

Release Notes - Rev. A

OmniSwitch 6360, 6465, 6560, 6860(E),
6860N, 6865

Release 8.9R1

These release notes accompany release 8.9R1. 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 OS9900 and OS6900 platforms are currently not supported in AOS Release 8.9.73.R01.

(The OS9900 and OS6900 are referenced in the 8.9R1 documentation but are currently not supported platforms in AOS Release 8.9.73.R01.)

Contents

Contents 2

Related Documentation..... 3

System Requirements 4

[IMPORTANT] *MUST READ*: AOS Release 8.9R1 Prerequisites and Deployment Information 10

Licensed Features 14

ALE Secure Diversified Code..... 15

New / Updated Hardware Support and Guidelines 16

New Software Features and Enhancements 17

Open Problem Reports and Feature Exceptions 26

Hot-Swap/Redundancy Feature Guidelines 31

Technical Support..... 34

Appendix A: Feature Matrix 36

Appendix B: MACsec Platform Support 45

Appendix C: SPB L3 VPN-Lite Service-based (Inline Routing) / External Loopback Support / BVLAN Guidelines 46

Appendix D: General Upgrade Requirements and Best Practices 50

Appendix E: Standard Upgrade - OmniSwitch Standalone or Virtual Chassis 54

Appendix F: ISSU - OmniSwitch Chassis or Virtual Chassis 56

Appendix G: FPGA / U-boot Upgrade Procedure 59

Appendix H: CPLD Upgrade Procedure for ONIE-Based Devices 62

Appendix I: Fixed Problem Reports 63

Appendix J: Installing/Removing Packages 74

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-C32E	8GB	64GB
OS6900-X48C6/T48C6/X48C4E/T24C2/X24C2	8GB	32GB
OS6900-V48C8	16GB	32GB
OS9900	16GB	2GB

U-Boot and FPGA Requirements

The software versions listed below are the MINIMUM required, except where otherwise noted. Switches running the minimum versions, as listed below, do not require any U-Boot or FPGA upgrades but it's recommended to upgrade to the current version 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 8.9.73.R01 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6360-10	8.7.149.R02	8.7.30.R03 ²	0.11	0.11
OS6360-P10	8.7.149.R02	8.7.30.R03 ²	0.11	0.11

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6360-P10A (904324-90)	8.8.2.R03	8.8.2.R03	0.1	0.1
OS6360-24	8.7.149.R02	8.7.30.R03 ²	0.15	0.17 ¹
OS6360-P24	8.7.149.R02	8.7.30.R03 ²	0.15	0.17 ¹
OS6360-P24X	8.7.149.R02	8.7.30.R03 ²	0.12	0.12
OS6360-PH24	8.7.149.R02	8.7.30.R03 ²	0.12	0.12
OS6360-48	8.7.149.R02	8.7.30.R03 ²	0.15	0.17 ¹
OS6360-P48	8.7.149.R02	8.7.30.R03 ²	0.15	0.17 ¹
OS6360-P48X	8.7.149.R02	8.7.30.R03 ²	0.12	0.12
OS6360-PH48	8.8.114.R01	8.8.114.R01	0.12	0.12
1. FPGA version 0.17 is REQUIRED to address issues CRAOS8X-26370 and CRAOS8X-25033. 2. Optional uboot update for CRAOS8X-24464, ability to disable/authenticate uboot access.				

OmniSwitch 6465 - AOS Release 8.9.73.R01 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6465-P6	8.5.83.R01	8.7.2.R02 ² 8.7.30.R03 ³ 8.8.33.R01 ⁴	0.10	0.10
OS6465-P12	8.5.83.R01	8.7.2.R02 ² 8.7.30.R03 ³ 8.8.33.R01 ⁴	0.10	0.10
OS6465-P28	8.5.89.R02	8.7.2.R02 ² 8.7.30.R03 ³ 8.8.33.R01 ⁴	0.5	0.7 ¹
OS6465T-12	8.6.117.R01	8.7.2.R02 ² 8.7.30.R03 ³ 8.8.33.R01 ⁴	0.4	0.4
OS6465T-P12	8.6.117.R01	8.7.2.R02 ² 8.7.30.R03 ³ 8.8.33.R01 ⁴	0.4	0.4
OS6465-P12 (ENH-240)	8.8.33.R01	8.8.33.R01	0.5	0.5
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. 3. Optional uboot update for CRAOS8X-24464, ability to disable/authenticate uboot access. 4. Optional uboot update to support boot from USB feature.				

OmniSwitch 6560 - AOS Release 8.9.73.R01 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6560-24Z24	8.5.22.R01	8.7.2.R02 ³ 8.7.30.R03 ⁷	0.7	0.8 ⁵
OS6560-P24Z24	8.4.1.23.R02	8.7.2.R02 ³ 8.7.30.R03 ⁷	0.6	0.7 ¹ 0.8 ⁵
OS6560-24Z8	8.5.22.R01	8.7.2.R02 ³ 8.7.30.R03 ⁷	0.7	0.8 ⁵
OS6560-P24Z8	8.4.1.23.R02	8.7.2.R02 ³ 8.7.30.R03 ⁷	0.6	0.7 ¹ 0.8 ⁵
OS6560-24X4	8.5.89.R02	8.7.2.R02 ⁴ 8.7.30.R03 ⁷	0.4	0.4
OS6560-P24X4	8.5.89.R02	8.7.2.R02 ⁴ 8.7.30.R03 ⁷	0.4	0.4
OS6560-P48Z16 (903954-90)	8.4.1.23.R02	8.7.2.R02 ³ 8.7.30.R03 ⁷	0.6	0.7 ¹ 0.8 ⁵
OS6560-P48Z16 (all other PNs)	8.5.97.R04	8.7.2.R02 ³ 8.7.30.R03 ⁷	0.3	0.6 ² 0.7 ⁶
OS6560-48X4	8.5.97.R04	8.7.2.R02 ⁴ 8.7.30.R03 ⁷	0.4	0.7 ² 0.8 ⁶
OS6560-P48X4	8.5.97.R04	8.7.2.R02 ⁴ 8.7.30.R03 ⁷	0.4	0.7 ² 0.8 ⁶
OS6560-X10	8.5.97.R04	8.7.2.R02 ⁴ 8.7.30.R03 ⁷	0.5	0.8 ²
<ol style="list-style-type: none"> 1. FPGA version 0.7 is optional to address issue CRAOS8X-7207. 2. FPGA versions are optional to address issue CRAOS8X-16452. 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. 7. Optional uboot update for CRAOS8X-24464, ability to disable/authenticate uboot access. 				

OmniSwitch 6860(E) - AOS Release 8.9.73.R01 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6860/OS6860E (except U28/P24Z8)	8.1.1.70.R01	8.7.30.R03 ²	0.9	0.10 ¹
OS6860E-U28	8.1.1.70.R01	8.7.30.R03 ²	0.2	0.2
OS6860E-P24Z8	8.4.1.17.R01	8.7.30.R03 ²	0.5	0.7 ¹
<ol style="list-style-type: none"> 1. FPGA versions .7 and .10 are optional on the PoE models for the fast and perpetual PoE feature support. 2. Optional uboot update for CRAOS8X-24464, ability to disable/authenticate uboot access. 				

OmniSwitch 6860N - AOS Release 8.9.73.R01 (GA)

Hardware	Minimum ONIE	Current ONIE	Minimum CPLD	Current CPLD
OS6860N-U28	2019.05.00.10	2019.05.00.11	12	12
OS6860N-P48Z	2019.05.00.10	2019.05.00.11	12	13 ¹
OS6860N-P48M	2019.05.00.10	2019.05.00.11	11	12 ¹
O6860N-P24M	2019.05.00.11	2019.05.00.11	2	3 ¹
OS6860N-P24Z	2019.05.00.11	2019.05.00.11	2	3 ¹

1. Addresses CRAOS8X-29731/30471 - OS6860N power supply issue.

Note: These models use the **Uosn.img** image file.

OmniSwitch 6865 - AOS Release 8.9.73.R01 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6865-P16X	8.3.1.125.R01	8.7.2.R02 ² 8.7.30.R03 ³ 8.8.33.R01 ⁴	0.20	0.25 ¹
OS6865-U12X	8.4.1.17.R01	8.7.2.R02 ² 8.7.30.R03 ³ 8.8.33.R01 ⁴	0.23	0.25 ¹
OS6865-U28X	8.4.1.17.R01	8.7.2.R02 ² 8.7.30.R03 ³ 8.8.33.R01 ⁴	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.
3. Optional uboot update for CRAOS8X-24464, ability to disable/authenticate uboot access.
4. Optional uboot update to support boot from USB feature.

Note: CRAOS8X-4150 for the OS6865-U28X was fixed with FPGA version 0.12 and higher.

OmniSwitch 6900-X20/X40 - AOS Release 8.9.###.R01 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
CMM (if XNI-U12E support is not needed)	7.2.1.266.R02	8.7.30.R03 ¹	1.3.0/1.2.0	1.3.0/2.2.0
CMM (if XNI-U12E support is needed)	7.2.1.266.R02	8.7.30.R03 ¹	1.3.0/2.2.0	1.3.0/2.2.0

1. Optional uboot update for CRAOS8X-24464, ability to disable/authenticate uboot access.

OmniSwitch 6900-T20/T40 - AOS Release 8.9.###.R01 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
CMM (if XNI-U12E support is not needed)	7.3.2.134.R01	8.7.30.R03 ¹	1.4.0/0.0.0	1.6.0/0.0.0
CMM (if XNI-U12E support is needed)	7.3.2.134.R01	8.7.30.R03 ¹	1.6.0/0.0.0	1.6.0/0.0.0

1. Optional uboot update for CRAOS8X-24464, ability to disable/authenticate uboot access.

OmniSwitch 6900-Q32 - AOS Release 8.9.###.R01 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
CMM	7.3.4.277.R01	8.7.30.R03 ¹	0.1.8	0.1.8

1. Optional uboot update for CRAOS8X-24464, ability to disable/authenticate uboot access.

OmniSwitch 6900-X72 - AOS Release 8.9.###.R01 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
CMM	7.3.4.31.R02	8.6.189.R02 ¹ 8.7.30.R03 ²	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.
2. Optional uboot update for CRAOS8X-24464, ability to disable/authenticate uboot access.

OmniSwitch 6900-V72/C32/C32E/X48C6/T48C6/X48C4E/V48C8/T24C2/X24C2- AOS Release 8.9.###.R01 (GA)

Hardware	Minimum ONIE	Current ONIE	Minimum CPLD	Current CPLD
OS6900-V72	2017.08.00.01	2017.08.00.01	CPLD 1 - 5 CPLD 2 - 6 CPLD 3 - 8	CPLD 1 - 5 CPLD 2 - 6 CPLD 3 - 8
OS6900-C32	2016.08.00.03	2018.11.00.02	CPLD 1 - 10 CPLD 2 - 11 CPLD 3 - 11	CPLD 1 - 10 CPLD 2 - 11 CPLD 3 - 11
OS6900-C32E	2020.02.00.01	2020.02.00.01	CPLD 1 - 13 CPLD 2 - 9 CPLD 3 - 9	CPLD 1 - 13 CPLD 2 - 9 CPLD 3 - 9
OS6900-X48C6	2019.08.00.01	2019.08.00.01	CPLD 1 - 2 CPLD 2 - 2 CPLD 3 - 2 CPU CPLD - N/A	CPLD 1 - 3 CPLD 2 - 2 CPLD 3 - 2 CPU CPLD - 2.14 ¹
OS6900-T48C6	2019.08.00.01	2019.08.00.01	CPLD 1 - 2 CPLD 2 - 2 CPLD 3 - 4 CPU CPLD - N/A	CPLD 1 - 3 CPLD 2 - 2 CPLD 3 - 4 CPU CPLD - 2.14 ¹

Hardware	Minimum ONIE	Current ONIE	Minimum CPLD	Current CPLD
OS6900-X48C4E	2019.05.00.10	2019.05.00.10	CPLD 1 - 3 CPLD 2 - 2 CPLD 3 - 3 CPU CPLD - N/A	CPLD 1 - 3 CPLD 2 - 2 CPLD 3 - 3 CPU CPLD - 2.14 ¹
OS6900-V48C8	2020.02.00.01	2020.02.00.01	CPLD 1 - 2 CPLD 2 - 3 CPLD 3 - 2	CPLD 1 - 2 CPLD 2 - 3 CPLD 3 - 2
OS6900-T24C2	2019.08.00.03	2019.08.00.03	CPLD 1 - 2.0 CPLD 2 - 2.0 CPLD CPU - 6.0	CPLD 1 - 2.0 CPLD 2 - 2.0 CPLD CPU - 6.0
OS6900-X24C2	2019.08.00.03	2019.08.00.03	CPLD 1 - 6.0 CPLD 2 - 6.0 CPLD CPU - 6.0	CPLD 1 - 6.0 CPLD 2 - 6.0 CPLD CPU - 6.0
1. Optional CPU CPLD update to address CRAOS8X-30098.				
Note: These models use the Yos.img image file.				

