Activation Server's URL, if no option 43 switch will try to reach OV Cirrus Activation Server. Autofabric does not start discovery (cloud-agent) because did not receive message from Automatic Remote Config, cloud-agent remains stuck to Initial. 🔒 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 8.7R2. The package files are kept in the **flash/working/pkg** directory or can be downloaded from the Service & Support website.

Package	Package Description
MRP (mrp-8.7.R02-252.deb)	MRP Application
ams / ams-apps (ams-8.7.R02-252.deb/ams-apps-8.7R02-252.deb)	AOS Micro Services Application
OVSDB (aos-ovsdb-8.7.R02-252.deb)	OVSDB Application
- If a package is not committed it can result in image validation errors when trying to reload the switch. - Some packages are included as part of the AOS release and do not have to be installed separately. - File names will be prepended with platform specific prefixes.	

Installing Packages

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

```
-> pkgmgr verify nos-mrp-8.7.R02-252.deb
  Verifying MD5 checksum.. OK
-> pkgmgr install nos-mrp-8.7.R02-252.deb
-> write memory
-> show pkgmgr

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
  mrp           8.7.R02-252            installed          /flash/working/pkg/mrp/install.sh
```

Removing Packages

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

```
-> pkgmgr remove mrp
Purging mrp (8.7.R02-252)...
Removing package mrp.. OK
Write memory is required complete package mrp removal

-> write memory
Package(s) Committed

-> show pkgmgr
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
  mrp           8.7.R02-252           removed            /flash/working/pkg/mrp/install.sh
```

Remove the Debian package installation file. For example:

```
 -> rm /flash/working/pkg/nos-mrp-8.7.R02-252.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 or later release 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.
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 or later release 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.
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.