

Release Notes - Rev. A

OmniSwitch 6360, 6465, 6560(E),
6570M, 6860(E), 6860N, 6865, 6900-
V72/C32/
C32E/X48C6/T48C6/X48C4E/V48C8/
T24C2/X24C2, 9900

Release 8.10R1

These release notes accompany release 8.10R1. These release notes provide important information on individual software features and hardware modules. Since much of the information in these release notes is not included in the hardware and software user manuals, it is important that you read all sections of this document before installing new hardware or loading new software.

Note: The OS6900-T20/T40/X20/X40/X72/Q32 models are no longer being supported starting with AOS Release 8.10R1. AOS Release 8.9R4 is that last release with support for these models.

Contents

Contents 2

Related Documentation..... 3

System Specifications 4

[IMPORTANT] *MUST READ*: AOS Release 8.10R1 Prerequisites and Deployment Information 10

Licensed Features 13

ALE Secure Diversified Code..... 16

New / Updated Hardware Support and Guidelines 17

8.10R1 New Feature and Enhancements..... 18

Open Problem Reports and Feature Exceptions 24

Hot-Swap/Redundancy Feature Guidelines 28

Technical Support..... 30

Appendix A: Feature Matrix 32

Appendix B: MACsec Platform Support 41

Appendix C: SPB L3 VPN-Lite Service-based (Inline Routing) / External Loopback Support / BVLAN Guidelines 42

Appendix D: General Upgrade Requirements and Best Practices 45

Appendix E: Standard Upgrade - OmniSwitch Standalone or Virtual Chassis 50

Appendix F: ISSU - OmniSwitch Chassis or Virtual Chassis 52

Appendix G: FPGA / U-boot Upgrade Procedure 55

Appendix H: CPLD Upgrade Procedure for ONIE-Based Devices 58

Appendix I: Fixed Problem Reports 60

Appendix J: Installing/Removing Packages 71

Appendix K: Fixed CVEs 73

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 6570M 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 Specifications

Memory Specifications

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
OS6570M	2GB	8GB
OS6860(E)	2GB	2GB
OS6860N	4GB	16GB
OS6865	2GB	2GB
OS6900-V72/C32	16GB	16GB
OS6900-X48C6/T48C6/X48C4E/T24C2/X24C2	8GB	32GB ¹
OS6900-V48C8/C32E	16GB ²	64GB ¹
OS9900	16GB	2GB
1. Size of physical memory. Partitioned to 16GB flash memory. 2. Previous release notes incorrectly listed 8GB.		

U-Boot and FPGA Specifications

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 8.10.102.R01 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6360-10	8.7.149.R02	8.7.30.R03 ² 8.9.85.R02 ⁴	0.11	0.11 0.12 ⁵
OS6360-P10	8.7.149.R02	8.7.30.R03 ² 8.9.85.R02 ⁴	0.11	0.11 0.12 ⁵
OS6360-P10A (904324-90)	8.8.2.R03	8.8.2.R03 8.9.85.R02 ⁴	0.1	0.1 0.2 ⁵

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6360-24	8.7.149.R02	8.7.30.R03 ² 8.9.85.R02 ⁴	0.15	0.17 ¹ 0.20 ³
OS6360-P24	8.7.149.R02	8.7.30.R03 ² 8.9.85.R02 ⁴	0.15	0.17 ¹ 0.20 ³
OS6360-P24X	8.7.149.R02	8.7.30.R03 ² 8.9.85.R02 ⁴	0.12	0.12 0.13 ⁵
OS6360-PH24	8.7.149.R02	8.7.30.R03 ² 8.9.85.R02 ⁴	0.12	0.12 0.13 ⁵
OS6360-48	8.7.149.R02	8.7.30.R03 ² 8.9.85.R02 ⁴	0.15	0.17 ¹ 0.20 ³
OS6360-P48	8.7.149.R02	8.7.30.R03 ² 8.9.85.R02 ⁴	0.15	0.17 ¹ 0.20 ³
OS6360-P48X	8.7.149.R02	8.7.30.R03 ² 8.9.85.R02 ⁴	0.12	0.12 0.13 ⁵
OS6360-PH48	8.8.114.R01	8.8.114.R01 8.9.85.R02 ⁴	0.12	0.12 0.13 ⁵

1. FPGA version 0.17 is REQUIRED to address issues CRAOS8X-26370 and CRAOS8X-25033.
2. Optional U-boot update for CRAOS8X-24464, ability to disable/authenticate U-boot access.
3. Optional FPGA update for reduced fan speed at boot up.
4. Highly recommended to address NAND flash corruption issue CRAOS8X-35470. Also adds support for Gowin CPLD.
5. For switches currently shipping from the factory. No upgrade required for existing switches.

OmniSwitch 6465 - AOS Release 8.10.102.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 8.9.85.R02 ⁵	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 8.9.85.R02 ⁵	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 8.9.85.R02 ⁵	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 8.9.85.R02 ⁵	0.4	0.4
OS6465T-P12	8.6.117.R01	8.7.2.R02 ² 8.7.30.R03 ³	0.4	0.4

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
		8.8.33.R01 ⁴ 8.9.85.R02 ⁵		
OS6465-P12 (ENH-240)	8.8.33.R01	8.8.33.R01 8.9.85.R02 ⁵	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 U-boot update for CRAOS8X-24464, ability to disable/authenticate U-boot access. 4. Optional U-boot update to support boot from USB feature. 5. Highly recommended to address the NAND flash corruption issue CRAOS8X-35470.				

OmniSwitch 6560 - AOS Release 8.10.102.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 8.9.85.R02 ⁹	0.7	0.8 ⁵ 0.9 ⁹
OS6560-P24Z24	8.4.1.23.R02	8.7.2.R02 ³ 8.7.30.R03 ⁷ 8.9.85.R02 ⁹	0.6	0.7 ¹ 0.8 ⁵ 0.9 ⁹
OS6560-24Z8	8.5.22.R01	8.7.2.R02 ³ 8.7.30.R03 ⁷ 8.9.85.R02 ⁹	0.7	0.8 ⁵ 0.9 ⁹
OS6560-P24Z8	8.4.1.23.R02	8.7.2.R02 ³ 8.7.30.R03 ⁷ 8.9.85.R02 ⁹	0.6	0.7 ¹ 0.8 ⁵ 0.9 ⁹
OS6560-24X4	8.5.89.R02	8.7.2.R02 ⁴ 8.7.30.R03 ⁷ 8.9.85.R02 ⁸	0.4	0.4
OS6560-P24X4	8.5.89.R02	8.7.2.R02 ⁴ 8.7.30.R03 ⁷ 8.9.85.R02 ⁸	0.4	0.4
OS6560-P48Z16 (903954-90)	8.4.1.23.R02	8.7.2.R02 ³ 8.7.30.R03 ⁷ 8.9.85.R02 ⁹	0.6	0.7 ¹ 0.8 ⁵ 0.9 ⁹
OS6560-P48Z16 (all other PNs)	8.5.97.R04	8.7.2.R02 ³ 8.7.30.R03 ⁷ 8.9.85.R02 ⁹	0.3	0.6 ² 0.7 ⁶
OS6560-48X4	8.5.97.R04	8.7.2.R02 ⁴ 8.7.30.R03 ⁷ 8.9.85.R02 ⁸	0.4	0.7 ² 0.8 ⁶
OS6560-P48X4	8.5.97.R04	8.7.2.R02 ⁴ 8.7.30.R03 ⁷ 8.9.85.R02 ⁸	0.4	0.7 ² 0.8 ⁶

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6560-X10	8.5.97.R04	8.7.2.R02 ⁴ 8.7.30.R03 ⁷ 8.9.85.R02 ⁸	0.5	0.8 ²
OS6560E-P24Z8	8.9.85.R02	8.9.85.R02	0.9	0.9
OS6560E-P48Z16	8.9.85.R02	8.9.85.R02	0.7	0.7
<p>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 U-boot update for CRAOS8X-24464, ability to disable/authenticate U-boot access. 8. Highly recommended to address the NAND flash corruption issue CRAOS8X-35470. 9. Ships from factory. No upgrade required, there are no functional changes in this U-boot version for these models.</p>				

OmniSwitch 6570M - AOS Release 8.10.102.R01 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6570M-12	8.9.25.R02	8.9.25.R02 8.9.92.R02 ¹ 8.9.139.R03 ³ 8.9.92.R04 ⁴	0.11	0.11
OS6570M-12D	8.9.25.R02	8.9.25.R02 8.9.92.R02 ¹ 8.9.139.R03 ³ 8.9.92.R04 ⁴	0.11	0.11
OS6570M-U28	8.9.25.R02	8.9.25.R02 8.9.92.R02 ¹ 8.9.139.R03 ³ 8.9.70.R04 ⁴	0.11	0.11 0.12 ²
<p>1. Adds support for Gowin CPLD. 2. Addresses power supply interrupt issue. 3. Addresses CRAOS8X-40924 for disabling U-boot access. 4. Adds support for signed AOS images.</p>				

OmniSwitch 6860(E) - AOS Release 8.10.102.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	0.20	0.20
OS6860E-P24Z8	8.4.1.17.R01	8.7.30.R03 ²	0.5	0.7 ¹

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
1. FPGA versions .7 and .10 are optional on the PoE models for the fast and perpetual PoE feature support. 2. Optional U-boot update for CRAOS8X-24464, ability to disable/authenticate U-boot access.				