OmniSwitch 9900 - AOS Release 8.9.###.R01 (GA)

Hardware	Minimum Coreboot-uboot	Current Coreboot-uboot	Minimum Control FPGA	Current Control FPGA	Minimum/Current Power FPGA
OS99-CMM	8.3.1.103.R01	8.3.1.103.R01 8.7.30.R03 ¹	2.3.0	2.3.0	0.8
OS9907-CFM	8.3.1.103.R01	8.3.1.103.R01	-	-	-
OS9907-CFM2	8.9.X	8.9.X	-	-	-
OS99-GNI-48	8.3.1.103.R01	8.3.1.103.R01 8.8.152.R01 ²	1.2.4	1.2.4 1.2.5 ²	0.9
OS99-GNI-P48	8.3.1.103.R01	8.3.1.103.R01 8.8.152.R01 ²	1.2.4	1.2.4 1.2.5 ²	0.9
OS99-XNI-48 (903753-90)	8.3.1.103.R01	8.3.1.103.R01 8.8.152.R01 ²	1.3.0	1.3.0 1.5.0 ²	0.6
OS99-XNI-48 (904049-90)	8.6.261.R01	8.6.261.R01 8.8.152.R01 ²	1.4.0	1.4.0 1.5.0 ²	0.7
OS99-XNI-U48 (903723-90)	8.3.1.103.R01	8.3.1.103.R01 8.8.152.R01 ²	2.9.0	2.9.0 2.11.0 ²	0.8
OS99-XNI-U48 (904047-90)	8.6.261.R01	8.6.261.R01 8.8.152.R01 ²	2.10.0	2.10.0 2.11.0 ²	0.8
OS99-GNI-U48	8.4.1.166.R01	8.4.1.166.R01 8.8.152.R01 ²	1.6.0	1.6.0 1.7.0 ²	0.2
OS99-CNI-U8	8.4.1.20.R03	8.4.1.20.R03 8.8.152.R01 ²	1.7	1.7 1.9 ²	N/A
OS99-XNI-P48Z16	8.4.1.20.R03	8.4.1.20.R03 8.8.152.R01 ²	1.4	1.4 1.6 ²	0.6

Hardware	Minimum Coreboot-uboot	Current Coreboot-uboot	Minimum Control FPGA	Current Control FPGA	Minimum/Current Power FPGA
OS99-XNI-U24	8.5.76.R04	8.6.261.R01 8.8.152.R01 ²	1.0	2.9.0 2.11.0 ²	0.8
OS99-XNI-P24Z8	8.5.76.R04	8.6.261.R01 8.8.152.R01 ²	1.1	1.4.0 1.6.0 ²	0.7
OS99-XNI-U12Q	8.6.117.R01	8.6.117.R01 8.8.152.R01 ²	1.5.0	1.5.0 1.6.0 ²	N/A
OS99-XNI-UP24Q2	8.6.117.R01	8.6.117.R01 8.8.152.R01 ²	1.5.0	1.5.0 1.6.0 ²	N/A

1. Optional uboot update for CRAOS8X-24464, ability to disable/authenticate uboot access.
2. Optional Uboot/FPGA update for future CMM2 and OS9912 compatibility.

[IMPORTANT] *MUST READ*: AOS Release 8.9R1 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 D](#) 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 (all other PNs) - 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 attacker¹. For this reason, we have disabled the "ssh-rsa" public key signature algorithm by default. 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.
- Beginning in August 2022 ALE will begin placing QR codes on physical products as well as the corrugated shipping boxes, the QR codes allow for additional information such as MAC addresses to be included. To allow time for customers and partners to adjust to the new barcodes there will be a 6 to 12 month transition period that will include both the QR code and the linear style barcodes. After the transition period ends only the QR codes will be included.

Deprecated Features / Functionality Changes

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

AOS Release 8.5R4
<p>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.</p>
<p>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:</p> <ul style="list-style-type: none"> - ntp server synchronized - ntp server unsynchronized
AOS Release 8.6R1
<p>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.</p>
<p>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.</p>
<p>SAA - The vlan-priority and drop-eligible parameters have been deprecated from all SAA commands beginning in 8.6R1.</p>
<p>MACsec is now supported on ports 33-48 of the 6560-(P)48X4. CRAOS8X-7910 was resolved in 8.6R1.</p>
AOS Release 8.6R2
<p>Distributed ARP - Beginning 8.6R2 distributed ARP is no longer supported.</p>
<p>WRED - Beginning in 8.6R2 WRED is no longer supported.</p>
<p>QoS - Beginning in 8.6R2 the 'qos dscp-table' command is no longer supported.</p>
<p>NTP - The ntp parameter for the 'ip service source-ip' command was deprecated in 8.5R4. Support has been added back in 8.6R2.</p>
AOS Release 8.7R1
<p>MACsec - Static mode is not supported on OS6860N.</p>
<p>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.</p>
<p>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 C for additional information.</p>
AOS Release 8.7R2
<p>There are new default user password polices being implemented in 8.7R2. This change does not affect existing users.</p> <ul style="list-style-type: none"> - cannot-contain-username: enable - min-uppercase: 1 - min-lowercase: 1 - min-digit: 1 - min-nonalpha: 1
<p>The OmniSwitch 6360 does not contain a real-time clock.</p> <ul style="list-style-type: none"> - 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.
AOS Release 8.7R3
<p>The Kerberos Snooping is not supported in bridge mode in this release.</p>

AOS Release 8.8R1
Unsupported commands (Part of AOS 88R1 but not supported) <ul style="list-style-type: none">- mrp interconnect- show mrp interconnect- clear mrp interconnect
<p>A software check was added in AOS releases 8.7R1, 8.7R2, and 8.7R3 restricting the use of the affected power supplies below while awaiting certification on the OS6560. This check was removed in 8.8R1 after the power supplies were certified resulting in the minimum AOS version 8.8R1 requirement.</p> <p>OS6560-BP-PH - This OS6560 600W power supply, OS6560-BP-PH (904072-90), requires a minimum AOS version of 8.8R1.</p> <p>OS6560-BP-PX - This OS6560 920W power supply, OS6560-BP-PX (904073-90), requires a minimum AOS version of 8.8R1.</p> <p>Refer to the OmniSwitch 6560 Hardware Guide for additional power supply information.</p>
AOS Release 8.8R2
The French language support is being removed from WebView to help reduce package size. If the default language is French it will default to English after upgrade.
AOS Release 8.9R1
Metro License Features - Some Metro features are now licensed on the OS6560 beginning in 8.9R1. See Metro License for information on re-enabling them after upgrading to 8.9R1.

Licensed Features

The table below lists the CAPEX 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: Supported on OS6900-X20/X40/T20/T40/Q32/X72 models.	

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
<p>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.</p> <p>2. Performance software license is optional allowing the 2 RJ45/SFP+ combo ports (25/26 or 49/50) of the OS6360-PH24 or OS6360-PH48 models to operate at 10G speed. Ports support 1G by default.</p> <p>3. MACsec is supported on the OS6900-X48C4E.</p>							

Metro License Required	
OmniSwitch 6560	
Licenses Features	
CPE Test Head	Yes
PPPoE-IA	Yes
Ethernet OAM	Yes
SAA	Yes
Link OAM	Yes
VLAN Stacking	Yes
DPA	Yes
Hardware Loopback	Yes
Note: Starting in 8.9R1 the following features require a Metro license.	

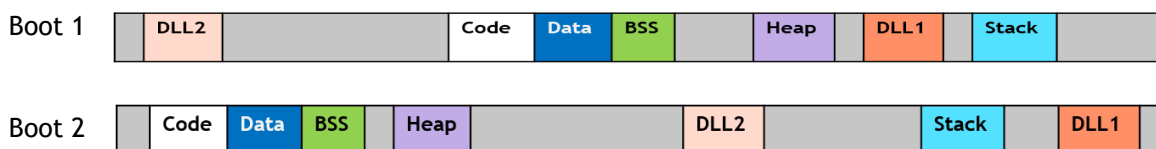
ALE Secure Diversified Code

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.



Please contact customer support for additional information.

New / Updated Hardware Support and Guidelines

The following new hardware is being introduced in this release.

OS6900-T24C2

Fixed configuration industrial chassis in a 1U form factor with:

- Twenty-four (24) - 10GBaseT (100M/1G/10G) ports.
- Two (2) - SFP+ (1G/10G) ports.
- Two (2) - QSFP28 (4X10G/40G/4X25G/100G) ports.
- Five (5) - Individual fan trays.
- Two (2) - Power supply bays

OS6900-X24C2

Fixed configuration industrial chassis in a 1U form factor with:

- Twenty-four (24) - SFP+ (1G/10G) ports.
- Two (2) - SFP+ (1G/10G) ports.
- Two (2) - QSFP28 (4X10G/40G/4X25G/100G) ports.
- Five (5) - Individual fan trays.
- Two (2) - Power supply bays

OS9907-CFM2

The OS9907-CFM2 is the second generation fabric card for the OS9907 chassis. This fabric card provides a high performance fabric plane for the OS9907 chassis and provides inter-module connectivity for the data traffic.

Please note the following requirements:

- The OS9907-CFM2 requires a minimum AOS version of 8.9R1.
- **AOS MUST be upgraded prior to inserting the OS9907-CFM2 into the chassis.**
- The OS9907-CFM2 cannot be mixed with the existing OS9907-CFM in the same chassis.

Transceivers

The following transceivers have been added in this release. Please refer to the Transceivers and Hardware guides for additional information.

- **SFP-10G-BX-D40** - SFP+ transceiver with an LC connector. This bi-directional transceiver is designed for use over single mode fiber up to ~40 km. Transmits 1330nm and receives 1270nm.
- **SFP-10G-BX-U40** - SFP+ transceiver with an LC connector. This bi-directional transceiver is designed for use over single mode fiber up to ~40 km. Transmits 1270nm and receives 1330nm.
- **SFP-25G-BX-D40** - SFP28 transceiver with an LC connector. This bi-directional transceiver is designed for use over single mode fiber up to ~40 km. Transmits 1310nm and receives 1270nm.
- **SFP-25G-BX-U40** - SFP28 transceiver with an LC connector. This bi-directional transceiver is designed for use over single mode fiber up to ~40 km. Transmits 1270nm and receives 1310nm.
- **QSFP-40G-PSM4** - QSFP+ transceiver with an MPO connector. Designed for use over single mode fiber up to ~10 km at 1310nm. Supports both 40G and 4X10G speeds.
- **QSFP-100G-C40CM** - QSFP28 direct attached copper 40cm cable.

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.

8.9R1 New Feature/Enhancements Summary

Feature	Platform
Management Features	
USB Ethernet Dongle	All (non-EMP models)
Metro License	6560
Security Admin Account	All (with MACsec support)
Advanced Ethernet Loopback	6465, 6560
Webview Support	All
NaaS Enhancement - Per Feature Grace Period	All
Naas Enhancement - Feature Parsing	All
Console Access Through any VC Member	All
Layer 2 Features	
Multiple Untagged Traffic on UNP	6860N, 6900-X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2
MRP Interconnect / Multi-NI	6465, 6865
Sflow on non-default VRF	6860, 6860N, 6900-X72, 6900-V72, 6900-X48C6/T48C6/ X48C4E/V48C8/C32E, 9900
Security Features	
MACsec MKA Based on Time or Data Amount	All (with MACsec support)
MACsec on Network Port for SPB/L2GRE/VxLAN	6860N, 6860E-P24/P24Z8, 6900-X48C4E
OpenSSL 3.0 Upgrade	All
Kerberos Enhancement	All
QoS Anti-spoofing - Service Domain	6860N, OmniSwitch 6900 X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2
Encrypted SSH and WebView Private Keys	All
Parity Features	
UDLD on OS6900-X48C4E	6900-X48C4E
Port Mirroring - Remote	6900-X48C4E
DHL	6900-X48C4E
PPPoE	6560
CPE Testhead	6560
Ethernet OAM	6560
EEE	6465,6560
Ethernet Services (VLAN Stacking)	6560
L2 GRE Tunnel Access (Edge) on Bridge Ports	6860N
L2 GRE Tunnel Access (Edge) on Access Ports	6860N
L2 GRE Tunnel Aggregation - 6860N Platforms	6860N
LTP (location/time policy) (services:VxLAN, L2GRE)	686X, 6900X, 9900

Feature	Platform
UNP user-role (services: VXLAN, L2GRE)	686X, 6900X, 9900
Specifications and Security Updates	
Routing Table Size Increase to 256	6360, 6465
GRE Scalability for Guest Tunneling	6860, 6860N, 6865, 6900
CVE related CRs Resolution	All

Management Features

USB Ethernet Dongle

This feature allows for a USB-to-Ethernet interface for switches that lack an EMP port. This interface is treated just like an EMP interface. All functions and CLIs related to EMP are applicable to the USB-to-Ethernet dongle. The following chipsets were validated: ASIX 8817 interface and RealTek RTL8153.

- USB 3.0 version dongles are supported on OS6360/6465/6560 models.
- USB 2.0 version dongles are supported on all models.
- Reinsertion of a dongle should be done with at least a 10 second delay.
- All the chassis of a VC should have a USB-to-Ethernet dongle for proper VC EMP functionality.

The following CLI commands are associated with this feature:

- **ip interface emp**

Metro License

Starting from 8.9R1, Metro license support is added on all OmniSwitch 6560 models. A perpetual Metro license would be required for enabling this functionality.

Following features are included in Metro license.

- CPE Test Head
- PPPoE-IA
- Ethernet OAM
- SAA
- Link OAM
- VLAN Stacking
- DPA
- Hardware Loopback

Note: When upgrading a switch to 8.9R1 that had Metro licensed features configured, those features will no longer work. To re-enable the Metro features after upgrading to 8.9R1 the Metro license must be installed and the Metro features reconfigured.

Security Admin Account

Only users with MACsec read-write privilege can configure MACsec. Use 'user' command to enable MACsec read-write permissions to the users. The privilege can be configured by family or by security domain.

The following CLI commands are associated with this feature:

- **user user password password read-write macsec**
- **user user password password read-write domain-security**

Advanced Ethernet Loopback

Starting from 8.9R1, Advanced Ethernet loopback test support is added to Omni Switch OS6560 model. AOS is now upgraded to support configuration of 36 hardware loopback test profiles. The switch support configuration of 28 inward and 8 outward test profiles on the switch port.

For OS6465, out of 36 test profiles, only 2 test profiles can be active at any given time.

Whereas, for OS6560 all the 36 test profiles can be active at any given time. For defining the outward loopback test profile, the VLAN ID parameter is made optional and SAP ID parameter is not required.

The following CLI commands are associated with this feature:

- **loopback-test**

Webview Support

As part of this release WebView support is added on the following platforms:

OS6900-X24C2, and OS6900-T24C2.

NaaS Enhancement - Per Feature Grace Period

The NaaS per-feature grace-period is enforced for AOS-NaaS-Management-license and AOS-NaaS-Upgrade-license. In a VC environment, If a switch is in NaaS mode but with no valid license for any one unit of the VC, NaaS will trigger grace period, when entering degrade state. Grace period assigned from the License Activation Server is enforced for AOS-NaaS-Management-license and AOS-NaaS- Upgrade-license.

The following CLI commands are associated with this feature:

- **No new CLI**

NaaS Enhancement - Feature Parsing

When parsing license from the license string, NaaS will not process any new features unregistered, but rather report to OVC/OVE through OV Cloud Agent. The OmniSwitch parses through the license file regardless of the new features that are in AOS and does not display any parsing errors. AOS does not interpret the features not recognized or applicable as AOS NaaS licenses. After parsing the license file it includes all features found in the license file as part of the OmniVista Call home to License Activation Server.

The following CLI commands are associated with this feature:

- **No new CLI**

Console Access Through any VC Member

This feature allows access to the console of any chassis in a VC using the secure shell protocol (SSH).

The following CLI command is associated with this feature:

- **ssh-chassis *username@chassis-id***

Layer 2 Features

Multiple Untagged Traffic on UNP

This feature allows classification of different untagged users to the same UNP dynamic untagged SAP, which can be associated to different services (like SPB, L2GRE, and VXLAN). The untagged SAP creation on different services is supported only for UNP dynamic SAPs. A new command to enable or disable multiple untagged MAC association is added.

The following CLI commands are associated with this feature:

- **unp multi-untag-sap**
- **no unp multi-untag-sap**

MRP Interconnect / Multi-NI

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. MRP is designed to react deterministically on a single failure of an inter-switch link or switch in the ring or interconnection topology.

To redundantly connect two MRP rings, two nodes of each ring are assigned additional roles. One of the nodes has the role of a media redundancy interconnection manager (MIM), in addition to the role of a MRC or MRM. The function of the MIM is to observe and to control the redundant interconnection topology in order to react on interconnection faults. To cover a maximum of applications, two detection methods are provided by this international standard..

The following CLI commands are associated with this feature:

- **mrp interconnect**
- **show mrp interconnect**
- **clear mrp interconnect**

Sflow on non-default VRF

SFLOW can now be configured on non-default VRF. The OmniSwitch allows configuration of non-default VRF on SFLOW receiver, sampler, and poller.

The following CLI commands are associated with this feature:

- **vrf [name] sflow receiver**
- **vrf [name] show sflow receiver**
- **vrf [name] sflow sampler**
- **vrf [name] sflow poller**
- **vrf [name] show sflow sampler**
- **vrf [name] show sflow poller**
- **[vrf vrf_name] ip service source-ip sflow**

Security Related Features

MACsec MKA Based on Time or Data Amount

Session-time and Exchange-data configurations are supported to trigger the MKA protocol key-rotation for MACsec Dynamic in this release:

- Session-Time (in min) for SAK (Secure Association Key) regeneration - A timer for each MACsec interface will be created for triggering key-rotation when the configured max-session-time is reached.
- Exchange-Data (received or transmitted) between the MACsec endpoints. Key rotation happens when the exchanged data exceeds the configured max-exchange-data.

The following CLI commands are associated with this feature:

- **interfaces macsec key-rotation max-session-time**
- **interfaces macsec key-rotation max-exchange-data**
- **show interfaces macsec dynamic key-rotation**

MACsec on Network Port for SPB/L2GRE/VxLAN

MACsec is supported between two directly connected Service Access Ports or network ports for service type SPB/VXLAN/L2GRE to provide MACsec security on the tunneled traffic.

This is supported only on OmniSwitch 6900-X48C4E, OmniSwitch 6860N, OmniSwitch 6860E-P24, and OmniSwitch 6860E-P24Z8 platforms.

OpenSSL 3.0 Upgrade

AOS now supports OpenSSL 3.0 which further improves the AOS security compatibility. OpenSSL 3.0 offers:

- Modern Ciphers which aids the security certifications.

- FIPS 140-2 compliant.
- Support to all the FIPS Automated Cryptographic Algorithm Testing Requirements.
- Apache 2.0 license.
- Key Derivation Functions support.

Kerberos Enhancement

Due to the difference in the Kerberos packet sequence the Kerberos user authentication was failing. To overcome the difference in packet sequence, the action for Kerberos packets is changed to TRAP and DROP from TRAP and ACCEPT.

Platform	Port-Type			
	Bridge	Access		
		SPB	L2GRE	VXLAN
OS6860	Yes	No	No	No
OS6865	Yes	No	No	No
OS6900	Yes	No	No	No
OS6560	Yes	No	No	No
OS6465	Yes	No	No	No
OS6360	Yes	No	No	No
OS6860N	Yes	Yes	No	No
6900- X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/	Yes	Yes	No	No
OS9900	Yes	Yes	Yes	No

QoS Anti-spoofing Support

QoS Anti-Spoofing is currently supported across AOS platforms on VLAN domain. In this release, Anti-spoofing support is extended over service domain as well. Anti-spoofing on service is supported only on SPB SAP ports and is supported on OmniSwitch 6860N and OmniSwitch 6900 X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2 where inline routing is supported.

Encrypted SSH and WebView Private Keys

On Upgrade to 8.9R1:

When the switch is upgraded to 8.9.R1 (reload or ISSU) for the first time the encrypted SSH and WebView private keys will be generated on first upgrade. Once the keys are generated on the first upgrade, they need not be generated for the consecutive upgrades.

On Downgrade from 8.9R1:

The encrypted SSH and WebView private keys will not work on pre-89R01. When the switch is downgraded to any other pre-89R01 release the switch verifies the downgrade case on reload (command) and the encrypted SSH and WebView private keys are deleted automatically. The unencrypted private key files are generated on boot up with the pre-89R01 image.

If manual deletion is required for any reason the following private keys can be deleted:

- /flash/switch/web/default_WebViewCert.pem
- /flash/system/ssh_host_dsa_key
- /flash/system/ssh_host_rsa_key
- /flash/system/ssh_host_ecdsa_key
- /flash/system/ssh_host_ecdsa384_key

- /flash/system/ssh_host_ecdsa521_key

Parity Features

UDLD

This feature is now supported on OS6900-X48C4E models.

Port Mirroring - Remote

This feature is now supported on OS6900-X48C4E models.

DHL

This feature is now supported on OS6900-X48C4E models.

PPPoE

This feature is now supported on OS6560 models.

CPE Testhead

This feature is now supported on OS6560 models.

Ethernet OAM

This feature is now supported on OS6560 models.

EEE

This feature is now supported on OS6465 and OS6560 models.

Ethernet Services (VLAN Stacking)

This feature is now supported on OS6560 models.

L2 GRE Tunnel Access (Edge) on Bridge Ports

This feature is now supported on OS6860N models.

L2 GRE Tunnel Access (Edge) on Access Ports

This feature is now supported on OS6860N models.

L2 GRE Tunnel Aggregation

This feature is now supported on OS6860N models.

LTP (location/time policy) (services:VxLAN, L2GRE)

This feature is now supported on 6860x, 6900x, 9900 models.

UNP user-role (services: VXLAN, L2GRE)

This feature is now supported on 6860x, 6900x, 9900 models

Specifications and Security Updates

Routing Table Size Increase to 256

- Maximum IPv4 static routes for the OS6360 and OS6465 is increased from 32 to 256 in this release.
- Maximum IPv6 static routes for the OS6360 and OS6465 is increased from 4 to 32 in this release.

GRE Scalability for Guest Tunneling

The following L2 GRE Tunnel Aggregation scalability improvements are supported in this release.

- OS6860 - 2K
- OS6860N - 2K
- OS6865-2K
- OS6900-V72/C32/X48C6/T48C6/X48C4E/V48C8/C32E - 8K

CVE related CRs resolution

The following CRs were fixed in this release to address CVE related issues.

CR	Description
CRAOS8X-16576	CERT-IST/AV-2020.0121 Vulnerability in "sudo" on Linux/Unix (CVSS 7.8)
CRAOS8X-22210	openssl: Raccoon security vulnerability (CVSS 4.8)
CRAOS8X-22282	libxml2 security vulnerabilities after 2.9.10 (CVSS 5.0)
CRAOS8X-22394	Busybox: CERT Security Vulnerabilities (CVSS: 7.5 [8.1 US])
CRAOS8X-26419	openssh: Security vulnerability in 8.4 (CVSS 7.5)
CRAOS8X-29678	Python - IST Security Advisory after 3.9.4 (CVSS 7.8)
CRAOS8X-29679	curl: security vulnerabilities (CVSS: 7.3)
CRAOS8X-31643	ncurses: Security vulnerabilities (CVSS: 6.3 Medium)
CRAOS8X-31644	vsftpd: security vulnerabilities (CVSS: 7.4 High)
CRAOS8X-31646	Sqlite: security vulnerabilities / CERTs (CVSS 5.3 low)
CRAOS8X-31668	lighttpd: CERT-IST security vulnerability (CVSS 7.5)
CRAOS8X-31937	Expat: security vulnerabilities after 2.4.2 (CVSS 7.3)
CRAOS8X-32120	jquery: Security Vulnerability CVE-2020-7656 (CVSS 6.1 NIS)
CRAOS8X-33273	openssl: security vulnerabilities CVE-2022-1292, CVE-2022-1343, CVE-2022-1434, CVE-2022-1473 (CVSS:9.8 for group)

CRAOS8X-34306	opensst: CVE-2022-2097 and CVE-2022-2274 (CVSS:9.8 - medium for AOS)
---------------	----------------------------------------------------------------------

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-33705	Double tagged packets with size less than 64 bytes received as encapsulated inside a tunneled packet (eg: SPB encapsulated), are prone to get dropped at network port on OS6900-X24C2/T24C2.	There is no known workaround at this time.
CRAOS8X-34477	PMD gets generated for the bash process while configuring "qos apply" or "qos reset port" command.	There is no known workaround at this time. There's no functional impact, the command can be entered again.
CRAOS8X-35151	After configuring "ip name-server", while performing domain lookup a PMD gets generated for the "nslookup" command.	There is no known workaround at this time. There is no functional impact.
CRAOS8X-32460	Host Agent messages not found in syslog even after retrying for 15 seconds after NI reset.	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-23137	When high number of VLANs are mapped to DHL links then during failover traffic loss may be seen due to delay in hardware programming.	There is no known workaround at this time.
CRAOS8X-28757	Telnet traffic when going through spb network does not match DPI signatures.	There is no known workaround at this time.
CRAOS8X-27368	On an OS9900 when linkagg port is admin disabled, fdb flush is issued for that particular port which is resulting in flushing MACs on other fixed port which is unrelated to the linkagg.	There is no known workaround at this time.
CRAOS8X-10059	Toggling admin state of bulk of VLANs (disable/enable) very quickly may cause VPA state of the VLANs to be incorrectly stuck in blocking state (instead of forwarding).	Allow few seconds in between toggling admin state (disable/enable) of bulk of VLANs.
CRAOS8X-30045	High convergence is seen when a linkagg is disabled. Root cause of the issue is that linkagg disable is applied slower causing mac-move to be triggered first compared to mac-flush. This issue is seen only when linkagg is disabled through CLI, if individual links of the linkagg are down then convergence is proper.	Admin link-down individual ports of the linkagg instead of linkagg disable.

Hardware / Transceivers

CR	Description	Workaround
CRAOS8X-31402	On an OS6900-X48C6/T48C6, port 52 or 53 (100G-DAC) flaps while trying to bring 100G optical link on the neighbor port 52 or 53 respectively. This behavior is observed regardless of uplink or VFL link on port 52 or 53.	To avoid this link flap, it is recommended to use only 100G DACs OR 100G optical transceivers on both ports 52 and 53.
CRAOS8X-35257	OS6900-X24C2/T24C2: While configuring a feature using port range command, recommend to split the configuration to use the range only for non-splitter capable ports.	For splitter capable ports, use the port based command only instead of the port range.
CRAOS8X-30583	SFP-10G-T transceiver will not link up if the remote link partner is working at 1G speed except on OS6900-X48C6/V48C8/X48C4E and 6860N-25G ports. SFP-10G-T transceiver is supported only when paired at 10G speed on all 8.X platforms.	Enable 1G speed on the switch side (if the switch supports it).
CRAOS8X-32089	Traffic Loss seen above 8 Gbps speed on the XS-010S-Q,XGS PON ONT, 1x10GE transceiver (3FE49327AA).	There is no known workaround at this time.
CRAOS8X-32090	Untagged traffic is not forwarded on a tagged port configured on ISAM side.	There is no known workaround at this time.
CRAOS8X-34219	With CFM2 and XNI-U48 board, port recovery after violation takes additional 2 mins with WTR of 15 seconds.	There is no known workaround at this time.