OmniSwitch 6860N - AOS Release 8.10.102.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 8.10.102.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 U-boot update for CRAOS8X-24464, ability to disable/authenticate U-boot access. 4. Optional U-boot 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-V72/C32/C32E/X48C6/T48C6/X48C4E/V48C8/T24C2/X24C2- AOS Release 8.10.102.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

Hardware	Minimum ONIE	Current ONIE	Minimum CPLD	Current CPLD
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
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 CPU CPLD - 2.15 ²
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
<p>1. Optional CPU CPLD update to address CRAOS8X-30098. 2. Required CPLD update to address CRAOS8X-43968 (Hardware revision 6 only). Note: These models use the Yos.img image file.</p>				

OmniSwitch 9900 - AOS Release 8.10.102.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 8.8.152.R01	2.3.0	2.3.0	0.8
OS99-CMM2	8.9.183.R03	8.9.183.R03	1.4.0	1.4.0	1.2.0
OS9907-CFM	-	-	-	-	-
OS9907-CFM2	-	-	-	-	-
OS9912-CFM	-	-	-	-	-
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

Hardware	Minimum Coreboot-Uboot	Current Coreboot-Uboot	Minimum Control FPGA	Current Control FPGA	Minimum/Current Power FPGA
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 2.12.0 ³	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 1.8.0 ³	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 1.10 ³	N/A
OS99-XNI-P48Z16	8.4.1.20.R03	8.4.1.20.R03 8.8.152.R01	1.4	1.4 1.6	0.7
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 2.12.0 ³	0.8
OS99-XNI-P24Z8	8.5.76.R04	8.6.261.R01 8.8.152.R01	1.1	1.4.0 1.6.0	0.7
OS99-XNI-U12Q	8.6.117.R01	8.6.117.R01 8.8.152.R01	1.6.0	1.5.0 1.6.0	N/A
OS99-XNI-UP24Q2	8.6.117.R01	8.6.117.R01 8.8.152.R01	1.5.0	1.5.0 1.6.0	N/A
OS99-CNI-U20	8.9.183.R03	8.9.183.R03	1.2.0	1.2.0	0.4

1. Optional U-boot update for CRAOS8X-24464, ability to disable/authenticate U-boot access.
 2. Optional U-boot/FPGA update for CMM2 and OS9912 compatibility.
 3. Optional FPGA upgrade to address CRAOS8X-43592: 1G/10G SFP not recognized.

Note: Existing OS9900 NIs used in the OS9907 chassis that are to be used in the OS9912 chassis must first have the Uboot and FPGA upgraded before inserting them into the OS9912 chassis. See footnote #2.

[IMPORTANT] *MUST READ*: AOS Release 8.10R1 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 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.
 - OS6570M-12/12D ports 9 and 10 do not support fast 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.

Deprecated Features / Functionality Changes

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

AOS Release 8.5R4
EVb - Beginning in 8.5R4, support for EVb is being removed. Any switches with an EVb configuration cannot be upgraded to 8.5R4 or above.
NTP - Beginning with AOS Release 8.5R4, OmniSwitches will not synchronize with an unsynchronized NTP server (stratum 16), as per the RFC standard. Existing installations where OmniSwitches are synchronizing from another OmniSwitch, or any other NTP server which is not synchronized with a valid NTP server, will not be able to synchronize their clocks. The following NTP commands have been deprecated: <ul style="list-style-type: none"> - ntp server synchronized - ntp server unsynchronized
AOS Release 8.6R1
DHCPv6 Guard - Configuration via an IPv6 interface name is deprecated in 8.6R1. Commands entered using the CLI must use the new 'ipv6 dhcp guard vlan vlan-id' format of the command. The old format will still be accepted if present in a vcboot.cfg to preserve backwards compatibility.
IP Helper - The 'ip helper' commands have been deprecated in 8.6R1 and replaced with 'ip dhcp relay'. The old format will still be accepted if present in a vcboot.cfg to preserve backwards compatibility.
SAA - The vlan-priority and drop-eligible parameters have been deprecated from all SAA commands beginning in 8.6R1.
MACsec is now supported on ports 33-48 of the 6560-(P)48X4. CRAOS8X-7910 was resolved in 8.6R1.
AOS Release 8.6R2
Distributed ARP - Beginning 8.6R2 distributed ARP is no longer supported.
WRED - Beginning in 8.6R2 WRED is no longer supported.
QoS - Beginning in 8.6R2 the 'qos dscp-table' command is no longer supported.
NTP - The ntp parameter for the 'ip service source-ip' command was deprecated in 8.5R4. Support has been added back in 8.6R2.

AOS Release 8.7R1
MACsec - Static mode is not supported on OS6860N.
Transceivers - Beginning in AOS release 8.7R1 an error message will be displayed when the unsupported QSFP-4X25G-C transceiver is inserted on an OS99-CNI-U8 module.
SPB - Beginning in 8.7.R01 the default number of BVLANS created via Auto Fabric is reduced from 16 to 4. This new default value is only applicable to factory default switches running 8.7R1 with no vcboot.cfg file. Upgrading to 8.7.R1 will not change the number of configured BVLANS in an existing configuration. See Appendix C for additional information.
AOS Release 8.7R2
There are new default user password polices being implemented in 8.7R2. This change does not affect existing users. <ul style="list-style-type: none"> - cannot-contain-username: enable - min-uppercase: 1 - min-lowercase: 1 - min-digit: 1 - min-nonalpha: 1
The OmniSwitch 6360 does not contain a real-time clock. <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
The Kerberos Snooping is not supported in bridge mode in this release.
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
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. OS6560-BP-PH - This OS6560 600W power supply, OS6560-BP-PH (904072-90), requires a minimum AOS version of 8.8R1. OS6560-BP-PX - This OS6560 920W power supply, OS6560-BP-BX (904073-90), requires a minimum AOS version of 8.8R1. Refer to the OmniSwitch 6560 Hardware Guide for additional power supply information.
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.
AOS Release 8.9R4
OmniSwitch 6570 signed AOS image support with proper u-boot was added.
AOS Release 8.10R1
CRAOS8X-46556 (CVE-2024-6387) fix has been implemented by default in 8.10R1. See Appendix K: Fixed CVEs .

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. Refer to the licensing [portal](#).

Data Center License Required	
	OmniSwitch
Licensed Features	
DCB (PFC,ETS,DCBx)	Not Supported
FIP Snooping	Not Supported
FCoE VxLAN	Not Supported

Feature/Performance License Required								
	OS6360	OS6465	OS6560	OS6570M	OS6860	OS6860N	OS6900	OS9900
Licensed Features								
MACsec (OS-SW-MACSEC)	N/A	Yes	Yes	N/A	Yes	Yes	Yes ³	Yes
10G support (OS6560-SW-PERF)	N/A	N/A	Yes ¹	N/A	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	N/A
10G support (OS6570-SW-PERF4)	N/A	N/A	N/A	Yes ⁴	N/A	N/A	N/A	N/A
MPLS	N/A	N/A	N/A	N/A	N/A	Yes	N/A	N/A

1. Performance software license is optional allowing ports 25/26 (OS6560-24X4/P24X4) and ports 49/50 (OS6560-48X4/P48X4) to operate at 10G speed. Ports support 1G by default.
2. Performance software license is optional allowing the 2 RJ45/SFP+ combo ports (25/26 or 49/50) of the OS6360-PH24 or OS6360-PH48 models to operate at 10G speed. Ports support 1G by default.
3. MACsec is supported on the OS6900-X48C4E.
4. Performance software license is optional allowing the OS6570M-U28 ports 25-28 to operate at 10G speed. Ports support 1G by default.

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

Advanced Routing License Required		
	OmniSwitch 6570M	OmniSwitch 6560
Licensed Features		
OSPFv2 and OSPFv3	Yes	Yes (Up to 2 Areas)
PIM Multicast Routing (IPv4 & IPv6)	Yes	Yes
Multiple VRFs	Yes	Not Supported
ISIS (IPv4 and IPv6)	Yes	Not Supported

GRE Tunneling	Yes	Not Supported
IP-IP Tunneling	Yes	Not Supported
Route Redistribution	Yes	Yes
VRF Route Leaking	Yes	Not Supported
Note: Starting in 8.9R4 the table above lists the features supported with the Advanced Routing license.		

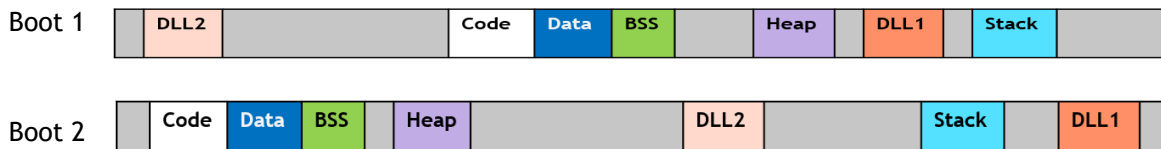
ALE Secure Diversified Code

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

OS6560E-P24Z8

Fixed configuration chassis in a 1U form factor with:

- Sixteen (16) - 10/100/1000 BaseT 802.3at PoE ports
- Four (4) - 100/1000/2.5G Base-T 802.3bt PoE ports
- Four (4) - 100/1000/2.5G/5G Base-T 802.3bt PoE ports
- Two (2) - SFP+ (1G/10G) ports
- USB port
- RJ-45 console port
- Ships with 600W AC PoE power supply (OS6560-BP-PH).

OS6560E-P48Z16

Fixed configuration chassis in a 1U form factor with:

- Thirty-two (32) - 10/100/1000 BaseT 802.3at PoE ports
- Four (4) - 100/1000/2.5G/5G Base-T 802.3bt PoE ports
- Twelve (12) - 100/1000/2.5G Base-T 802.3bt PoE ports
- Four (4) - SFP+ (1G/10G) ports
- Two (2) - 20G Virtual Chassis VFL ports
- USB port
- RJ-45 console port
- Ships with 920W AC PoE power supply (OS6560-BP-PX).

8.10R1 New Feature 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.

Summary Table

Feature	OmniSwitch Platform
<u>Management Features</u>	
Hybrid Interface Auto Detect	6465T, 6570M-U28
OVNA - Loop Detection Preventative Maintenance	6360, 6465, 6560, 6570M, 9900
Password-protected ONIE access	6860N, 6900
Signed AOS Image	6360, 6465, 6560, 6570M, 6860, 6860N, 6865, 6900, 9900
Prompt-On-Deletion Enhancement	6360, 6465, 6560, 6570M, 6860, 6860N, 6865, 6900, 9900
<u>Service Features</u>	
IPv4 Source Filtering Over SPB/VxLAN/VPLS Services	6860N, 6900
VxLAN Ethernet VPN (EVPN)	6900-X48C6/T48C6/X48C4E/ V48C8/ C32E/T24C2/X24C2
LACP Frames Over SPB L2-Services	6860, 6860N, 6865, 6900, 9900
Define Modulo Used by Switch to Calculate BVLAN	6860, 6860N, 6865, 6900, 9900
SPB Fabric Hashing Mechanism Enhancement	6860N, 6900
<u>QoS/Security Features</u>	
Bi-directional IPv6 ACL	6560, 9900
ACL Destination Port Group on IGMP Snooping	6360, 6465, 6560, 6570M, 9900
Policy VLAN Group Condition for QoS	6360, 6465, 6560, 6570M, 6860N, 6900-V72/C32, 9900
AP Mode for Third-party APs	All
<u>Licensed Features</u>	
Multicast Routing Support on OS6560	6560

Management Features

Hybrid Interface Auto Detect

The OmniSwitch can now auto detect the SFP or RJ-45 cable on the hybrid port and bring up the interface based on what is connected. To implement this a new configurable **hybrid-mode auto** is introduced to auto detect the connected device on the hybrid port.