QoS

PR	Description	Workaround
CRAOS8X-4424	With color-only policy action configured, egress queue is not honoring the color marking and packets drops are observed and expected traffic rate is not achieved.	There is no known workaround at this time.
CRAOS8X-10498	Configuring maximum ingress bandwidth (i.e. 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>'.
CRAOS8X-33587	On an OS9900, ingress bandwidth ratelimiting fails when ratelimiting is configured with more than 32G for a 40G port.	There is no known workaround at this time.
CRAOS8X-32278	Egress traffic distribution between linkagg members will only work on a per physical port basis. Traffic on different linkagg members would be distributed based on hashing of the traffic.	It is recommended to ensure load balancing first and validate distribution on linkagg members.

	<pre> #Configure a linkagg linkagg lacp agg 2 size 4 linkagg lacp agg 2 actor admin-key 4 linkagg lacp agg 2 admin-state ENABLE linkagg lacp port 1/1/2 actor admin-key 4 #Configure a vlan for the linkagg vlan 31 vlan 31 members linkagg 2 tagged #Configure a IP interface ip interface v31 address 31.100.200.1/24 vlan 31 eth2 #Configure the VFC mixed profile over the linkagg qos qsp 6 import qsp 1 qos qsp 6 qp 1 weight 15 scheduler wrr qos qsp 6 qp 2 scheduler wrr qos qsp 6 qp 3 scheduler sp qos qsp 6 qp 4 scheduler wrr qos qsp 6 qp 5 scheduler wrr qos qsp 6 qp 6 scheduler wrr qos qsp 6 qp 7 scheduler wrr qos qsp 6 qp 8 weight 4 scheduler wrr #Apply the VFC mixed profile to the linkagg qos apply qos qsi linkagg 2 qsp 6 #Enable statistic on the profile qos qsi linkagg 2 stats admin-state enable #Check the profile information show qos qsi linkagg 2 summary show qos qsi linkagg 2 </pre>	
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

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-33243	On OS6900-Q32/X72 platform, The maximum limit of VFI field in L2 table in Broadcom chipset is 4096, so only 4096 (4k) services are supported on these platform.	There is no known workaround at this time.

Virtual Chassis

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

Layer 2 / Multicast

PR	Description	Workaround
CRAOS8X-7428	IPMS Proxy is not supported on a service.	There is no known workaround at this time.
CRAOS8X-26502	While converging due to a link/node failure in a MRP ring network, sometimes a few multicast IGMP clients are not relearned with a large number of multicast streams (>200). Clients will be relearned after the next query interval.	There is no known workaround at this time.
CRAOS8X-29130	Multicast traffic drop seen on OS9900 when ‘hash-control load-balance non-unicast’ is enabled	There is no known workaround at this time.

Layer 3

PR	Description	Workaround
CRAOS8X-33472	<p>When BGP peering sessions operate over an IPv6 TCP connection between two OS9900s running AOS 8.9.R01, it has been observed that there could be intermittent flapping of BGP session due to loss of TCP synchronization between the BGP routers. An error log could be observed as follows:</p> <p><Timestamp> : bgp_0 tcp ERR message:</p> <p><Timestamp> OS9900 vrfId 0: [<peer description>,<AS>] Bad marker rcvd! Aborting peer session.</p> <p>The BGP peering session will get re-established, with no manual intervention necessary and the routing table will be restored.</p> <p>This behavior/symptom has not been observed on BGP peering sessions between OS9900 and OS6900/OS6860N switches running AOS 8.9.R01.</p>	There is no known workaround at this time.

	<p>This behavior/symptom is isolated to IPv6 BGP peer sessions and has not been observed on IPv4 BGP sessions.</p> <p>Impact of behavior:</p> <p>BGP IPv6 peering session toggles and restores with above error log output. This could result in temporary network route convergence. Switch logs will attempt to capture the loss of synchronization, if possible.</p>	
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

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

ALE technical support is committed to resolving our customer’s technical issues in a timely manner. Customers with inquiries should contact us at:

Country	Supported Language	Toll Free Number
France, Belgium, Luxembourg	French	+800-00200100
Germany, Austria, Switzerland	German	
United Kingdom, Italy, Australia, Denmark, Ireland, Netherlands, South Africa, Norway, Poland, Sweden, Czech Republic, Estonia, Finland, Greece, Slovakia, Portugal	English	
Spain	Spanish	
India	English	+1 800 102 3277
Singapore	English	+65 6812 1700
Hong-Kong	English	+852 2104 8999
South Korea	English	+822 519 9170
Australia	English	+61 2 83 06 51 51
USA	English	+1 800 995 2696
Your questions answered in English, French, German or Spanish.	English French German Spanish	+1 650 385 2193 +1 650 385 2196 +1 650 385 2197 +1 650 385 2198
Fax: +33(0)3 69 20 85 85 Email: ebg_global_supportcenter@al-enterprise.com Web : myportal.al-enterprise.com		

Internet: Customers with service agreements may open cases 24 hours a day via the support web page. 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+ with exceptions &	: /flash/foss/gpl-3.0.txt + /flash/foss/gpl-2.0.txt +
		GPLv2+ with exceptions & LGPLv2+ & BSD	/flash/foss/lgpl-2.1.txt + /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. © Copyright 2022 ALE International, ALE USA Inc. All rights reserved in all countries.

Appendix A: Feature Matrix

The following is a feature matrix for AOS Release 8.9R1.

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/X48C4E/V48C8/C32E T24C2/X24C2	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	8.6R1
Automatic Remote Configuration Download (RCL)	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.6R2	8.7R1	Y
Automatic/Intelligent Fabric	8.7R2	8.5R1	Y	Y	8.7R2	Y	Y	Y	Y	Y
Automatic VC	8.7R2	N	Y	Y	8.7R1	Y	Y	8.6R2	8.7R1	N
Bluetooth - USB Adapter with Bluetooth Technology	8.7R2	8.6R2	8.6R2	Y	8.7R1	8.6R2	8.7R1	8.6R2	N	N
Console Disable	8.7R2	8.6R2	8.6R2	8.6R2	8.7R1	8.6R2	8.6R2	8.6R2	8.7R1	8.6R2
Dying Gasp	N	Y	Y	Y	8.7R1	Y	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
EEE support	Y	8.9R1	8.9R1	Y	8.7R1	Y	Y	Y	Y	Y
Embedded Python Scripting / Event Manager	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.7R2	8.7R2	N
IP Managed Services	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Hitless Security Patch Upgrade	8.7R2	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1
In-Band Management over SPB	N	N	N	8.5R4	8.7R1	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4
ISSU	8.7R2	Y	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
NaaS	8.8R1	8.8R1	8.8R1	8.8R1	8.8R1	8.8R1	8.8R1	8.8R1	8.8R1	8.8R1
NAPALM Support	8.7R2	8.5R1	8.5R1	8.5R1	8.7R1	8.5R1	8.5R1	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	8.5R4
NTP - IPv6	8.7R3	8.7R3	8.7R3	8.7R3	8.7R3	8.7R3	8.7R3	8.7R3	8.7R3	8.7R3
OpenFlow	N	N	N	Y	N	N	Y	N	N	N
OV Cirrus - Zero touch provisioning	8.7R2	Y	Y	Y	8.7R1	Y	Y	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	8.5R4
OV Cirrus - Default Admin Password Change	8.7R2	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4

Feature	6360	6465	6560	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
OV Cirrus - Managed	8.7R2	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4
OVSDB	N	N	N	N	N	N	8.7R1 (X72/Q32)	8.7R1	N	N
Package Manager	8.7R2	8.6R2	8.6R2	8.6R2	8.7R1	8.6R2	8.6R2	8.6R2	8.7R1	8.6R2
Readable Event Log	8.7R2	8.6R1	8.6R1	8.6R1	8.7R1	8.6R1	8.6R1	8.6R1	8.7R1	8.6R1
Remote Chassis Detection (RCD)	N	N	N	8.6R2	8.7R1	N	Y	N	8.7R1	Y
SAA	8.7R2	8.5R1	8.9R1 Metro	Y	8.7R2	Y	Y	8.7R1	8.7R1	Y
SAA SPB	N	N	N	Y	8.7R2	Y	Y	8.7R1	8.7R1	8.6R2
SAA UNP	N	Y	N	Y	N	Y	Y	N	N	N
SNMP v1/v2/v3	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Thin Client	8.8R1	8.8R1	8.8R1	8.8R1	8.8R1	8.8R1	8.8R1	8.8R1	8.8R1	8.8R1
Uboot Enable/Disable/Authenticate	8.7R3	8.7R3	8.7R3	8.7R3	N	8.7R3	8.7R3	N	N	8.7R3
UDLD	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	N	X48C4E	EA
USB Disaster Recovery	8.7R2	8.5R1	Y	Y	8.7R1 (onie)	Y	Y	8.7R1 (onie)	8.7R1 (onie)	Y
USB Flash (AOS)	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	N	N	N
Virtual Chassis (VC)	8.7R2	8.5R2	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1 (except X48C4E model)	Y
Virtual Chassis Split Protection (VCSP)	8.7R2	Y	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
VRF	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
VRF - IPv6	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
VRF - DHCP Client	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Web Services & CLI Scripting	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.7R1	8.7R1	Y
Layer 3 Feature Support										
ARP	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
BFD	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
BGP	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
DHCP Client / Server	8.7R2	8.6R1	Y	Y	8.7R1	Y	Y	8.5R4	8.7R1	Y

Feature	6360	6465	6560	6860(E)	6860N	6865	6900	6900- V72/ C32	6900- X48C6/ T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
DHCP Relay	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R4	8.7R1	Y
DHCPv6 Server	N	N	N	Y	8.7R1	Y	Y	8.7R1	8.7R1	Y
DHCPv6 Relay	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.7R1	8.7R1	Y
DHCP Snooping / IP Source Filtering	8.7R2	8.5R4	Y	Y	8.7R1	Y	Y	8.6R2	8.7R1	Y
ECMP	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
IGMP v1/v2/v3	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
GRE	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.5R2
IP-IP tunneling	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.5R2
IPv6	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
IPv6 - DHCPv6 Snooping	8.7R2	8.6R1	8.6R1	8.5R3	8.7R1	8.5R4	N	8.6R2	8.7R1	8.7R1
IPv6 - Source filtering	8.7R2	N	8.6R1	8.5R3	8.7R1	8.5R4	N	8.6R2	8.7R1	8.7R1
IPv6 - DHCP Guard	EA	EA	EA	EA	N	EA	N	N	N	N
IPv6 - DHCP Client Guard	EA	EA	EA	EA	N	EA	N	N	N	N
IPv6 - RA Guard (RA filter)	N	N	8.5R2	Y	8.7R1	Y	Y	N	N	N
IPv6 - DHCP relay and Neighbor discovery proxy	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	N	N	Y
IP Multinetting	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
IPSec (IPv6)	N	N	N	Y	8.7R1	Y	Y	Y	Y	Y
ISIS IPv4/IPv6	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.5R2
M-ISIS	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.5R2
OSPFv2	N	N	8.5R2 ¹	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
OSPFv3	N	N	8.8R1 ¹	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
RIP v1/v2	N	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
RIPng	N	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
UDP Relay (IPv4)	8.7R2	8.5R4	8.5R4	Y	8.7R1	Y	Y	8.5R4	8.7R1	8.5R4
UDP Relay (IPv6)	8.7R2	8.6R1	8.6R1	8.6R1	8.7R1	8.6R	8.6R1	8.6R1	8.7R1	8.6R1

Feature	6360	6465	6560	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
VRRP v2	8.7R2	8.5R2	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
VRRP v3	8.7R2	8.5R2	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Server Load Balancing (SLB)	N	N	N	Y	N	Y	Y	N	N	N
Static routing	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Multicast Features										
DVMRP	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	N
IPv4 Multicast Switching	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Multicast *,G	8.7R2	Y	8.5R2	8.5R2	8.7R1	Y	Y	8.5R2	8.7R1	Y
IPv6 Multicast Switching	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
PIM-DM	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
PIM-SM	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
PIM-SSM	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
PIM-SSM Static Map	N	N	N	N	N	N	N	N	N	N
PIM-BiDir	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
PIM Message Packing	N	N	N	8.6R1	8.7R1	N	8.6R1	8.6R1	8.7R1	N
PIM - Anycast RP	N	N	N	8.6R2	8.7R1	8.6R2	8.6R2	8.6R2	8.7R1	8.6R2
Monitoring/Troubleshooting Features										
Ping and traceroute	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Policy based mirroring	N	N	N	Y	8.7R1	Y	Y	8.7R1	8.7R1	8.5R4
Port mirroring	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Port monitoring	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Port mirroring - remote	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.7R2	8.7R2	8.6R1
Port mirroring - remote over linkagg	N	N	N	Y	8.7R1	Y	Y	8.7R2	8.7R2	8.6R1
RMON	8.7R2	8.5R1	Y	Y	8.8R2	Y	Y	8.8R2	8.8R2	N

Feature	6360	6465	6560	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
SFlow	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.7R1	8.7R1	Y
Switch logging / Syslog	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
TDR	N	N	N	Y	N	Y	N	N	N	N
Layer 2 Feature Support										
802.1q	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
DHL	8.7R2	8.5R1	Y	Y	8.7R1	Y	N	N	X48C4E	N
ERP v2	N	8.5R1	8.5R2	Y	8.7R1	Y	Y	8.7R1	8.7R1	8.5R3
HAVLAN	N	EA	N	Y	8.8R1	Y	Y	8.6R2	8.7R1	EA
Link Aggregation (static and LACP)	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
LLDP (802.1ab)	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Loopback detection - Edge (Bridge)	8.7R2	8.5R1	Y	Y	8.7R1	Y	N	8.6R2	8.7R1	Y
Loopback detection - SAP (Access)	N	N	N	Y	8.7R1	Y	Y	8.6R2	8.7R1	Y
MAC Forced Forwarding / Dynamic Proxy ARP	8.7R2	8.7R1	N	8.6R1	N	8.6R1	N	N	N	N
MRP	N	8.7R2	N	N	N	8.7R2	N	N	N	N
Port mapping	8.7R2	Y	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	N
Private VLANs (PVLAN)	N	N	N	Y	8.7R2	Y	Y	N	8.7R2	N
SIP Snooping	N	N	N	Y	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	Y
Spanning Tree (PVST+, Loop Guard)	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
MVRP	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R4	8.7R1	Y
SPB ²	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
SPB - Over Shared Ethernet	N	N	N	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1
SPB - HW-based LSP flooding	N	N	N	N	N	N	N	N	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	Y
IPv4	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y

Feature	6360	6465	6560	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
IPv6	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Auto-Qos prioritization of NMS/IP Phone Traffic	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Auto-Qos - New MAC range	8.7R2	8.5R2	8.5R2	8.5R2	8.7R1	8.5R2	8.5R2	8.5R2	8.7R1	8.5R2
Groups - Port	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Groups - MAC	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Groups - Network	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Groups - Service	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Groups - Map	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Groups - Switch	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Ingress/Egress bandwidth limit	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Per port rate limiting	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	N
Policy Lists	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.7R1	8.7R1	Y
Policy Lists - Egress	N	N	N	Y	8.7R1	Y	Y	8.7R1	8.7R1	N
Policy based routing	N	N	N	Y	8.7R1	Y	Y	8.6R2	8.7R1	EA
Tri-color marking	N	N	N	Y	8.7R1	Y	Y	N	N	N
QSP Profiles 1	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
QSP Profiles 2/3/4	N	N	N	Y	QSP-2 only	Y	Y	QSP-2 only	QSP-2 only	N
QSP Profiles 5	8.7R2	8.5R1	Y	8.7R1	8.7R1	8.7R1	8.7R1 (X72)	N	N	Y
RoCEv2	N	N	N	N	N	N	N	8.7R2	N	N
Custom QSP Profiles	8.7R2	Y	Y	Y	Y	Y	X72 only (EA)	Y	Y	Y
GOOSE Messaging Prioritization	N	8.7R1	N	N	N	8.7R1	N	N	N	N
Metro Ethernet Features										
CPE Test Head	N	8.6R1	8.9R1 Metro	N	N	N	N	N	N	N
Ethernet Loopback Test	N	N	8.9R1 Metro	8.6R1	8.7R1	8.6R1	N	N	N	N

Feature	6360	6465	6560	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
Ethernet Services (VLAN Stacking)	N	8.5R1	8.9R1 Metro	Y	8.7R2	Y	Y	8.5R4	8.7R1	N
Ethernet OAM (ITU Y1731 and 802.1ag)	N	8.5R1	8.9R1 Metro	Y	8.7R1	Y	Y	8.7R1	8.7R1	EA
EFM OAM / Link OAM (802.3ah)	N	8.6R1	8.9R1 Metro	8.5R4	8.7R2	8.5R4	N	N	N	N
PPPoE Intermediate Agent	N	8.6R1	8.9R1 Metro	N	N	8.6R1	N	N	N	N
1588v2 End-to-End Transparent Clock	N	8.5R1	8.7R2	Y	N	Y	Y (X72/Q32)	N	N	N
1588v2 Peer-to-Peer Transparent Clock	N	8.8R2	8.7R2	N	N	N	N	N	N	N
1588v2 Across VC	N	N	N	N	N	N	8.5R2 (X72)	N	N	N
Access Guardian / Security Features										
802.1x Authentication	8.7R2	8.5R2	Y	Y	8.7R1	Y	Y	8.7R1	8.7R1	Y
Access Guardian - Bridge	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.6R1	8.7R1	Y
Access Guardian - Access	N	N	N	Y	8.7R1	Y	Y	8.5R4	8.7R1	Y
Application Fingerprinting	N	N	N	N	N	N	Y	N	N	N
Application Monitoring and Enforcement (Appmon)	N	N	N	Y	8.7R2	N	N	N	N	N
ARP Poisoning Protection	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
BYOD - COA Extension support for RADIUS	8.7R2	Y	Y	Y	8.7R1	Y	8.62	8.6R2	8.7R1	Y
BYOD - mDNS Snooping/Relay	8.7R2	Y	Y	Y	8.7R1	Y	8.62	8.6R2	8.7R1	Y
BYOD - UPNP/DLNA Relay	8.7R2	Y	Y	Y	8.7R1	Y	8.62	8.6R2	8.7R1	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	Y
Captive Portal	8.7R2	8.5R4	Y	Y	8.7R1	Y	8.62	8.6R2	8.7R1	Y
IoT Device Profiling	8.7R2	8.5R2	8.5R2	8.5R2	8.7R1	8.5R2	8.5R2	8.6R1	8.7R1	8.5R2
IoT Device Profiling (IPv6)	8.7R2	8.7R1	8.7R1	8.7R1	N	8.7R1	8.7R1	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	Y
Interface Violation Recovery	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.7R1	8.7R1	Y
Kerberos Snooping (services)	8.7R2	Y	8.6R2	8.6R2	Y	8.6R2	8.6R2	8.6R2	Y	8.6R2

Feature	6360	6465	6560	6860(E)	6860N	6865	6900	6900- V72/ C32	6900- X48C6/ T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
L2 GRE Tunnel Access (Edge) (bridge ports)	N	N	Y	Y	8.9R1	Y	8.6R1 ³	N	N	Y
L2 GRE Tunnel Access (Edge) (access ports)	N	N	N	8.6R1	8.9R1	8.6R1	8.6R1	8.7R1	8.7R2	8.6R1
L2 GRE Tunnel Aggregation	N	N	N	Y	8.9R1	Y	Y ³	8.7R1	8.7R2	Y
Learned Port Security (LPS)	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R4	8.7R1	Y
MACsec ⁴	N	8.5R1	8.5R4	Y	8.7R1	N	N	N	X48C4E	8.5R2
MACsec MKA Support ⁴	N	8.5R2	8.5R4	8.5R2	8.7R1	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
RADIUS - RFC-2868 Support	8.7R2	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4
Role-based Authentication for Routed Domains	N	N	N	8.5R4	8.7R1	8.5R4	8.5R4	8.6R1	8.7R1	8.5R4
Storm Control (flood-limit)	8.7R2	Y	Y	Y	8.7R1	Y	Y	Y	8.7R1	Y
Storm Control (Unknown unicast with action trap/shutdown)	N	N	N	Y	N	Y	Y	N	N	N
TACACS+ Client	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.6R1	8.7R1	Y
TACACS+ command based authorization	8.7R2	N	N	Y	8.7R1	Y	Y	8.7R2	8.7R2	N
TACACS+ - IPv6	8.7R3	8.7R3	8.7R3	8.7R3	8.7R3	8.7R3	8.7R3	8.7R3	8.7R3	8.7R3
PoE Features										
802.3af and 802.3at	8.7R2	8.5R1	Y	Y	8.7R1	Y	N	N	N	Y
802.3bt	8.7R2	Y	8.6R2	N	8.7R1	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	Y
Display of detected power class	8.7R2	8.5R1	Y	Y	8.7R1	Y	N	N	N	Y
LLDP/802.3at power management TLV	8.7R2	8.5R1	Y	Y	8.7R1	Y	N	N	N	Y
HPOE support	8.7R2 (95W)	8.5R1 (60W)	Y (95W)	Y (60W)	8.7R1 (95W)	Y (75W)	N	N	N	Y (75W)
Time Of Day Support	8.7R2	8.5R1	Y	Y		Y	N	N	N	Y
Perpetual PoE	8.7R2	N	N	Y	Y	Y	N	N	N	N
Fast PoE	8.7R2	N	N	Y	Y	Y	N	N	N	N
Data Center Features (License May Be Required)										
CEE DCBX Version 1.01	N	N	N	N	N	N	Y	N	N	N

Feature	6360	6465	6560	6860(E)	6860N	6865	6900	6900- V72/ C32	6900- X48C6/ T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
Data Center Bridging (DCBX/ETS/PFC)	N	N	N	N	N	N	Y	N	N	N
EVB	N	N	N	N	N	N	N	N	N	N
FCoE / FC Gateway	N	N	N	N	N	N	Y	N	N	N
VXLAN ⁵	N	N	N	N	8.8R1	N	Q32/X72	8.5R3	8.8R1	N
VM/VXLAN Snooping	N	N	N	N	N	N	Y	N	N	N
FIP Snooping	N	N	N	N	N	N	Y	N	N	N
Notes: 1. OS6560 supports stub area only. 2. See protocol support table in Appendix C. 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: MACsec Platform Support

The following table lists the platforms and modules that support the MACsec functionality.

MACsec Support (MACsec site license required)	
OmniSwitch 9900	
OS99-CMM	4X10G mode only (Static mode only)
OS99-GNI-48/P48	10M/100M/1G ports
OS99-XNI-48/P48	10G ports (Static mode only)
OS99-XNI-U48	10G ports (Static mode only)
OS99-XNI-P48Z16	1G/2.5G/5G/10G (16x) 1G/10G (32x)
OS99-GNI-U48	1G ports
OS99-XNI-U24	10G ports (Static mode only)
OS99-XNI-P24Z8	1G/2.5G/5G/10G (8x) 1G/10G (16x)
OS99-XNI-U12Q	10G / 4x10G Uplink (Static mode only)
OS99-XNI-UP24Q2	10G(Fiber)/4x10G Uplink (Static mode only) 10G (Copper) (Static mode only)
OS99-CNI-U8	Not Supported
OmniSwitch 6900	
OS6900-X48C4E	Dynamic mode only on all ports. Supports 256-bit key length.
OmniSwitch 6860(E)	
OS6860(E)	All models support MACsec on 10G ports.
OS6860E-P24	1G/10G ports.
OS6860E-P24Z8	1G/10G ports (not supported on 2.5G ports).
OmniSwitch 6860N	
OS6860N-U28	SFP (1-24), SFP+ (25-28) and SFP28 (31-34) ports
OS6860N-P48Z	SFP28 (51-54) ports
OS6860N-P48M	- Expansion modules (Not supported on any 4X10G splitter transceivers). - Multi-rate Gigabit Ports (37-48)
OS6860N-P24Z	SFP28 (27-30) ports
OS6860N-P24M	- Expansion modules (Not supported on any 4X10G splitter transceivers) - Multi-rate Gigabit Ports (1-24)
OmniSwitch 6560	
OS6560-P24X4/24X4	- Ports 1-24 (Static and Dynamic modes) - Ports 25-30 (Not Supported)
OS6560-P48X4/48X4	- Ports 1-48 (Static and Dynamic modes) - Ports 49-52 (Dynamic mode only) - Ports 53-54 (Not Supported)
OS6560-P48Z16 (904044-90 only)	- Ports 1-32 (Static and Dynamic Modes) - Ports 33-48 (Static and Dynamic modes) - Ports 49-52 (Dynamic mode only) - Ports 53-54 (Not Supported)
OS6560-X10	- Ports 1-8 (10G ports only. Dynamic mode only) - Ports 9-10 (Not Supported)
OmniSwitch 6465	
	- OS6465-P28 - supported on all ports except ports 27 and 28. - OS6465T-12 and OS6465T-P12 - Not supported on ports 11 and 12. - All other models support MACsec on all ports.