In auto mode the OmniSwitch will scan for signals on both the copper and fiber media. If a link is detected on the fiber media, the OmniSwitch will enable the fiber mode, or if a link is detected on RJ-45 port the OmniSwitch will enable the copper mode.

If both cables are connected simultaneously, fiber mode is enabled as the preferred mode.

The following CLI commands are associated with this feature:

- **interfaces {slot chassis/slot | port chassis/slot/port[-port2]} hybrid-mode {fiber | copper | auto}**

OmniVista Network Advisor (Preventative Maintenance)

To indicate the potential loop in the network a loop detection threshold counter is introduced in the swlog. When the threshold is breached, it indicates a potential loop in the network. There will be continuous MAC movements in the event of a network loop which will be counted by a loop detection counter. When this counter exceeds the maximum threshold a log will be added in the swlog indicating the potential loop in the network. The maximum threshold is configurable.

The following CLI commands are associated with this feature:

- **debug mac-learning loop-detection-threshold num**
- **debug show mac-learning loop-detection-threshold**

Password-protected ONIE Access

Enable or disables authentication for access to ONIE.

- When the authentication option is enabled ONIE access is allowed only after authenticating with a password.
- When the authentication option is disabled ONIE access is allowed without a password.
- If ONIE authentication is disabled after being enabled, any existing password is reset.
- In the case of a VC, the ONIE authentication will be synchronized to all existing units of the VC. The authentication will not be synchronized to any new unit joining the VC. The configuration needs to be set before adding a new unit to the VC.
- During disaster recovery the correct password must be entered to recover the switch if ONIE authentication is enabled. If the password is forgotten there is no other mechanism to perform disaster recovery and the switch needs to undergo RMA.

The following CLI commands are associated with this feature:

- **onie authentication {enable password <password> | disable}**
- **show onie config**

Signed AOS Image

This feature enhancement provides the ability for an OmniSwitch to determine if the AOS software comes from a trusted source and to detect if it has been tampered with after signing. Using RSA-4096 and SHA-256, AOS images are signed with a private key allowing AOS to verify the signature with a corresponding public key during reload and flash synchronization.

- The signature will be stored as part of the AOS image file, there are no U-boot or ONIE dependencies for this feature.
- Starting in 8.10R1, the required code signing certificate containing the public key and the associated CA bundle will automatically be setup on the switch for signature verification.

Prompt-On-Deletion Enhancement

This enhancement provides the **prompt-on-deletion** parameter to prevent accidental deletion of a single VLAN or range of VLANs with member ports attached. When enabled, the user will be prompted to confirm the deletion of a VLAN with member ports attached.

The following CLI commands are associated with this feature.

- **[no] vlan prompt-on-deletion**
- **show vlan configuration**

Service Features

IPv4 Source Filtering Over SPB/VxLAN/VPLS Services

ISF can be enabled across the four services supported in AOS. Service level source filtering and port level source filtering are mutually exclusive. ISF on a service is not supported on Dynamic Service IDs.

The following CLI commands are associated with this feature.

- **dhcp-snooping ip-source-filter service**
- **show dhcp-snooping ip-source-filter service**
- **show dhcp-snooping isf-statistics service**

VxLAN Ethernet VPN (EVPN)

The OmniSwitch Ethernet Virtual Private Network (EVPN) feature is implemented as described in RFC 7432. AOS EVPN adapts the latest specification of the RFC (draft-ietf-bess-rfc7432bis-07). The EVPN protocol is based on the MP-BGP and provides several improvements to the existing AOS overlay services.

The EVPN based services provide multihoming capability for the access host devices along with the L2 and L3 mobility for the connected hosts. The multihoming of the hosts will provide better network utilization due to the multi-path routes and provide network redundancy for the hosts. The EVPN based networks also reduces the amount of broadcast traffic in the overlay network. This is achieved by managing the L2 and L3 host FDB entries in the control plane.

The BGP EVPN protocol is supported by using the BGP route types (Type 1 to 4, and Type 6 to 8) to orchestrate the EVPN functionality. Each route type has a specific function in the operation of an overlay EVPN network. Additionally, EVPN will also support the default gateway functionality using the BGP default gateway extended community as defined in RFC 7432.

In AOS, the EVPN protocol is based on MP-BGP and provides several improvements to the existing AOS overlay services. In this release, EVPN is supported only on VxLAN services.

The OmniSwitch supports VxLAN based EVPN. The EVPN works on the control plane and the VxLAN works on the data plane. This enhances the layer 2 and layer 3 efficiency and scalability. It allows to scale the network by extending the Layer 2 connectivity across different locations by a network overlay in an existing physical network.

The following CLI commands are associated with this feature.

Service Manager commands

- `service bgp-evpn`
- `service igmp-mld-proxy`
- `service proxy-arp`
- `service bgp-evpn mac-mobility`
- `show service evpn ethernet-segment`
- `show service evpn evi`
- `service vxlan`
- `show service debug-info`
- `show service`
- `show service proxy-arp config`
- `service access`

BGP commands

- `ip bgp neighbor activate-evpn`
- `ip bgp address-family evpn`
- `show ip bgp`
- `show ip bgp neighbors`

IP commands

- `show ip evpn proxy-arp`
- `ip anycast-gateway-mac auto`
- `ip interface anycast-gateway-address`
- `debug ip proxy-arp aging-time`
- `arp`
- `ip interface`
- `show ip interface`
- `show ip config`
- `clear arp-evpn-proxy-cache`

Source Learning commands

- `mac-learning domain evpn-vxlan static mac-address`
- `mac-learning flush domain evpn-vxlan service`
- `show mac-learning evpn-vxlan`
- `show mac-learning`

IP Multicast Swtiching commands

- `show ip multicast evpn`
- `show ip multicast group`

LACP Frames Over SPB L2-Services

Supports tunnelling of 802.3ad Link Aggregation Control Protocol frames over an SPB network.

The following CLI commands are associated with this feature.

- **service l2profile**
- **show service l2profile**

Define Modulo Used by Switch to Calculate BVLAN

BVLAN modulo number is used to dynamically calculate an SPB BVLAN value for a System Default profile. As part of this enhancement, a new CLI is added to configure the BVLAN modulo value to dynamically calculate an SPB BVLAN value for a System Default profile. This configured value will be used to derive BVLAN for auto service creation for UNP user learning. The default value of **bvlan-mod** is set to 8.

Note: Not supported with auto-fabric configuration.

The following CLI commands are associated with this feature.

- **unp system-default bvlan-mod**
- **show unp global configuration**

SPB Fabric Hashing Mechanism Enhancement

Currently, the hashing process relies on MAC addresses of ingress/egress BEB and ISID. However, certain traffic patterns result in inconsistent BEB nodes and ISID, leading to uneven traffic distribution or the saturation of a link when the BEB nodes and ISIDs are the same. To address the hashing issue source/destination IPs and ports within SPB packets will be incorporated into the hashing algorithm. A new command is provided to configure the new mode to enable or disable source/destination IP addresses and ports in the SPB MAC-in-MAC payload.

The following CLI commands are associated with this feature:

- **hash-control extended spb-payload {enable | disable}**
- **show hash-control**

QoS/Security Features

Bi-directional IPv6 ACL

The OmniSwitch is enhanced to support configuration of bi-directional IPv6 ACL. The bi-directional IPv6 can be configured using the CLI, **capability profile tcam mode source-dest-ipv6**. The existing **capability profile tcam mode** command is modified to accommodate both the source and destination IPv6 in the ACL. When the new capability profile **source-dest-ipv6** is selected, the write memory must be performed and the switch must be reloaded. The **show capability profile** command is modified to display the configured/active TCAM mode settings. The following CLI commands are associated with this feature.

- **show capability profile**
- **capability profile tcam mode source-dest-ipv6**

ACL Destination Port Group on IGMP Snooping IPv6 ACL

The OmniSwitch now supports policy condition destination port or port group along with multicast IPv4 addresses on OS6360, OS6465, OS6560, OS6570, and OS9900 platforms.

The following CLI command example is associated with this feature.

- **policy port group pg_xyz 1/1/25 1/2/25**
- **policy condition igmp_qry destination port group pg_xyz multicast ip 224.0.0.1**
- **policy rule igmp_qry precedence 2000 condition igmp_qry action accept**

- **policy rule block_mcast precedence 800 condition traf_mcast action deny**

Policy VLAN Group Condition for QoS

This enhancement allows for the configuration of a VLAN group and its associated VLAN ID numbers. A VLAN group may be attached to a policy condition. The action associated with that policy will be applied to all members of the VLAN group.

The following CLI commands are associated with this feature.

- **policy vlan group group_name {vlan[-vlan2]} [vlan[-vlan2]]**
- **no policy vlan group group_name**
- **policy vlan group group_name no {vlan[-vlan2]} [vlan[-vlan2]]**
- **policy condition condition_name source vlan group vlan_group**
- **policy condition condition_name no source vlan group**
- **show [applied] policy vlan group [vlan_group]**

AP Mode for Third-party APs

The OmniSwitch allows support for both Stellar and third-party APs. The AP mode feature for third-party APs can be configured with the option “all”. The existing CLI **unp ap-mode** is modified to configure the support for third-party APs.

The following CLI commands are associated with this feature.

- **unp ap-mode {enable | disable} {secure [enable | disable]} {type [stellar | all]}**
- **show unp global configuration**

Licensed Features

Multicast Routing Support on the OmniSwitch 6560

Adds support for PIMv4 and PIMv6 to the OS6560 with the Advanced Routing license.