Appendix C: 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 6900-X48C4E/V48C8	OmniSwitch 6900-C32E	OmniSwitch 6860N	OmniSwitch 6900-X/T24C2
IPv4 Protocols							
Static Routing	Y	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
RIP v1/v2	Y	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
OSPF	Y	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
BGP	Y	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
VRRP	Y	8.7R1	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
IS-IS	N	N	N	N	N	N	N
PIM-SM/DM	8.5R3	8.6R2	Y	Y	8.8R1	Y	8.9R1
DHCP Relay	8.5R3	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
UDP Relay	8.5R4	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
DVMRP	N	N	N	N	N	N	N
BFD	8.7R2	8.7R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
IGMP Snooping	Y	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
IP Multicast Headend Mode	Y	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
IP Multicast Tandem Mode	8.5R4	8.6R2	8.8R1	8.8R1	8.8R1	8.8R1	8.9R1
IPv6 Protocols							
Static Routing	8.5R4	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
RIPng	8.5R4	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
OSPFv3	8.5R4	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
BGP	8.5R4	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
VRRPv3	8.5R4	8.7R1	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
IS-IS	N	N	N	N	N	N	N
PIM-SM/DM	8.5R4	8.6R2	8.8R1	8.8R1	8.8R1	8.8R1	8.9R1
DHCP Relay	8.6R1	8.7R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
UDP Relay	8.6R1	8.7R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
BFD	8.7R2	8.7R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
IPv6 MLD Snooping	Y	8.7R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
IPv6 Multicast Headend Mode	Y	8.7R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
IPv6 Multicast	8.5R4	8.7R2	8.8R1	8.8R1	8.8R1	8.8R1	8.9R1

Tandem Mode							
----------------	--	--	--	--	--	--	--

External Loopback Support									
	OmniSwitch 9900	OmniSwitch 6860/6865	OmniSwitch 6860N	OmniSwitch 6900	OmniSwitch 6900-V72/ C32	OmniSwitch 6900-X48C6/ T48C6	OmniSwitch 6900-X48C4E	OmniSwitch 6900-V48C8	OmniSwitch 6900- X/T48C2
IPv4 Protocols									
Static Routing	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
RIP v1/v2	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
OSPF	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
BGP	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
VRRP	8.6R1	8.5R4	8.7R1	Y	8.7R1	8.7R2	8.7R2	8.7R3	8.9R1
IS-IS	Y	Y	Y	Y	Y	Y	8.7R2	8.7R3	8.9R1
PIM-SM/DM	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
DHCP Relay	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
UDP Relay	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
DVMRP	N	N	N	N	N	N	N	N	N
BFD	Y	Y	Y	Y	Y	Y	8.7R2	8.7R3	8.9R1
IGMP Snooping	8.5R4	Y	8.7R1	Y	8.6R1	8.7R1	8.7R2	8.7R3	8.9R1
IP Multicast Headend Mode	8.5R4	Y	8.7R1	Y	8.6R1	8.7R1	8.7R2	8.7R3	8.9R1
IP Multicast Tandem Mode	8.5R4	Y	8.7R1	Y	8.6R1	Y	Y	Y	8.9R1
IPv6 Protocols									
Static Routing	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
RIPng	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
OSPFv3	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
BGP	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
VRRPv3	8.5R4	8.5R4	8.7R1	Y	8.7R1	8.7R2	8.7R2	8.7R3	8.9R1
IS-IS	Y	Y	Y	Y	Y	Y	8.7R2	8.7R3	8.9R1
PIM-SM/DM	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
DHCP Relay	8.6R1	8.6R1	8.7R1	8.6R1	8.6R1	8.7R1	8.7R2	8.7R3	8.9R1
UDP Relay	8.6R1	8.6R1	8.7R1	8.6R1	8.6R1	8.7R1	8.7R2	8.7R3	8.9R1
BFD	Y	Y	Y	Y	Y	Y	8.7R2	8.7R3	8.9R1
IPv6 MLD Snooping	8.5R4	Y	8.7R1	Y	Y	8.7R2	8.7R2	8.7R3	8.9R1
IPv6 Multicast Headend Mode	8.5R4	Y	8.7R1	Y	Y	8.7R2	8.7R2	8.7R3	8.9R1
IPv6 Multicast Tandem Mode	8.5R4	Y	8.7R1	Y	Y	Y	Y	Y	8.9R1

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:
```

```

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 D: 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 chassis-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 8.9R1 (GA)
OS6360	8.8.56.R02 (Minor GA) 8.8.152.R01 (Major GA) 8.7.98.R03 (Minor GA) 8.7.252.R02 (Major GA)
OS6360-P10A	8.8.8.R03 (Minor GA) - Note: Uses same image file as other OS6360 platforms.
OS6465	8.8.56.R02 (Minor GA) 8.8.152.R01 (Major GA) 8.7.98.R03 (Minor GA) 8.7.252.R02 (Major GA)
OS6560	8.8.56.R02 (Minor GA) 8.8.152.R01 (Major GA) 8.7.98.R03 (Minor GA) 8.7.252.R02 (Major GA)
OS6860(E)	8.8.56.R02 (Minor GA) 8.8.152.R01 (Major GA) 8.7.98.R03 (Minor GA) 8.7.252.R02 (Major GA)
OS6860N*	8.8.56.R02 (Minor GA) 8.8.153.R01 (Major GA)
OS6865	8.8.56.R02 (Minor GA) 8.8.152.R01 (Major GA) 8.7.98.R03 (Minor GA) 8.7.252.R02 (Major GA)
OS6900	8.8.56.R02 (Minor GA) 8.8.152.R01 (Major GA) 8.7.98.R03 (Minor GA) 8.7.252.R02 (Major GA)
OS6900-V72/C32/ X48C6/T48C6/X48C4E/V48C8*	8.8.56.R02 (Minor GA) 8.8.153.R01 (Major GA) 8.8.152.R01 (Major GA)
OS9900	8.8.56.R02 (Minor GA) 8.8.152.R01 (Major GA) 8.7.98.R03 (Minor GA) 8.7.252.R02 (Major GA)
*ISSU is not supported to 8.9.R01 from any release prior to an 8.8.R01 build. This is due to improvements made by transitioning from software on chip (SoC) to software development kit (SDK) APIs that were implemented in 8.8.R01. ISSU functionality will be supported for all future releases from 8.8R1 and above.	

8.9R1 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 E](#) for specific steps to follow.
- If upgrading a VC using ISSU please refer to [Appendix F](#) for specific steps to follow.

Appendix E: 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:

- OS6360 - Nosa.img
 - Refer to [Appendix G](#) for recommended/required FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6465 - Nos.img
 - Refer to [Appendix G](#) for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6560 - Nos.img
 - Refer to [Appendix G](#) for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6860 - Uos.img
 - Refer to [Appendix G](#) for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6860N - Uosn.img
 - Refer to [Appendix H](#) for recommended CPLD upgrades. AOS must be upgraded prior to upgrading the CPLD/U-boot.
- OS6865 - Uos.img
 - Refer to [Appendix G](#) for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6900 - Tos.img
 - Refer to [Appendix G](#) for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6900-V72/C32 - Yos.img.
- OS6900-X48C6/T48C6/X48C4E/V48C8 - Yos.img.
- OS9900 - Mos.img, Mhost.img, Meni.img
- imgsha256sum (not required) -This file is only required when running in Common Criteria mode. Please refer to the Common Criteria Operational Guidance Document for additional information.

2. FTP the Upgrade Files to the Switch

FTP the image files to the *Running* directory of the switch you are upgrading. The image files and directory will differ depending on your switch and configuration.

3. Upgrade the image file

Follow the steps below to upgrade the image files by reloading the switch from the *Running* directory.

```
OS6900-> reload from working no rollback-timeout
Confirm Activate (Y/N) : y
This operation will verify and copy images before reloading.
It may take several minutes to complete....
```

If upgrading a VC the new image file will be copied to all the Slave chassis and the entire VC will reboot. After approximately 5-20 minutes the VC will become operational.

4. Verify the Software Upgrade

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

```
OS6900-> show microcode
/flash/working
Package           Release           Size           Description
-----+-----+-----+-----
Tos.img           8.9.73.R01       239607692     Alcatel-Lucent OS
```

```
6900-> show running-directory
CONFIGURATION STATUS
Running CMM           : MASTER-PRIMARY,
CMM Mode              : VIRTUAL-CHASSIS MONO CMM,
Current CMM Slot      : CHASSIS-1 A,
Running configuration : WORKING,
Certify/Restore Status : CERTIFY NEEDED
SYNCHRONIZATION STATUS
Running Configuration : SYNCHRONIZED
```

Note: If there are any issues after upgrading the switch can be rolled back to the previous certified version by issuing the **reload from certified no rollback-timeout** command.

5. Certify the Software Upgrade

After verifying the software and that the network is stable, use the following commands to certify the new software by copying the *Running* directory to the Certified directory.

```
OS6900-> copy running certified

-> show running-directory
CONFIGURATION STATUS
Running CMM           : MASTER-PRIMARY,
CMM Mode              : VIRTUAL-CHASSIS MONO CMM,
Current CMM Slot      : CHASSIS-1 A,
Running configuration : WORKING,
Certify/Restore Status : CERTIFIED
SYNCHRONIZATION STATUS
Running Configuration : SYNCHRONIZED
```

Appendix F: 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:

- OS6360 - Nosa.img
 - Refer to [Appendix G](#) for recommended/required FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6465 - Nos.img
 - Refer to [Appendix G](#) for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6560 - Nos.img
 - Refer to [Appendix G](#) for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6860 - Uos.img
 - Refer to [Appendix G](#) for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6860N - Uosn.img
 - Refer to [Appendix H](#) for recommended CPLD upgrades. AOS must be upgraded prior to upgrading the CPLD/U-boot.
- OS6865 - Uos.img
 - Refer to [Appendix G](#) for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6900 - Tos.img
 - Refer to [Appendix G](#) for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6900-V72/C32 - 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
Chas  Role           Status           Chas ID  Pri   Oper  MAC-Address      System
-----+-----+-----+-----+-----+-----+-----+-----
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           8.8.56.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 G: 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	OS6465(T), 6560-24X4/P24X4/48X4/P48X4/X10
CRAOS8X-13819	Description	Uboot unable to mount eUSB flash
	U-boot Version	8.7.2.R02
	Platforms	OS6560-24Z24/P24Z24/24Z8/P24Z8/P48Z16 (all PNs), 6865
CRAOS8X-22857	Description	OS6560-P24Z24 reloads continuously with pmuds
	FPGA Version	0.8
	Platforms	OS6560-24Z24/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
8.7R3 Release		
CRAOS8X-26370 CRAOS8X-25033	Description	Required upgrade to enable 12V Power Fail Interrupt (CRAOS8X-26370). Required upgrade to address fan speed issue. (CRAOS8X-25033)
	FPGA Version	0.17
	Platforms	OS6360-24/P24/48/P48
CRAOS8X-24464	Description	Uboot update for CRAOS8X-24464, ability to disable / authenticate uboot access.
	Uboot Version	8.7.30.R03
	Platforms	OS6360, 6465, 6560, 6860, 6865, 6900, 9900. (Not applicable for platforms that use ONIE)
8.8R1 Release		
Boot from USB	Description	Uboot update to allow switch to boot from USB.
	Uboot Version	8.8.33.R01
	Platforms	OS6465, OS6865
8.8R2 Release		
Future compatibility	Description	Uboot/FPGA update to allow future CMM2/OS9912 NI compatibility.
	Uboot/FPGA Versions	See OS9900 Table for versions.
	Platforms	9907
8.9R1 Release		
N/A	There are no Uboot/FPGA upgrade requirements in this release.	

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_7715
- U-boot.8.8.R01.152.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_7715
Parse /flash/fpga_kit_7715
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.8.8.R02.15.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 H: CPLD Upgrade Procedure for ONIE-Based Devices

The following CRs or features can be addressed by performing a CPLD upgrade on the respective models.

CR / Feature	Summary	
8.8R2 Release		
CRAOS8X-29731/30471	Description	OS6860N power supplies
	CPLD Version	os6860n_p48m_p48z_u28_maincpu_20220318.updater os6860n_p24m_p24z_maincpld_22020309.updater
	Platforms	OS6860N-P48M/P48Z/P24M/P24Z
CRAOS8X-30098	Description	ismt_smbus 0000:00:12.0: completion wait timed out (Please refer to CRAOS8X-30098 for additional details)
	CPU CPLD Version	denverton_cpucpld_v0b.02.0eh_20211124.jbc.updater
	Platforms	OS6900-X48C6/T48C6/X48C4E
Notes: <ol style="list-style-type: none"> Upgrading the CPLD on ONIE-based models is only supported beginning with AOS Release 8.8.R02 and when using the AOS command procedure. Any other procedure to upgrade the CPLD may damage the switch and void the warranty. CPLD versions are compatible with previous AOS releases. Downgrading to a previous AOS release is supported: <ol style="list-style-type: none"> Backup the configuration files from previous release. Upgrade to AOS Release 8.8.R02. Upgrade the CPLD. Downgrade to previous release. (ISSU is not supported when downgrading AOS) Restore the configuration. 		

Note: AOS must be upgraded prior to performing a CPLD upgrade.

1. Download and extract the upgrade archive from the Service & Support website. In addition to the AOS images, the archive will also contain a CPLD upgrade file, for example.

- CPLD File - *.updater

2. FTP (Binary) the files to the /flash directory on the primary CMM.






3. Enter the following to upgrade the CPLD. The 'all' parameter is currently not supported, each element in a VC must be upgraded individually, for example:







```
-> update fpga-cpld cmm 1/1 file os6860n_p24m_p24z_maincpld_20220309.updater
Starting CMM 1/1  FPGA Upgrade
CMM 1/1
starting onie update
Removing firmware update results: os6860n_p24m_p24z_maincpld_20220309.updater
Staging firmware update: /flash/os6860n_p24m_p24z_maincpld_20220309.updater
onie update successful
Successfully updated
Reload required to activate new firmware.
```





4. Once complete, a reboot is required.








Appendix I: Fixed Problem Reports








The following problem reports were closed in this release.