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-23137	When high number of vlans are mapped to DHL links, during failover some traffic loss may be seen.	There is no known workaround at this time.
CRAOS8X-41054	On an OS9912, when upgrading coreboot on both CMMs at the same time and reloading from working, CMM-B becomes primary instead of CMM-A as expected.	Upgrade one CMM at a time.
CRAOS8X-41328	On an OS9912 if a member port of a link aggregate with hashing/load-balancing enabled is disabled all the traffic may be sent on just one of the other ports instead of being load-balanced across the link aggregate.	There is no known workaround at this time.
CRAOS8X-41385	In some instances, during a reboot or Virtual Chassis failover scenario, junk/ineligible characters may be seen on the OS9907/OS9912 CMM console port(s).	There is no known workaround at this time. Display only no functional impact.
CRAOS8X-44303	With na AOS system name of more than 32 characters, BYOD functionality will not work with OV since system name is one of the attributes in COA/DM messages and NAS-ID in OV can't be set beyond 32 characters.	Decrease AOS system name to 32 characters or less.
Hardware / Transceivers		
CRAOS8X-41538	Intermittently (rarely) OS99-CNI-U20 module can fail to come up and park in an unpowered state. A messages similar to the following may be seen on console (and NI swlogs): \+++ NI in slot [s] power-good failure in 3 attempts - disabling	Hot-swap the NI (unplug/replug) or power cycle the chassis.
CRAOS8X-41609	On 6860N 25G ports with a 4x10G transceiver, on intermittent admin disables one or more ports will continue to display up.	Admin enable the port when peer is disabled or disconnect/remove the transceiver.
CRAOS8X-41611	On an OS99-CNI-U8 with 4x25G DAC link sometimes does not come up for certain lanes.	Use the QSFP-100G-SR4 fiber transceiver with 4X25G capability.
CRAOS8X-43486	On some platforms (OS6860N 25G ports, OS6900 10G and 25G ports, OS6560-P48X4 ports 53/54 and OS6360 uplink ports), the SFP-10G-GIG-LR/SR only links up at 10G and is unstable at 1G speed.	If 1G speed is required, use 1G transceivers.

CRAOS8X-44378	A fake link with SFP-DUAL-BX-D/U on the 25G ports may sometimes be seen.	There is no known workaround at this time.
CRAOS8X-46185	Fiber ports with SFP-GIG-T connected to peer at 10M speed is operational as expected. However, when the peer link changes from 10M to 100M or 1G speed, user may (intermittently) see link down with peer side link up.	On OS6570M-U28 a hot-swap of the SFP-GIG-T recovers the port. On OS6570M-12/12D a switch reload may be required to recover port.
CRAOS8X-46195	VFL links using 4X25G splitters require additional configuration to prevent CRC errors being seen on the link.	The preferred method is configuring inter-frame-gap to 13 on both sides of the link. An alternate method is configuring FEC to FC and auto-negotiation disable on both sides of the link. Note: Configuring FEC and disabling auto-negotiation will cause link to reset.
Layer 2		
CRAOS8X-26502	While converging due to a link/node failure in a MRP ring network, sometimes a very few multicast IGMP clients are not relearned when there are more than 200 multicast streams.	Clients will be relearned after the next query interval.
CRAOS8X-37429/41707	When configuring an ERP ring and verifying convergence with link down/up and node down/up event, the convergence number is high for an average 10 iterations.	There is no known workaround at this time.
CRAOS8X-38898	When configuring ip multicast with non-default profiles and enabling zero-based-query, no zero-based-query packet received after toggling UNP port.	There is no known workaround at this time.
Layer 3		
CRAOS8X-11084	Packet drop seen in BFD config when VRRP VLAN interface is toggled.	There is no known workaround at this time.
CRAOS8X-33472	When BGP peering sessions operate over an IPv6 TCP connection between two OS9900s 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 may be observed as follows: : bgp_0 tcp ERR message: OS9900 vrfId 0: <,> Bad marker rcvd! Aborting peer session. The BGP peering session will get re-established with	There is no known workaround at this time.

	no manual intervention necessary and the routing table will be restored.	
CRAOS8X-39691	On an OS9912 a BGP neighbor in a VRF may get stuck in idle state after NI reset if the same VLANs are associated to two different NIs.	After approximately 90 seconds the neighbor association will be restored.
CRAOS8X-44230	When IPMVLAN is enabled on a switch with rvlan configured on the receiver port, after a write memory flash-synchro and reload, when the ipmvlan configs are removed the slave unit still retains the routing mode on it. Now if IPMVLAN is enabled without rvlan on receiver port and the current slave becomes the master due to VC-takeover, it starts behaving like L3 mode with forward and source table getting populated when source traffic flows.	There is no known workaround at this time.
QoS/Security		
CRAOS8X-34219	With CFM2 and XNI-U48 board, port recovery after violation takes additional 2 mins with WTR of 15 secs.	
CRAOS8X-40989	On an OS99-XNI-P24Z8 the dynamic MACsec port status is down after a reload. The issue is only specific to the first 8 ports.	Toggle the MACsec admin state on the port.
CRAOS8X-41038	When configuring static MACsec without encryption and keys are mismatched, the traffic can still go through. Works as expected with encryption enabled.	There is no known workaround at this time.
Services		
CRAOS8X-33705	Double tagged packets with size less than 64 bytes received as encapsulated inside a tunneled packet (eg: SPB encapsulated), may get dropped on the network port of an OS6900.	There is no known workaround at this time.
CRAOS8X-38026	On an OS9912 some traffic drop seen when sending traffic on two different ISIDs after disabling trust tag on UNP port.	There is no known workaround at this time.
CRAOS8X-41204	When sending traffic for a maximum number of 1K VPLS Services, some traffic may be dropped when interfaces such as LER/LSR, IP, or OSPF are toggled.	The traffic will recover in approximately 15 to 25 seconds after link recovery.
CRAOS8X-41214	When sending traffic on a VPLS, the MACs are not being learned on SAP access and network ports after OSPF interface toggle. The traffic is successfully received on the egress of the and access ports. Issue is only seen when 1K MAC addresses are sent.	Resend the traffic after the toggle. Issue will not be seen with continuous traffic.
Virtual Chassis		
CRAOS8X-3877	On an OS6900 untagged packets are mirrored as tagged traffic when monitored port is across VC	Use port mirroring.

	chassis. On standalone chassis, monitored egress traffic is tagged.	
Other		
CRAOS8X-40728	<p>OS6900-V48C8 - Supports End-to-End Transparent Clock in a VC of 1 configuration at 1G/10G speeds. Not supported at 25G and 100G speeds.</p> <p>OS6860N-P48Z - Supports End-to-End Transparent Clock in VC of 1 configuration at 1G/10G speeds. Not supported at 2.5G, 5G, and 25G. At 1G speeds with Fiber Transceivers the CF accuracy (2Way Mean) is in the range of 100ns to 200ns for traffic at packet sizes 512 and random.</p> <p>OS6860N-U28 - Supports End-to-End Transparent Clock in VC of 1 configuration at 1G/10G speeds. Not supported at 25G speeds. At 1G speeds with Copper/Fiber Transceivers, the CF accuracy (2Way Mean) is in the range of 100ns to 350ns for traffic at packet sizes 512 and random.</p>	There is no known workaround at this time.

Hot-Swap/Redundancy Feature Guidelines

Hot-Swap Feature Guidelines

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

- When connecting or disconnecting a power supply to or from a chassis, the power supply must first be disconnected from the power source.
- 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 Slot	Hot-Swap/Hot-Insert compatibility
Empty	All modules can be inserted
OS99-CMM	OS99-CMM
OS99-CMM2	OS99-CMM2
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
OS99-CNI-U20	OS99-CNI-U20

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-V72 must be replaced with an OS6900-V72).
- 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: ale.welcomecenter@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+ : /flash/foss/gpl-3.0.txt +
with exceptions & /flash/foss/gpl-2.0.txt +
GPLv2+ with exceptions /flash/foss/lgpl-2.1.txt +
& LGPLv2+ & BSD /flash/foss/bsdl.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 2024 ALE International, ALE USA Inc. All rights reserved in all countries.

Appendix A: Feature Matrix

The following is a feature matrix for AOS Release 8.10R1.

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	OS6570M	6860(E)	6860N	6865	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
Management Features										
AOS Micro Services (AMS)	8.7R2	8.6R1	8.6R1	8.9R2	8.6R1	8.7R1	8.6R1	8.6R1	8.7R1	8.6R1
Automatic Remote Configuration Download (RCL)	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.6R2	8.7R1	Y
Automatic/Intelligent Fabric	8.7R2	8.5R1	Y	8.9R2	Y	8.7R2	Y	Y	Y	Y
Automatic VC	8.7R2	N	Y	8.9R2	Y	8.7R1	Y	8.6R2	8.7R1	N
Bluetooth - USB Adapter with Bluetooth Technology	8.7R2	8.6R2	8.6R2	8.9R2	Y	8.7R1	8.6R2	8.6R2	N	N
Console Disable	8.7R2	8.6R2	8.6R2	8.9R2	8.6R2	8.7R1	8.6R2	8.6R2	8.7R1	8.6R2
Dying Gasp	8.9R3	Y	Y	8.9R3	Y	8.7R1	Y	N	N	N
Dying Gasp (EFM OAM / Link OAM)	N	8.6R1	8.6R1	8.9R3	8.6R1	8.7R1	8.6R1	N	N	N
EEE support	Y	8.9R1	8.9R1	8.9R2	Y	8.7R1	Y	Y	Y	Y
Embedded Python Scripting / Event Manager	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.7R2	8.7R2	Y
IP Managed Services	N	N	N	N	Y	8.7R1	Y	8.5R2	8.7R1	Y
Hitless Security Patch Upgrade	8.7R2	8.7R1	8.7R1	8.9R2	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1
In-Band Management over SPB	N	N	N	N	8.5R4	8.7R1	8.5R4	8.5R4	8.7R1	8.5R4
ISSU	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
NaaS	8.8R1	8.8R1	8.8R1	8.9R2	8.8R1	8.8R1	8.8R1	8.8R1	8.8R1	8.8R1
NAPALM Support	8.7R2	8.5R1	8.5R1	8.9R2	8.5R1	8.7R1	8.5R1	8.7R2	8.7R2	N
NTP - Version 4.2.8.p11	8.7R2	8.5R4	8.5R4	8.9R2	8.5R4	8.7R1	8.5R4	8.5R4	8.7R1	8.5R4
NTP - IPv6	8.7R3	8.7R3	8.7R3	8.9R2	8.7R3	8.7R3	8.7R3	8.7R3	8.7R3	8.7R3
OpenFlow	N	N	N	N	Y	N	N	N	N	N
OV Cirrus - Zero touch provisioning	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	8.7R2	8.7R2	N
OV Cirrus - Configurable NAS Address	8.7R2	8.5R4	8.5R4	8.9R2	8.5R4	8.7R1	8.5R4	8.5R4	8.7R1	8.5R4
OV Cirrus - Default Admin Password Change	8.7R2	8.5R4	8.5R4	8.9R2	8.5R4	8.7R1	8.5R4	8.5R4	8.7R1	8.5R4

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
OV Cirrus - Managed	8.7R2	8.5R4	8.5R4	8.9R2	8.5R4	8.7R1	8.5R4	8.5R4	8.7R1	8.5R4
OVSDB	N	N	N	N	N	N	N	8.7R1	N	N
Package Manager	8.7R2	8.6R2	8.6R2	8.9R2	8.6R2	8.7R1	8.6R2	8.6R2	8.7R1	8.6R2
Readable Event Log	8.7R2	8.6R1	8.6R1	8.9R2	8.6R1	8.7R1	8.6R1	8.6R1	8.7R1	8.6R1
Remote Chassis Detection (RCD)	N	N	N	N	8.6R2	8.7R1	N	N	8.7R1	Y
SAA	8.7R2	8.5R1	8.9R1 Metro	8.9R2	Y	8.7R2	Y	8.7R1	8.7R1	Y
SAA SPB	N	N	N	N	Y	8.7R2	Y	8.7R1	8.7R1	8.6R2
SAA UNP	N	Y	N	N	Y	N	Y	N	N	N
Signed AOS Image	8.10R1	8.10R1	8.10R1	8.9R4	8.10R1	8.10R1	8.10R1	8.10R1	8.10R1	8.10R1
SNMP v1/v2/v3	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
Thin Client	8.8R1	8.8R1	8.8R1	8.9R2	8.8R1	8.8R1	8.8R1	8.8R1	8.8R1	8.8R1
U-boot Enable/Disable/Authenticate	8.7R3	8.7R3	8.7R3	8.9R2	8.7R3	N	8.7R3	N	N	8.7R3
UDLD	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	N	X48C4E	EA
USB Disaster Recovery	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1 (onie)	Y	8.7R1 (onie)	8.7R1 (onie)	Y
USB Flash (AOS)	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	N	N	N
Virtual Chassis (VC)	8.7R2	8.5R2	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y (9907) N (9912)
Virtual Chassis Split Protection (VCSP)	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
VRF	N	N	N	8.9R4	Y	8.7R1	Y	8.5R2	8.7R1	Y
VRF - IPv6	N	N	N	8.9R4	Y	8.7R1	Y	8.5R2	8.7R1	Y
VRF - DHCP Client	N	N	N	8.9R4	Y	8.7R1	Y	8.5R2	8.7R1	Y
Web Services & CLI Scripting	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.7R1	8.7R1	Y
Layer 3 Feature Support										
ARP	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
BFD	N	N	N	N	Y	8.7R1	Y	8.5R2	8.7R1	Y
BGP	N	N	N	N	Y	8.7R1	Y	8.5R2	8.7R1	Y

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6900- V72/ C32	6900- X48C6/ T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
BGP-EVPN	N	N	N	N	N	N	N	N	8.10R1	N
DHCP Client / Server	8.7R2	8.6R1	Y	8.9R2	Y	8.7R1	Y	8.5R4	8.7R1	Y
DHCP Relay	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R4	8.7R1	Y
DHCPv6 Server	N	N	N	N	Y	8.7R1	Y	8.7R1	8.7R1	Y
DHCPv6 Relay	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.7R1	8.7R1	Y
DHCP Snooping / IP Source Filtering	8.7R2	8.5R4	Y	8.9R2	Y	8.7R1	Y	8.6R2	8.7R1	Y
ECMP	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
VxLAN EVPN	N	N	N	N	N	N	N	N	8.10R1	N
IGMP v1/v2/v3	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
GRE Tunneling	N	N	N	8.9R4 ⁶	Y	8.7R1	Y	8.5R2	8.7R1	8.5R2
IP-IP Tunneling	N	N	N	8.9R4 ⁶	Y	8.7R1	Y	8.5R2	8.7R1	8.5R2
IPv6	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
IPv6 - DHCPv6 Snooping	8.7R2	8.6R1	8.6R1	8.9R2	8.5R3	8.7R1	8.5R4	8.6R2	8.7R1	8.7R1
IPv6 - Source filtering	8.7R2	N	8.6R1	8.9R2	8.5R3	8.7R1	8.5R4	8.6R2	8.7R1	8.7R1
IPv6 - DHCP Guard	EA	EA	EA	8.9R2	EA	N	EA	N	N	N
IPv6 - DHCP Client Guard	EA	EA	EA	8.9R2	EA	N	EA	N	N	N
IPv6 - RA Guard (RA filter)	Y	Y	8.5R2	8.9R2	Y	8.7R1	Y	Y	Y	Y
IPv6 - DHCP relay and Neighbor discovery proxy	8.7R2	8.5R1	Y	N	Y	8.7R1	Y	N	N	Y
IP Multinetting	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
IPSec	N	N	N	N	Y	8.7R1	Y	Y	Y	N
ISIS IPv4/IPv6	N	N	N	8.9R4 ⁶	Y	8.7R1	Y	8.5R2	8.7R1	8.5R2
M-ISIS	N	N	N	N	Y	8.7R1	Y	8.5R2	8.7R1	8.5R2
OSPFv2	N	N	8.9R4 ¹	8.9R4 ⁶	Y	8.7R1	Y	8.5R2	8.7R1	Y
OSPFv3	N	N	8.9R4 ¹	8.9R4 ⁶	Y	8.7R1	Y	8.5R2	8.7R1	Y
RIP v1/v2	N	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6900- V72/ C32	6900- X48C6/ T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
RIPng	N	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
UDP Relay (IPv4)	8.7R2	8.5R4	8.5R4	8.9R2	Y	8.7R1	Y	8.5R4	8.7R1	8.5R4
UDP Relay (IPv6)	8.7R2	8.6R1	8.6R1	8.9R2	8.6R1	8.7R1	8.6R	8.6R1	8.7R1	8.6R1
VRRP v2	8.7R2	8.5R2	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
VRRP v3	8.7R2	8.5R2	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
Server Load Balancing (SLB)	N	N	N	N	Y	8.9R4	Y	8.9R4	8.9R4	N
Static routing	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
Multicast Features										
DVMRP	N	N	N	N	Y	8.7R1	Y	8.5R2	8.7R1	N
IP Multicast VLAN (IPMVLAN)	N	8.9R3	8.9R3 Metro	8.9R3	N	N	N	N	N	N
IPv4 Multicast Switching	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
Multicast *,G	8.7R2	Y	8.5R2	8.9R2	8.5R2	8.7R1	Y	8.5R2	8.7R1	Y
IPv6 Multicast Switching	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
PIM-DM	N	N	8.10R1 ⁶	8.9R4 ⁶	Y	8.7R1	Y	8.5R2	8.7R1	Y
PIM-SM	N	N	8.10R1 ⁶	8.9R4 ⁶	Y	8.7R1	Y	8.5R2	8.7R1	Y
PIM-SSM	N	N	8.10R1 ⁶	8.9R4 ⁶	Y	8.7R1	Y	8.5R2	8.7R1	Y
PIM-SSM Static Map	N	N	N	N	N	N	N	N	N	N
PIM-BiDir	N	N	8.10R1 ⁶	8.9R4 ⁶	Y	8.7R1	Y	8.5R2	8.7R1	Y
PIM Message Packing	N	N	8.10R1 ⁶	8.9R4 ⁶	8.6R1	8.7R1	N	8.6R1	8.7R1	N
PIM - Anycast RP	N	N	8.10R1 ⁶	8.9R4 ⁶	8.6R2	8.7R1	8.6R2	8.6R2	8.7R1	8.6R2
Monitoring/Troubleshooting Features										
Ping and traceroute	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
Policy based mirroring	N	N	N	N	Y	8.7R1	Y	8.7R1	8.7R1	8.5R4
Port mirroring	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
Port monitoring	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
Port mirroring - remote	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.7R2	8.7R2	8.6R1
Port mirroring - remote over linkagg	N	N	8.9R3	N	Y	8.7R1	Y	8.7R2	8.7R2	8.6R1
RMON	8.7R2	8.5R1	Y	8.9R2	Y	8.8R2	Y	8.8R2	8.8R2	N
SFlow	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.7R1	8.7R1	Y
Switch logging / Syslog	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
TDR	8.9R3	8.9R3	8.9R3	N	Y	8.9R3	Y	N	N	N
Layer 2 Feature Support										
802.1q	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
DHL	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	N	Y	N
ERP v2	8.9R3	8.5R1	8.5R2	8.9R2	Y	8.7R1	Y	8.7R1	8.7R1	8.5R3
HAVLAN	N	EA	N	N	Y	8.8R1	Y	8.6R2	8.7R1	EA
Link Aggregation (static and LACP)	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
LLDP (802.1ab)	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
Loopback detection - Edge (Bridge)	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.6R2	8.7R1	Y
Loopback detection - SAP (Access)	N	N	N	N	Y	8.7R1	Y	8.6R2	8.7R1	Y
MAC Forced Forwarding / Dynamic Proxy ARP	8.7R2	8.7R1	N	8.9R2	8.6R1	N	8.6R1	N	N	N
MPLS	N	N	N	N	N	8.9R3	N	N	N	N
MRP	N	8.7R2	N	N	N	N	8.7R2	N	N	N
Port mapping	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	N
Private VLANs (PVLAN)	N	N	N	N	Y	8.7R2	Y	N	8.7R2	N
SIP Snooping	N	N	N	N	Y	N	N	N	N	N
Spanning Tree (1X1, RSTP, MSTP)	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
Spanning Tree (PVST+, Loop Guard)	N	Y	Y	8.9R2	Y	Y	Y	Y	Y	Y
MVRP	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R4	8.7R1	Y
SPB ²	N	N	N	N	Y	8.7R1	Y	8.5R2	8.7R1	Y