CR/PR NUMBER	Description
Case: 00628581 CRAOS8X-34396	Summary: Switch losing the complete Access port and Service configuration upon reload. Explanation: The switch was configured with many UNP access ports and services that were created mapping to these access ports. Though the write memory and copy working certified actions performed well, upon reload of the switch, the mentioned configuration was getting lost completely. The fix is available in 8.9R1  Click for Additional Information
Case: 00630520 CRAOS8X-34275	Summary: How to configure Temp threshold in 8.x switches. Explanation: None of the 8.x code platform switches would be allowed to configure the temperature threshold values, hence, in the switch there is no CLI command to change the same. The HW guide documentation would be corrected from AOS 8.9 R01 GA.  Click for Additional Information
Case: 00622489 CRAOS8X-33709	Summary: Port flaps on OS99-CNI-U8 only when using ATOP QSFP-100G-CWDM4. Explanation: The observed issue is only with the combination of OS99-CNI-U8 with ATOP QSFP manufacturer model. Any other ALE certified vendor SPFs (Source Photonics) used will not showcase the port flap issue. The observed issue is identified as a bug in AOS and fix will be available from AOS 8.9 R01 GA.  Click for Additional Information
Case: 00616320 CRAOS8X-33140	Summary: Cannot configure interface flood limiting on linkagg member port. Explanation: Upon trying to configure rate limiting on ports parts of linkagg is not allow with below error: WARNING: Cannot configure Flood-limit on Linkagg member port 1/1/x  Click for Additional Information
Case: 00619345 CRAOS8X-33293	Summary: ASA Bitmap feature is missing from AOS 8.8 R01 microcode versions. Explanation: The Upon authentication, the user need to be assigned with privileges weather to READ or READ/WRITE. To obtain the privilege for all the families, administrator can find them under Bitmap Calculator via the WEBGUI access of switch. However, it is not available now. Fix will be available from AOS 8.9 R01 GA.  Click for Additional Information
Case: 00620991 CRAOS8X-34028	Summary: Loopback detection mechanism not working when the linkagg is configured as service access. Explanation: Due to human error, the links part of same linkagg which is configured as Service access have been connected back to back in a loop. The LBD was enabled however, the scenario






	<p>has created a loop in the network. Fix to block the port via LBD will be available in AOS 8.9 R01 GA.</p> <p> Click for Additional Information</p>
<p>Case: 00614846 CRAOS8X-33038</p>	<p>Summary: SnmpEngineBoots not getting updated upon switch reboot.</p> <p>Explanation: Switch was configured with SNMPv3. On a cold reboot (powering off and on) of the equipment, the "SnmpEngineBoots" value under ->show snmp statistics does not increment the number of restarts. The observed issue has been fixed to make the "SnmpEngineBoots" value to increment with both Cold and Warm boot of the switch. The fix will be available from AOS 8.9 R01 GA.</p> <p> Click for Additional Information</p>
<p>Case: 00609624 CRAOS8X-32675</p>	<p>Summary: The configured Policy under DHCP-Snooping are not getting saved.</p> <p>Explanation: The configured Policy under DHCP-Snooping is not getting saved. After configuring policy KEEP and saving the configuration, on reboot the policy REPLACE is present. Fix will be available under AOS 8.9 R01 GA.</p> <p> Click for Additional Information</p>
<p>Case: 00628116 CRAOS8X-34397</p>	<p>Summary: OS6860N: Radius Change of Authorization (CoA) does not work on UNP Service ports.</p> <p>Explanation: For Change of Authorization (CoA) functionality, ""redirect-port-bounce"" parameter needs to be added on the UNP port. In 88R02 and previous releases, the parameter cannot be added on a port-template if the port-template is mapped to the UNP service port.</p> <p> Click for Additional Information</p>
<p>Case: 00623344 CRAOS8X-34016</p>	<p>Summary: OS6900-V48C8: VXLAN traffic received on SAP port is discarded if the DST UDP Port is 4789.</p> <p>Explanation: The VXLAN traffic is received on OS6900-V48C8, however, the traffic is discarded. It is observed that the OS6900-V48C8 receives traffic on the SAP port, however, it is not forwarded to other SAP ports or to the SPB ports. The behavior is only seen if the destination UDP port of the VXLAN traffic 4789.</p> <p> Click for Additional Information</p>
<p>Case: 00624283 CRAOS8X-33981</p>	<p>Summary: 2xOS6900-C32: Upon link toggle, the Virtual Chassis generates TCAM error logs and then freezes.</p> <p>Explanation: Upon link toggle, the Virtual Chassis generates TCAM error logs and then freezes. During the issue state, modifying the QoS configuration causes the Virtual Chassis to reload.</p> <p> Click for Additional Information</p>






<p>Case: 00621753 CRAOS8X-33630</p>	<p>Summary: OS6900-X40: eBGP adjacency flaps with BGP notification message CEASE.</p> <p>Explanation: BGP adjacency flaps with the error message that incoming BGP prefixes is exceeding the maximum-prefixes limit", however the actual number of incoming BGP prefixes are lower than the configured maximum-prefixes.</p> <p>Click for Additional Information</p>
<p>Case: 00621139 CRAOS8X-33632</p>	<p>Summary: OS6860E: LPF - Link fault propagation does not work when one source ports include a combination of linkagg and non-linkagg ports.</p> <p>Explanation: Link Fault Propagation feature is expected to shutdown destination port/s, only if all source ports go DOWN. However, if the source ports include a combination of linkagg and non linkagg ports, then the feature does not work as expected.</p> <p> Click for Additional Information</p>
<p>Case: 00612515 CRAOS8X-32752</p>	<p>Summary: OS6860N-U28: After ERP toggle, the slave chassis becomes unresponsive. OS680N VC splits due to IP multicast flood unknown enabled.</p> <p>Explanation: The issue is observed due to OS680N VC split due to IP Multicast Flooding Unknown Enabled'. The issue would be seen only under below conditions: Traffic flow should be multicast, across VC via VFL. IP Multicast Flood-unknown command should be enabled. The switch model should be OS6860N alone.</p> <p> Click for Additional Information</p>
<p>Case: 00604477 CRAOS8X-32199</p>	<p>Summary: Switch generates OSPF Network LSA for the Down interfaces</p> <p>Explanation: If an OSPF node receives a network LSA (LSA type 2), and if the receiving node has an interface with the same IP address as the LSID of the receiving Network LSA, the receiving node generates a new network LSA. This happens even if the OPSF interface on the receiving node is DOWN. This results in LSA ping pong effect.</p> <p> Click for Additional Information</p>
<p>Case: 00605648 00636460 CRAOS8X-32310</p>	<p>Summary: OS6360-P10 interface does not come UP when it is connected to OS6900-X48C6 using the SFP GBIC-SX.</p> <p>Explanation: When connecting OS6360-P10 model switch to the OS6900- X48C6 model switch, the interface of the OS6360 switch does not coming up. However, the OS6900 switch interface is up.</p> <p> Click for Additional Information</p>
<p>Case: 00604980 CRAOS8X-26697</p>	<p>Summary: OS6860E-24: After link flap, the OSPF adjacency gets stuck in EXSTART/EXCH state.</p> <p>Explanation:</p>







	<p>After OSPF adjacency flap, OSPF routes are properly updated in the software but not in hardware. This results in loss of connectivity.</p> <p> Click for Additional Information</p>
<p>Case: 00634369 CRAOS8X-34920</p>	<p>Summary: OS6900-V72: SPB configuration is lost after AOS upgrade from release 8.7.252.R02 to 8.8.153.R01.</p> <p>Explanation: The SPB configuration on virtual chassis 2xOS6900-V72 is lost after the AOS upgrade from release 8.7.252.R02 to release 8.8.153.R01.</p> <p> Click for Additional Information</p>
<p>Case: 00627437 CRAOS8X-33962</p>	<p>Summary: MAC sec port unable to receive with packet size more than 1440.</p> <p>Explanation: The maximum receivable unit size is not set to maximum value after reload.</p> <p> Click for Additional Information</p>
<p>Case: 00627437 CRAOS8X-33962</p>	<p>Summary: MAC sec port unable to receive with packet size more than 1440.</p> <p>Explanation: The maximum receivable unit size is not set to maximum value after reload.</p> <p> Click for Additional Information</p>
<p>Case: 00639107 CRAOS8X-34880</p>	<p>Summary: DHCP snooping doesn't support on UNP SAP port in SPB domain-Documentation update.</p> <p>Explanation: The DHCP offer packet are not trapped on virtual ports as the snooping rule is not applicable for sap ports.DHCP snooping is not supported in service domain, it works in the vlan domain.</p> <p> Click for Additional Information</p>
<p>Case: 00613052 CRAOS8X-32770</p>	<p>Summary: Issue with a Microsoft Network Load Balancing (NLB) cluster is not reachable from outside the subnet.</p> <p>Explanation: OS6900-V48C6, enabling egress filtering was done when it was required to support Havlan on TOR(legacy).</p> <p> Click for Additional Information</p>
<p>Case: 00624339 CRAOS8X-33958</p>	<p>Summary: OS6900-V48C8: 10G ports showing as 25G ports after vc-takeover.</p> <p>Explanation: After VC-takeover all the master's ports being recognised as 25G interfaces in the CLI instead of SFP Plus SR (10G) that are plugged in this ports. This issue is not seen when entire VC is reloaded</p> <p> Click for Additional Information</p>
<p>Case: 00621021 CRAOS8X-33419</p>	<p>Summary: OS6900-V48C8 and OS6900-C32 FEC disabled configuration is not taken in account after switch reboot.</p>






	<p>Explanation: OS6900-V48C8 and OS6900-C32 FEC configuration is disabled, after reload the FEC status is not disabled. FEC disabled config is present in the vboot.cfg however it's like it was not applied post reboot.</p> <p> Click for Additional Information</p>
<p>Case: 00593242 CRAOS8X-31534</p>	<p>Summary: OS6900T48C6: Some PCs model are not coming up when connected to the switch.</p> <p>Explanation: After connecting PC(Fujitsu) to the OS6900T48C6 it doesn't comes up until changing the NIC parameter wait-link to off. This behavior is not affecting other switch models.</p> <p> Click for Additional Information</p>
<p>Case: 005621709 CRAOS8X-33449</p>	<p>Summary: OS6865 Switch reboots due to out of memory.</p> <p>Explanation: The ntpd.log file in saved in unevictable memory keeps increasing gradually. This causes the high memory usage leading to the switch reboot. A fix is available in 8.7.261 R02. The fix prevents continuous logging in the ntpd.log file thus avoiding high memory.</p> <p> Click for Additional Information</p>
<p>Case: 00619232 CRAOS8X-33332</p>	<p>Summary: 1G Port comes UP when just the SFP is connected without the cable.</p> <p>Explanation: The fake link up is due to a bug in software link scan. This issue is fixed in 8.9 R01.</p> <p> Click for Additional Information</p>
<p>Case: 00601484 CRAOS8X-31989</p>	<p>Summary: OS6860E switches are reporting fan failure OV trap displays incorrect index value.</p> <p>Explanation: OV receives a switch trap from the 6860 switches that are reporting fan failures and indicates the fan number as 1, 2, or 3. However, the 6860E switch trap displays a fan index value of 65. The issue is fixed in 8.9R01.</p> <p> Click for Additional Information</p>
<p>Case: 00619285 CRAOS8X-33432</p>	<p>Summary: After upgrading the OS6860 switches from OV the switch lost management access.</p> <p>Explanation: Tried upgrading the OS6860 switch from 8.7.354.R01 To 8.8.56.R02 via OV and noticed the switch lost management (MGMT) access. Configuring MGMT IP interface with "no forward" was not reachable. The MGMT IP interface with forwarding state, it was reachable.</p> <p> Click for Additional Information</p>
<p>Case: 00604718 CRAOS8X-32267</p>	<p>Summary: Not able to remove VRRP interface after IP interface is removed.</p> <p>Explanation: When removing the IP interface we cannot remote the VRRP Interface, following error is displayed: ERROR: Interface 'management' doesn't exist.</p> <p> Click for Additional Information</p>





<p>Case: 00607069 CRAOS8X-32396</p>	<p>Summary: High CPU noticed when FIPS is enabled.</p> <p>Explanation: The CLI task is continuously running which is invoking FIPS self-tests. In FIPS mode the self-tests are invoked when an application loads OpenSSL module, because of this relationship the tests are called for every CLI commands and result in CPU resources high usage.</p> <p> Click for Additional Information</p>
<p>Case: 00611346 CRAOS8X-32657</p>	<p>Summary: Wrong port number returned by bcmd appid when network loop occurs.</p> <p>Explanation: For some models, when enabling debug on bcmd appid during network loop the port printed into the swlogs does not correspond to the right UserPort.</p> <p> Click for Additional Information</p>
<p>Case: 00613637 CRAOS8X-32813</p>	<p>Summary: MACSEC secure link does not establish when switches are using different HW revision c0c0 and c1c1.</p> <p>Explanation: If MACSEC is enabled between two OmniSwitches using different HW revision, the link will be secured and then in next seconds will goes operationally DOWN.</p> <p> Click for Additional Information</p>
<p>Case: 00619175 CRAOS8X-33226</p>	<p>Summary: Syslog-ng core dump when syslog over TLS is enabled.</p> <p>Explanation: This issue happens when function reloads the OpenSSL library.</p> <p> Click for Additional Information</p>
<p>Case: 00626969 CRAOS8X-33912</p>	<p>Summary: Add the chassis ID in the log generated for DDM.</p> <p>Explanation: When DDM log is generated the chassis ID is missing: WARN: cmmEsmCheckDDMThresholdViolations: SFP\XFP Rx Power=-26.8 dBm on slot=1 port=9, crossed DDM threshold low alarm.</p> <p> Click for Additional Information</p>
<p>Case: 00626982 CRAOS8X-33914</p>	<p>Summary: Add the chassis ID in the log generated for DDM.</p> <p>Explanation: When DDM log is generated the chassis ID is missing: Port 13 FAULT State change 1b to 25 desc: Port is off: Improper Capacitor Detection results or Detection values indicating short (Fail due to out-of-range capacitor value or Fail due to detec.</p> <p> Click for Additional Information</p>
<p>Case: 00629417 CRAOS8X-34144</p>	<p>Summary: Add the system name in the log generated for SPB L1 Lost Adjacency</p> <p>Explanation: When SPB Adjacent node connectivity is lost, following log is generated but system name</p>