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
SPB - Over Shared Ethernet	N	N	N	N	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1
SPB - HW-based LSP flooding	N	N	N	N	8.6R1	N	8.6R1	N	N	8.5R4
QoS Feature Support										
802.1p / DSCP priority mapping	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
IPv4	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
IPv6	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
Auto-Qos prioritization of NMS/IP Phone Traffic	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
Auto-Qos - New MAC range	8.7R2	8.5R2	8.5R2	8.9R2	8.5R2	8.7R1	8.5R2	8.5R2	8.7R1	8.5R2
Groups - Port	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
Groups - MAC	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
Groups - Network	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
Groups - Service	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
Groups - Map	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
Groups - Switch	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
Groups - VLAN	8.10R1	8.10R1	8.10R1	8.10R1	8.10R1	8.10R1	8.10R1	8.10R1	8.10R1	8.10R1
Ingress/Egress bandwidth limit	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
Per port rate limiting	N	N	N	N	Y	8.7R1	Y	8.5R2	8.7R1	N
Policy Lists	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.7R1	8.7R1	Y
Policy Lists - Egress	N	N	N	N	Y	8.7R1	Y	8.7R1	8.7R1	N
Policy based routing	N	N	N	8.9R4	Y	8.7R1	Y	8.6R2	8.7R1	8.9R4
Tri-color marking	N	N	N	N	Y	8.7R1	Y	N	N	N
QSP Profiles 1	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
QSP Profiles 2/3/4	N	N	N	QSP-2 Only	Y	QSP-2 only	Y	QSP-2 only	QSP-2 only	N
QSP Profiles 5	8.7R2	8.5R1	Y	N	8.7R1	8.7R1	8.7R1	N	N	Y
RoCEv2	N	N	N	N	N	N	N	8.7R2	N	N

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
Custom QSP Profiles	8.7R2	Y	Y	8.9R2	Y	Y	Y	Y	Y	Y
GOOSE Messaging Prioritization	N	8.7R1	N	N	N	N	8.7R1	N	N	N
Metro Ethernet Features										
CPE Test Head	N	8.6R1	8.9R1 Metro	8.9R2	N	N	N	N	N	N
Ethernet Loopback Test	N	Y	8.9R1 Metro	8.9R2	8.6R1	8.7R1	8.6R1	N	N	N
Ethernet Services (VLAN Stacking)	N	8.5R1	8.9R1 Metro	8.9R2	Y	8.7R2	Y	8.5R4	8.7R1	N
Ethernet OAM (ITU Y1731 and 802.1ag)	N	8.5R1	8.9R1 Metro	8.9R2	Y	8.7R1	Y	8.7R1	8.7R1	EA
EFM OAM / Link OAM (802.3ah)	N	8.6R1	8.9R1 Metro	8.9R2	8.5R4	8.7R2	8.5R4	N	N	N
PPPoE Intermediate Agent	N	8.6R1	8.9R1 Metro	8.9R2	N	N	8.6R1	N	N	N
1588v2 End-to-End Transparent Clock	N	8.5R1	8.7R2	N	Y	8.9R3	Y	N	8.9R3 (except C32E)	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	N	N	N	N
Access Guardian / Security Features										
802.1x Authentication	8.7R2	8.5R2	Y	8.9R2	Y	8.7R1	Y	8.7R1	8.7R1	Y
Access Guardian - Bridge	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.6R1	8.7R1	Y
Access Guardian - Access	N	N	N	N	Y	8.7R1	Y	8.5R4	8.7R1	Y
Application Fingerprinting	N	N	N	N	N	N	N	N	N	N
Application Monitoring and Enforcement (Appmon)	N	N	N	N	Y	8.7R2	N	N	N	N
ARP Poisoning Protection	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R2	8.7R1	Y
BYOD - COA Extension support for RADIUS	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	8.6R2	8.7R1	Y
BYOD - mDNS Snooping/Relay	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	8.6R2	8.7R1	Y
BYOD - UPNP/DLNA Relay	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	8.6R2	8.7R1	Y
BYOD - Switch Port location information pass-through in RADIUS requests	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	8.6R2	8.7R1	Y
Captive Portal	8.7R2	8.5R4	Y	8.9R2	Y	8.7R1	Y	8.6R2	8.7R1	Y
IoT Device Profiling	8.7R2	8.5R2	8.5R2	8.9R2	8.5R2	8.7R1	8.5R2	8.6R1	8.7R1	8.5R2

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
IoT Device Profiling (IPv6)	8.7R2	8.7R1	8.7R1	8.9R2	8.7R1 ⁵	8.9R3	8.7R1 ⁵	8.9R3	8.9R3	8.7R1
Directed Broadcasts - Control	8.7R2	8.5R2	8.5R2	8.9R2	8.5R2	8.7R1	8.5R2	8.7R1	8.7R1	Y
Interface Violation Recovery	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.7R1	8.7R1	Y
Kerberos Snooping (services)	8.7R2	Y	8.6R2	N	8.6R2	Y	8.6R2	8.6R2	Y	8.6R2
L2 GRE Tunnel Access (Edge) (bridge ports)	N	N	Y	N	Y	8.9R1	Y	N	N	Y
L2 GRE Tunnel Access (Edge) (access ports)	N	N	N	N	8.6R1	8.9R1	8.6R1	8.7R1	8.7R2	8.6R1
L2 GRE Tunnel Aggregation	N	N	N	N	Y	8.9R1	Y	8.7R1	8.7R2	Y
Learned Port Security (LPS)	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.5R4	8.7R1	Y
MACsec ³	N	8.5R1	8.5R4	N	Y	8.7R1	N	N	X48C4E	8.5R2
MACsec MKA Support ³	N	8.5R2	8.5R4	N	8.5R2	8.7R1	N	N	X48C4E	8.5R2
MACsec on Network Port for SPB/L2GRE/VxLAN	N	N	N	N	8.9R1 (6860E)	8.9R1	N	N	8.9R1 (X48C4E)	N
Quarantine Manager	N	8.7R2	8.7R2	8.9R2	Y	8.7R2	Y	8.7R2	8.7R2	8.7R2
RADIUS - RFC-2868 Support	8.7R2	8.5R4	8.5R4	8.9R2	8.5R4	8.7R1	8.5R4	8.5R4	8.7R1	8.5R4
Role-based Authentication for Routed Domains	N	N	N	N	8.5R4	8.7R1	8.5R4	8.6R1	8.7R1	8.5R4
Storm Control (flood-limit)	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	Y	8.7R1	Y
Storm Control (Unknown unicast with action trap/shutdown)	N	N	N	N	Y	N	Y	N	N	N
TACACS+ Client	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.6R1	8.7R1	Y
TACACS+ command based authorization	8.7R2	N	N	8.9R2	Y	8.7R1	Y	8.7R2	8.7R2	N
TACACS+ - IPv6	8.7R3	8.7R3	8.7R3	8.9R2	8.7R3	8.7R3	8.7R3	8.7R3	8.7R3	8.7R3
PoE Features										
802.3af and 802.3at	8.7R2	8.5R1	Y	N	Y	8.7R1	Y	N	N	Y
802.3bt	8.7R2	Y	8.6R2	N	N	8.7R1	N	N	N	N
Auto Negotiation of PoE Class-power upper limit	8.7R2	8.5R1	Y	N	Y	8.7R1	Y	N	N	Y
Display of detected power class	8.7R2	8.5R1	Y	N	Y	8.7R1	Y	N	N	Y
LLDP/802.3at power management TLV	8.7R2	8.5R1	Y	N	Y	8.7R1	Y	N	N	Y

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
HPOE support	8.7R2 (95W)	8.5R1 (60W)	Y (95W)	N	Y (60W)	8.7R1 (95W)	Y (75W)	N	N	Y (75W)
Time Of Day Support	8.7R2	8.5R1	Y	N	Y		Y	N	N	Y
Perpetual PoE	8.7R2	N	N	N	Y	Y	Y	N	N	N
Fast PoE	8.7R2	N	N	N	Y	Y	Y	N	N	N
Delayed Start	8.9R3	8.9R3	8.9R3	N	N	N	N	N	N	N
Data Center Features (License May Be Required)										
CEE DCBX Version 1.01	N	N	N	N	N	N	N	N	N	N
Data Center Bridging (DCBX/ETS/PFC)	N	N	N	N	N	N	N	N	N	N
EVB	N	N	N	N	N	N	N	N	N	N
FCoE / FC Gateway	N	N	N	N	N	N	N	N	N	N
VxLAN ⁴	N	N	N	N	N	8.8R1	N	8.5R3	8.8R1	N
VM/VxLAN Snooping	N	N	N	N	N	N	N	N	N	N
FIP Snooping	N	N	N	N	N	N	N	N	N	N
Notes: 1. OS6560 supports 2 OSPF areas with Advanced Routing license. 2. See protocol support table in Appendix C. 3. Site license required beginning in 8.6R1. 4. L2 head-end only on OS6900-V72/C32. 5. HTTP IPv6 only supported on OS6860(E) and OS6865 6. Advanced Routing license required.										