	<p>is missing: swlogd isis_spb_0 ADJACENCY INFO: Lost L1 adjacency with 9424.e161.7a61 on ifld 201054.</p> <p> Click for Additional Information</p>
<p>Case: 00635578 00592556 CRAOS8X-31513</p>	<p>Summary: In OS6560-48X4, running 8.7.R02, executing any show commands in CLI throw an error as "ERROR: specified application not loaded".</p> <p>Explanation: Some of the system related commands uses the application SSAPP which is found to be disconnected. When user executes a CLI command, the request will be forwarded to the related backend via MIPGW that are SSAPP, CAPMAN. MIPGW didn't find them due to the disconnection then it warned "specified application not loaded".</p> <p> Click for Additional Information</p>
<p>Case: 00624222 CRAOS8X-33701</p>	<p>Summary: How to stop TCP timestamp vulnerability in AOS 8x switches.</p> <p>Explanation: The fix for "TCP timestamp vulnerability" is available from 8.7.R02. The respective CLI commands and how to use them will be clearly documented in 8.9 R01 GA.</p> <p>Click for Additional Information</p>
<p>Case: 00611569 CRAOS8X-32670</p>	<p>Summary: Are OS6900/OS6860/OS6560 affected by CVE-2022-0778 running in AOS version 8.8.152.R02?</p> <p>Explanation: CVE-2022-0778 mentioned, affects AOS switches which are using OpenSSL-1.0.2u.</p> <ul style="list-style-type: none"> ▪ This vulnerability has been discovered in OpenSSL being used in configuration. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. ▪ OpenSSL version will be upgraded to the latest version 3.0.2 from 8.9R01 onwards. <p> Click for Additional Information</p>
<p>Case: 00618723 CRAOS8X-33251</p>	<p>Summary: Post upgrade to 8.8R01, noticed mip_lib and Lanpower errors.</p> <p>Explanation: These error logs appear due to any i2c bus internal error at the first msg transmission. This log is required to know the functionality of Lan power module. Hence this log message is moved from "Error" to "debug" level in build 8.9R01 and later.</p> <p> Click for Additional Information</p>
<p>Case: 00612161 CRAOS8X-32722</p>	<p>Summary: Post upgrade from 8.6R01 to 8.7R03 a "cspbroke.conf" file is generated in the working directory.</p> <p>Explanation: The "cspbroke.conf" file is used for communication between switch and HAN NMS. This config file is generated without enabling any feature in the switch. The fix is available in 8.9R01 and later builds.</p> <p> Click for Additional Information</p>

<p>Case: 00621425 CRAOS8X-33428</p>	<p>Summary: ASA enhanced mode config is not working as described in 8.8.R01. <ol style="list-style-type: none"> 1. Unable to create user account with "allow-config" parameter. 2. Unable to login into enhanced mode config. </p> <p>Explanation: The "allow config" and "config" parameters in authenticated switch access enhanced mode are not supported in 8.8.R01. This is a document error in switch management guide in 8.8.R01. This will be corrected from 8.9.R01 build.</p> <p> Click for Additional Information</p>
<p>Case: 00642599 CRAOS8X-35120</p>	<p>Summary: AOS 8.x / AOS 5.x - when doing show tech-support eng complete script must collect api_libcurl logs in flash directory for NaaS troubleshooting.</p> <p>Explanation: When doing a show-tech support eng complete this log is now collected from AOS 8.9 R01 build.</p> <p> Click for Additional Information</p>
<p>Case: 00627287 CRAOS8X-34017</p>	<p>Summary: LLDP packet are not sending right TLV in 8.8 R02.</p> <p>Explanation: If management vlan is 0, location tlv and port-vlan tlv will not be send in case of unport. That was getting applied for the non-unp port also.</p> <p> Click for Additional Information</p>
<p>Case: 00618609 CRAOS8X-33183</p>	<p>Summary: IOT Classification with DHCP option 55 was not applied when Discover packet was sent.</p> <p>Explanation: Code fix to process DHCP discover from DP side has been made.</p> <p> Click for Additional Information</p>
<p>Case: 00626208 CRAOS8X-34149</p>	<p>Summary: In OS6900-X72 switch, it is observed that the flood-limit and STP configurations are displayed twice for some random ports.</p> <p>Explanation: This issue is seen due to bug in overflow handling scenario while printing the snapshot for STP and Interface modules. Issue could be only seen with certain number of configuration line and also the type of configuration.</p> <p> Click for Additional Information</p>
<p>Case: 00599099 CRAOS8X-32102</p>	<p>Summary: Aruba AP-515 connected to OS6860E stack reports that the power negotiated via LLDP is 0.0W. The AP continued to work properly with the necessary power.</p> <p>Explanation: As per the datasheet, the Aruba AP-515 requires 25.5W to work without any restriction. During LLDP negotiation, the PD (Aruba AP-515) requested for 25.5 watt; however, the PSE (OS6860 switch) allocated 0.0 watt. Even though the LLDP negotiation was unsuccessful, the OS6860 switch did provide "PoE-AT" power, which is 30W. From the "Power Status" output of the AP, it is evident that the AP is running with "PoE-AT" power and the current Operational state is "No restrictions".</p>

	<p> Click for Additional Information</p>
<p>Case: 00609535 CRAOS8X-32682</p>	<p>Summary: loss of connectivity, for some users connected to UNP/Dynamic SAP, caused by virtual ports failing to be created. The command 'show service <serviceid> debug-info' will display only couple of users, some others missing.</p> <p>Explanation: Some additional configuration (UNP profile statically assigned to a UNP port-template) applied when traffic was running, created stale entries, then newer virtual ports could not get created for these SAP ports.</p> <p> Click for Additional Information</p>
<p>Case: 00620765 CRAOS8X-33680</p>	<p>Summary: Wireless connected devices to Stellar AP (with GRE tunnel established with 6860 GTTS) are not reachable once AP management VLAN is moved to SPB service between 6860 GTTS and 6900 X72 CORE switch (gateway for the L2GRE traffic).</p> <p>Explanation: the packets containing L2GRE header embedded were getting dropped, because of a flag configured per default on the OS6900 X72 SAP port, telling the packets with a L2GRE termination to get dropped and not tunneled. (at the Hardware low level)</p> <p>Note: a simpler design with the L2GRE tunnel gateway being on where the tunnel ends (on 6860 GTTS) would have avoided this problem.</p> <p> Click for Additional Information</p>
<p>Case: 00598831 CRAOS8X-31932</p>	<p>Summary: BYOD-Captive Portal: HTTPS redirect is not success for some of the packets when bulk packets are sent from Jmeter.</p> <p>Explanation: In the BYOD setup, when more than 100 HTTPS packets pushed from single user using the application Jmeter, there are "503 service unavailable" errors for the packets which exceeds 100 HTTPS packets. This is a limitation in OS6860E that only 100 HTTPS concurrent packets per sec which could be redirected.</p> <p> Click for Additional Information</p>
<p>Case: 00619224 CRAOS8X-33249</p>	<p>Summary: Ports[1/1/25-26-1 GIG SFP] not coming up when connected between OS6560-P24X4 to OS6900-X48C6, no issue with OS6560-P48X4.</p> <p>Explanation: This is a bug related to inband auto-negotiation for the phyless ports in OS6560-24X4. It is fixed in 89R01.</p> <p> Click for Additional Information</p>
<p>Case: 00633729 CRAOS8X-34561</p>	<p>Summary: OS6560 and OS6900-V48: Ports 1/27-30 ports doesn't come up while using 1G SFP Fiber when connected between OS6560 and OS6900-V48.</p> <p>Explanation: This is a bug related to inband auto-negotiation in OS6560-24X4. It is fixed in 89R01.</p> <p> Click for Additional Information</p>
<p>Case: 00625499 CRAOS8X-33799</p>	<p>Summary: Error message "Tech support timer expired. Abandoning command. Died on: qos statistics" while running "show tech-support eng complete" from slave unit</p>

	<p>Explanation: show tech-support eng complete” shouldn’t be allowed from slave chassis. Following error message will be displayed when show tech-support eng complete is executed from slave.</p> <p>-> <i>show tech-support eng complete</i> WARNING: <i>Cannot generate running.cfg file for tech-support when running on slave or secondary CMM.</i> Fix will be available in 89R01.</p> <p> Click for Additional Information</p>
<p>Case: 00638951 CRAOS8X-35013</p>	<p>Summary: AP goes to Unprovisioned 802.1x failed state after reboot of AP/switch in LPS+802.1x+MAC enabled port.</p> <p>Explanation: The issue is not seen after disabling the configuration “port-security learning-window 0 learn-as-static enable”. Once the MAC is converted to static in UNP user table, the current eapld used for message exchange between Switch and AP is lost. As a result, when EAP_SUCCESS is sent, it carried the eapld as zero. AP will reject the eap success packet with incorrect eapld value. This causes the AP to be in un-authenticated state. In non issue state, eap success packet value should be the increment of previous value.</p> <p>The behavior of sending EAP success with 0 is fixed in 89R01.</p> <p> Click for Additional Information</p>
<p>Case: 00607909 CRAOS8X-32689</p>	<p>Summary: This is about the new feature allowing the AP to act as an 802.1x client (refer to KCS#000066386). It is found that with wireless clients connected to the AP, the AP is frequently re-authenticating.</p> <p>Explanation: Changes have been made to not send the EAP-Success/Fail packets which are intended to clients, to the AP. EAP-Success/fail packets intended to the AP will be sent to the AP alone. The fix will be available as from AOS 8.9.R01.</p> <p> Click for Additional Information</p>
<p>Case: 00612062 CRAOS8X-32698</p>	<p>Summary: OS6860N: Policy rule log does not show the flow in "show qos log".</p> <p>Explanation: Configure QoS on the SAP port of OS6860 switch. The Policy works fine but it does not write on the QoS log. Currently, the policy rule "log" option is not supported for the service domain traffic. It is documented in 8.9.R01 guides.</p> <p> Click for Additional Information</p>
<p>Case: 00636034 CRAOS8X-34751</p>	<p>Summary: Lanpower capacitor-detection configuration disappeared after upgrading to 8.8R02.</p> <p>Explanation: Global level capacitor-detection command is changed to port-level capacitor-detection command in 8.8R02. However, automatic conversion does not work while upgrading to 8.8R02. Capacitor detection command will be automatically converted to port-level capacitor-detection while upgrading from AOS 87R03 to 89R01 after upgrade.</p> <p> Click for Additional Information</p>

<p>Case: 00639126 CRAOS8X-34890</p>	<p>Summary: OS6900-X72 acting as a DHCP relay agent is not forwarding any DHCP packet from client to the server. This issue started after upgrading from 8.4.1R03 to 8.7.98R03 step-by-step ISSU upgrade.</p> <p>Explanation: IP interface name containing 32 characters will not forward DHCP packets when it is used as a DHCP relay interface. There is an issue in the code while retrieving the DHCP relay interface with more than 31 characters.</p> <p> Click for Additional Information</p>
<p>Case: 00625687 CRAOS8X-33840</p>	<p>Summary: Show interfaces displays incorrect SFP model in OS6900-X72. The SFP is an SFP_PLUS_ZR, however it shows as SFP_PLUS_ER.</p> <p>Explanation: Code changes are done in AOS 8.9R01 to display the correct SFP model in show interfaces for SFP_PLUS_ZR SFPs.</p> <p> Click for Additional Information</p>
<p>Case: 00619588 CRAOS8X-33374</p>	<p>Summary: When a Switch is rebooted, its DHCP interface will not re-negotiate a new IP from the new IP DHCP network automatically. It requires an ip interface dhcp-client release/renew to get the new IP address.</p> <p>Explanation: This is a bug. Initially, the switch OS6360-P10 gets an IP address from DHCP. Once it does, it will retain the IP address permanently. The Switch will not get another IP address from a different DHCP server even after a reboot. Issue fixed in 8.9.R01</p> <p> Click for Additional Information</p>
<p>Case: 00589114 CRAOS8X-31634</p>	<p>Summary: After re-distributing local routes, the MED value is increased to 1. If a loopback is used for BGP, the aggregation will no longer work and display as in-active.</p> <p>Explanation: When the program enters the function "bgpComputeAggregate", there is an if condition checking the current status of aggregate address is "active" and else condition for "not-active". As per the current code, control flow enters both if and else part, hence returning the oper-state of aggr-address "not-active", when the debug command "debug ip bgp adv-loopback0" is enabled. While the debug command is disabled, everything is working as expected. Issue fixed in 8.9.R01.</p> <p> Click for Additional Information</p>

Appendix J: 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 8.7R3. 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-v#.deb)	MRP Application
ams / ams-apps (ams-v#.deb/ams-apps-v#.deb)	AOS Micro Services Application
OVSDB (aos-ovsdb-v#.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.	

Installing Packages

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

```
-> pkgmgr verify nos-mrp-v1.deb
    Verifying MD5 checksum.. OK
-> pkgmgr install nos-mrp-v1.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.R03-xxx	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.R03-xxx)...
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.R03-xxx	removed
-----	-------------	---------

/flash/working/pkg/mrp/install.sh

Remove the Debian package installation file. For example:

```
-> rm /flash/working/pkg/nos-mrp-v#.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.