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 and Dynamic (128-bit) modes
OS99-CMM2	Not Supported
OS99-GNI-48/P48	10M/100M/1G ports - Static and Dynamic (128-bit) modes
OS99-XNI-48/P48	10G ports - Static and Dynamic (128-bit) modes
OS99-XNI-U48	10G ports - Static and Dynamic (128-bit) modes
OS99-XNI-P48Z16	1G/2.5G/5G/10G (16x) - Static and Dynamic (128-bit) modes 1G/10G (32x) - Static and Dynamic (128-bit) modes
OS99-GNI-U48	1G ports - Static and Dynamic (128-bit) modes
OS99-XNI-U24	10G ports - Static and Dynamic (128-bit) modes
OS99-XNI-P24Z8	1G/2.5G/5G/10G (8x) - Static and Dynamic (128-bit) modes 1G/10G (16x) - Static and Dynamic (128-bit) modes
OS99-XNI-U12Q	10G / 4x10G Uplink - Static and Dynamic (128-bit) modes
OS99-XNI-UP24Q2	10G(Fiber)/4x10G Uplink - Static and Dynamic (128-bit) modes 10G (Copper) - Static and Dynamic (128-bit) modes
OS99-CNI-U8	Not Supported
OS99-CNI-U20	40G/100G - Static and Dynamic (128-bit) modes
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 Tandem Mode	8.5R4	8.7R2	8.8R1	8.8R1	8.8R1	8.8R1	8.9R1

External Loopback Support								
	OmniSwitch 9900	OmniSwitch 6860/6865	OmniSwitch 6860N	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	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
RIP v1/v2	8.5R4	Y	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
OSPF	8.5R4	Y	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
BGP	8.5R4	Y	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
VRRP	8.6R1	8.5R4	8.7R1	8.7R1	8.7R2	8.7R2	8.7R3	8.9R1
IS-IS	Y	Y	Y	Y	Y	8.7R2	8.7R3	8.9R1
PIM-SM/DM	8.5R4	Y	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
DHCP Relay	8.5R4	8.5R4	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
UDP Relay	8.5R4	8.5R4	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
DVMRP	N	N	N	N	N	N	N	N
BFD	Y	Y	Y	Y	Y	8.7R2	8.7R3	8.9R1
IGMP Snooping	8.5R4	Y	8.7R1	8.6R1	8.7R1	8.7R2	8.7R3	8.9R1
IP Multicast Headend Mode	8.5R4	Y	8.7R1	8.6R1	8.7R1	8.7R2	8.7R3	8.9R1
IP Multicast Tandem Mode	8.5R4	Y	8.7R1	8.6R1	Y	Y	Y	8.9R1
IPv6 Protocols								
Static Routing	8.5R4	Y	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
RIPng	8.5R4	Y	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
OSPFv3	8.5R4	Y	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
BGP	8.5R4	Y	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
VRRPv3	8.5R4	8.5R4	8.7R1	8.7R1	8.7R2	8.7R2	8.7R3	8.9R1
IS-IS	Y	Y	Y	Y	Y	8.7R2	8.7R3	8.9R1
PIM-SM/DM	8.5R4	8.5R4	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
DHCP Relay	8.6R1	8.6R1	8.7R1	8.6R1	8.7R1	8.7R2	8.7R3	8.9R1
UDP Relay	8.6R1	8.6R1	8.7R1	8.6R1	8.7R1	8.7R2	8.7R3	8.9R1
BFD	Y	Y	Y	Y	Y	8.7R2	8.7R3	8.9R1
IPv6 MLD Snooping	8.5R4	Y	8.7R1	Y	8.7R2	8.7R2	8.7R3	8.9R1
IPv6 Multicast Headend Mode	8.5R4	Y	8.7R1	Y	8.7R2	8.7R2	8.7R3	8.9R1
IPv6 Multicast Tandem Mode	8.5R4	Y	8.7R1	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						Services	Num	Tandem
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 8.10R1 (GA)
OS6360	8.9.94.R04 (Major GA) 8.9.221.R03 (Major GA) 8.9.107.R02 (Minor GA) 8.9.73.R01 (Major GA)
OS6465	8.9.94.R04 (Major GA) 8.9.221.R03 (Major GA) 8.9.107.R02 (Minor GA) 8.9.73.R01 (Major GA)
OS6560	8.9.94.R04 (Major GA) 8.9.221.R03 (Major GA) 8.9.107.R02 (Minor GA) 8.9.73.R01 (Major GA)
OS6570M	8.9.94.R04 (Major GA) 8.9.221.R03 (Major GA) 8.9.107.R02 (Minor GA) 8.9.63.R02 (Major GA)
OS6860(E)	8.9.94.R04 (Major GA) 8.9.92.R04 (Major GA) 8.9.221.R03 (Major GA) 8.9.107.R02 (Minor GA) 8.9.73.R01 (Major GA)
OS6860N	8.9.94.R04 (Major GA) 8.9.92.R04 (Major GA) 8.9.221.R03 (Major GA) 8.9.107.R02 (Minor GA) 8.9.73.R01 (Major GA)
OS6865	8.9.94.R04 (Major GA) 8.9.92.R04 (Major GA) 8.9.221.R03 (Major GA) 8.9.107.R02 (Minor GA) 8.9.73.R01 (Major GA)
OS6900- X20/X40/T20/T40/Q32/X72	No longer supported
OS6900-V72/C32/C32E X48C6/T48C6/V48C8/ X24C2/T24C2	8.9.94.R04 (Major GA) 8.9.92.R04 (Major GA) 8.9.221.R03 (Major GA) 8.9.107.R02 (Minor GA) 8.9.78.R01 (Major GA)
OS6900-X48C4E	8.9.94.R04 (Major GA) 8.9.92.R04 (Major GA)
OS9900 (OS9907)	8.9.94.R04 (Major GA) 8.9.221.R03 (Major GA)

- ISSU from 8.9.92.R04 is not supported on platforms: OS6560, OS6465, OS6570M, OS9900, OS6360 (due to SSH issue on build 8.9.92.R04)
- OS6900-X48C4E VC support introduced in 8.9.R04.

8.10R1 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-V72 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.
- 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-V72/C32/X48C6/T48C6/X48C4E/V48C8 - Yos.img.
 - Refer to [Appendix H](#) for recommended CPLD upgrades. AOS must be upgraded prior to upgrading the CPLD.
- 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
-----+-----+-----+-----
Yos.img           8.10.102.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 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.
- OS6570M - Wos.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.
- 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-V72/C32/X48C6/T48C6/X48C4E/V48C8 - Yos.img.
 - Refer to [Appendix H](#) for recommended CPLD upgrades. AOS must be upgraded prior to upgrading the CPLD.
- 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

(Note: If upgrading a standalone (VC-of-1), modular OS9900 with dual CMMs, skip to step 7).

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
Yos.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      Config      Oper      System
-----+-----+-----+-----+-----+-----
Chas ID Pri  Group  MAC-Address  Ready
-----+-----+-----+-----+-----+-----
1      Master    Running     1      100    19    e8:e7:32:b9:19:0b  Yes
2      Slave     Running     2      99     19    e8:e7:32:b9:19:43  Yes
```

10. Verify the Software Upgrade

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

```
OS6900-> show microcode
/flash/working
Package      Release      Size      Description
-----+-----+-----+-----
Yos.img      8.10.102.R01 239607692 Alcatel-Lucent OS
```

11. Certify the Software Upgrade

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

```
OS6900-> write memory flash-synchro

-> 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
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	U-boot 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	U-boot 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 pmds
	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) Supported on 1G and 10G ports only. Not supported 2.5G ports.
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	U-boot update for CRAOS8X-24464, ability to disable / authenticate U-boot access.
	U-boot Version	8.7.30.R03
	Platforms	OS6360, 6465, 6560, 6860, 6865, 9900. (Not applicable for platforms that use ONIE)
8.8R1 Release		
Boot from USB	Description	U-boot update to allow switch to boot from USB.
	U-boot Version	8.8.33.R01
	Platforms	OS6465, OS6865
8.8R2 Release		
Future compatibility	Description	U-boot/FPGA update to allow future CMM2/OS9912 NI compatibility.
	U-boot/FPGA Versions	See OS9900 Table for versions.
	Platforms	9907
8.9R1 Release		
N/A	There are no U-boot/FPGA upgrade requirements in this release.	
8.9R2 Release		
Fan Speed	Description	Reduced fan speed at boot-up
	FPGA Version	0.20
	Platforms	OS6360-(P)24/(P)48/PH48
CRAOS8X_35470 and CPLD Support	Description	U-boot fix for NAND flash bad file system block. Support of Gowin CPLD ¹
	U-boot	8.9.85.R02
	Platforms	OS6360 (All)
CPLD Support	Description	Support of Gowin CPLD ¹
	U-boot	8.9.92.R02
	Platforms	OS6570M-12/12D/U28
CRAOS8X_35470	Description	U-boot fix for NAND flash bad file system block
	U-boot/FPGA Versions	8.9.85.R02
	Platforms	OS6465 (All), OS6560-(P)24X4/(P)48X4/X10
1. Existing switches do not contain the new CPLD component and do not need to upgrade. Switches with the new CPLD component will ship from the factory with the correct version.		
8.9R3 Release		
CRAOS8X-40924	Description	Address issue when disabling U-boot access.
	U-boot Version	8.9.139.R03
	Platforms	OS6570M-12/12D/U28
Power Supply Interrupt	Description	Address power supply interrupt issue.
	FPGA Version	0.12
	Platforms	OS6570M-U28

8.9R4 Release		
Signed AOS Images	Description	Adds support for signed images when used with AOS 8.9R4 GA release.
	U-boot Version	8.9.70.R04
	Platforms	OS6570M-12/12D/U28
8.10R1 Release		
CRAOS8X-43592	Description	1G/10G SFP not recognized.
	U-boot Version	XNI_U24 - 2.12.0 XNI_U48 - 2.12.0 GNI_U48 - 1.8.0 CNI_U8 - 1.10
	Platforms	OS9907/OS9912

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_8757
- U-boot.8.9.R04.70.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_8757
Parse /flash/fpga_kit_8757
fpga file: OS6360-10_CPLD_V19_20230110.vme
Please wait...
fpga file: OS6360-10_CPLD_V19_20230110.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.8.9.R04.70.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. Follow the guidelines in the General Upgrade Requirements and Best Practices appendix prior to upgrading.

8.8R2 Release		
OS6860N-P48M/P48Z/P24M/P24Z		
CRAOS8X-29731 / 30471	Description	OS6860N power supplies
	CPLD File	os6860n_p48m_p48z_u28_maincpu_20220318.updater os6860n_p24m_p24z_maincpld_22020309.updater
8.9R1 Release		
OS6900-T48C6		
CRAOS8X-30098	Description	Fixed I2C lockup issue on CPU board. (Please refer to CRAOS8X-30098 for additional details)
	CPLD File	denverton_cpucpld_v0b.02.0eh_20211124.jbc.updater
No CR	Description	Improved power down sequence when PSU shut down.
	CPLD File	os6900_t48c6_mainpld_v1.03.02.04.jbc.updater
OS6900-X48C6		
CRAOS8X-30098	Description	Fixed I2C lockup issue on CPU board. (Please refer to CRAOS8X-30098 for additional details)
	CPLD File	denverton_cpucpld_v0b.02.0eh_20211124.jbc.updater
No CR	Description	Improved power down sequence when PSU shut down.
	CPLD File	os6900_x48c6_mainpldall_bp_v1.03.02.02h.jbc.updater
OS6900-X48C4E		
CRAOS8X-30098	Description	Fixed I2C lockup issue on CPU board. (Please refer to CRAOS8X-30098 for additional details)
	CPLD File	OS6900_XC48C4E_MAIN_CPU_FAN_CPLD_2e3228_20220322.updater
8.9R4 Release		
OS6900-X48C4E		
CRAOS8X-43968	Description	Fixed temperature error on OS6900-X48C4E (Hardware revision: 6) with a single power supply.
	CPLD File	updater_kit_8629 (version 2.15)
8.10R1 Release		
N/A	Description	N/A
	CPLD File	N/A
<p>Notes:</p> <ol style="list-style-type: none"> 1. Upgrading the CPLD on ONIE-based models using an updater kit is supported beginning with AOS Release 8.9.R03. 2. The updater kit contains all the necessary individual updater files. 3. CPLD versions are compatible with previous AOS releases. Downgrading to a previous AOS release is supported: <ol style="list-style-type: none"> a. Backup the configuration files from previous release. b. Upgrade to AOS Release 8.9.R03. c. Upgrade the CPLD. d. Downgrade to previous release. (ISSU is not supported when downgrading AOS) e. Restore the configuration. 		

Note: AOS must be upgraded to 8.10R1 prior to performing a CPLD upgrade using the updater kit.

ONIE-based platforms contain multiple CPLDs. The upgrade process will pick the correct updater file from the kit based on the platform and the CPLD type. The procedure will check for a version mismatch and upgrade the CPLD one at a time (i.e. Main board or CPU board). The CPLD will be upgraded one at a time so it may be necessary to run the command multiple times. If no upgrade is required, the command will display a message indicating there are no pending upgrades. See example below (file and product names will vary).

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 kit, for example.

- CPLD Kit - updater_kit_8629

2. Ensure the configuration is certified and synchronized prior to upgrading the CPLD. It's recommended to have a console connection in case there are any issues during the CPLD upgrade procedure.

3. FTP (Binary) the updater kit to the `/flash` directory on the primary CMM.

4. Enter the following to upgrade the CPLD. Use the 'all' parameter to upgrade each element in a VC, for example:

```
-> update fpga-cpld all 1/1 file updater_kit_8629
Starting CMM 1/1  FPGA Upgrade
CMM 1/1
starting onie update
Removing firmware update results: OS6900_XC48C4E_MAIN_CPU_FAN_CPLD_2f3238_20240315.updater
Staging firmware update: /flash/ OS6900_XC48C4E_MAIN_CPU_FAN_CPLD_2f3238_20240315.updater
onie update successful
Successfully updated
Reload required to activate new firmware.
```

4. If multiple CPLDs have to be upgraded the command must be run several times.

5. Once the CPLDs have been upgraded a manual reload is required. This will boot each of the units to "ONIE: Update ONIE" mode. **Note:** Do not press any keys while in ONIE mode.





6. The switch will update the CPLD and then reboot to the *Certified* directory. **Note:** The switch will not boot back to the last running directory.






7. OS6860N models (except U28) will then automatically power cycle. For all other models manually power cycle the units to refresh the CPLD image. The switch will then again boot back to the *Certified* directory.





8. Reload to the running-directory.

Appendix I: Fixed Problem Reports




The following problem reports were closed in this release.





CR/PR NUMBER	Description
<p>Case: 00733478 CRAOS8X-43718</p>	<p>Summary: Unable to remove the interface from the policy port group. policy port group “testing” no 1/1/45 ERROR: “testing”: Groups must have at least one entry</p> <p>Explanation: The port bitmap comparison to check if ports are part of a port-group was only to check for the first 32 user ports of the device. Any port-group policy having ports 33 or above was not compared to whether its bitmap was set or not and hence was returning an error saying the group should have at least one member. Changes were added to check all the bits in the port bitmap instead of checking only the first 32 bits and it is fixed in 8.10R01.</p> <p> Click for Additional Information</p>
<p>Case: 00750068 CRAOS8X-45604</p>	<p>Summary: The OS6900 core switch stuck in the boot loop during the upgrade from 8.7.354.R01 to 8.9.94.R04.</p> <p>Explanation: The root cause of the issue is due to the configuration of "debug ip bgp adv-loopback0 enable". Fix is given in 8.10R01</p> <p> Click for Additional Information</p>
<p>Case: 00719941, 00742179 CRAOS8X-42339, CRAOS8X-44429</p>	<p>Summary: Qos port violation noticed for TCP 53 and TCP 179 on the UserPorts. When switch receives the TCP RST ACK packets with source port 53 (for DNS) and 179(BGP), the switch shutdowns the port for violation. qos trust-ports user-port shutdown dns-reply bgp</p> <p>Explanation: The fix is given in AOS 8.10R01.</p> <p> Click for Additional Information</p>
<p>Case: 00734062, 00721704 CRAOS8X-43714, CRAOS8X-42394</p>	<p>Summary: CVE-2024-0727, CVE-2023-5678: Vulnerability Analysis for AOS 8X switches.</p> <p>Explanation: The vulnerability has been resolved in OpenSSL version 3.0.13. Fix in provided in 8.10R01.</p> <p> Click for Additional Information</p>
<p>Case: 00664503 CRAOS8X-36871</p>	<p>Summary: CVE-2021 41617 & CVE-2021-36368 need vulnerability analysis for AOS 8.X switches.</p> <p>Explanation: This vulnerability is fixed in AOS 8.10R01.</p>






	<p> Click for Additional Information</p>
<p>Case: 00741513 CRAOS8X-44482</p>	<p>Summary: 802.1x supplicant clients are not responding to EAP ID requests within 3 seconds for 3 retries attempted from AOS switch.</p> <p>Explanation: The switch sends 3 EAP (max-req=3) requests each second to determine if the device is supplicant or non-supplicant. If no response is received, it is considered a non-supplicant.</p> <p>The other timers, like Tx-timeout and supplicant-timeout, are used when the PC responds to the EAP.</p> <p>Fix is given to allow 802.1x supplicant PCs to take more retries to respond to EAP ID request of AOS switch before considering this client as non-supplicant. Max-req can now be set to 50 times while the default max-req is 2 times.</p> <p>- unip port <port> 802.1x-authentication max-req 50</p> <p> Click for Additional Information</p>
<p>Case: 00708315 CRAOS8X-41378</p>	<p>Summary: Vulnerability check of CVE-2023-24329 for AOS 8X switches.</p> <p>Explanation: Python version will be upgraded to 3.11.4 from AOS 8.10R01.</p> <p> Click for Additional Information</p>
<p>Case: 00719316 CRAOS8X-42207</p>	<p>Summary: Vulnerability check of CVE-2023-5363 for AOS 8X switches.</p> <p>Explanation: OpenSSL upgraded to 3.0.13 version that has the fix for this CVE. Fix is given in 8.10R01.</p> <p> Click for Additional Information</p>
<p>Case: 00734322, 00745117 CRAOS8X-43897, CRAOS8X-44695</p>	<p>Summary: There is no CVLAN tag in the DHCP discover packets egressing on the NNI Port of the switch.</p> <p>Explanation: The fix will be available in AOS release 8.10R01.</p> <p> Click for Additional Information</p>






<p>Case: 00739642 CRAOS8X-44869</p>	<p>Summary: This is about an error message "cannot enable sflow sampler on the port" received while trying to configure "sflow sampler" on a linkagg with only a single port 1/1/49A on an OS6900-X48C6 switch.</p> <p>Explanation: The fix will be available in AOS release 8.10R01.</p> <p> Click for Additional Information</p>
<p>Case: 00758170 CRAOS8X-45639</p>	<p>Summary: Chassis.2 status is showing "Failure-Shutdown" on OS6560-48X4 switches in VC after upgrading to 8.9.94.R04 from 8.9R03.</p> <p>Explanation: This issue has been reported only in AOS 8.9R04 with FIPS mode enabled. This issue will be fixed in AOS 8.10R01.</p> <p><i>Workaround:</i> Disable FIP and then perform VC upgrade.</p> <p> Click for Additional Information</p>
<p>Case: 00728419 CRAOS8X-43326</p>	<p>Summary: IP multicast VLAN (IPMVLAN) is not working. IGMP queries ingress on UNI with CVLAN ID tag. However multicast data traffic is not egress on UNI port with CVLAN ID tag. CVLAN tag translate was not working for IPMVLAN implementation. SVLAN and CVLAN are different VLAN ID in this use case.</p> <p>Explanation: There are changes done in AOS 8.X IPMVLAN implementation to ensure the multicast data traffic forwarded with required CVLAN while egressing on UNI port.</p> <ol style="list-style-type: none"> 1. Same VLAN ID is used for both CVLAN and SVLAN. 2. There are 2 SAP configured for same UNI port for CVLAN tag translate to work fine. <ol style="list-style-type: none"> (i) to tag CVLAN on same SAP service (ii) to tag IPMVLAN on another SAP service. <p>The fix will be available in AOS release 8.10R01.</p> <p> Click for Additional Information</p>
<p>Case: 00726097 CRAOS8X-42858</p>	<p>Summary: There are logs as given below when using sflow agent.</p> <p>pd:pd_free: Cpps trying to free a buffer it doesn't own (state=Free owner=None prev owner=Pd)</p> <p>Explanation: There are double free of the PD (Packet Driver) buffer when the packet driver queue is full. When the queue is full, the buffer is freed, and the same buffer is assigned back to the client list.</p> <p>Fix is done to remove the extra free of freeing the packet driver buffer in AOS 8.10R01.</p> <p> Click for Additional Information</p>





Case: 00731546 CRAOS8X-43499	Summary: Vulnerability check of CVE-2023-6129 for AOS 8.X switches. Explanation: Fix is available in 8.10R01 GA. 🔒 Click for Additional Information
Case: 00747235 CRAOS8X-45002	Summary: The information displayed is wrong in the OS6900-V48C8 for the command: ->show interfaces 1/1/57. The information port 51 details are displayed. Explanation: This is a cosmetic issue and there will be no operational impact. The cosmetic issue is fixed in AOS 8.10R01. 🔒 Click for Additional Information
Case: 00734658 CRAOS8X-43844	Summary: Random IP Phone never receives IP and continuous error "svcNi mSVC ERR SVCN:SAP:: Process SAP Cfg Entry[0] failed" in console Explanation: <ul style="list-style-type: none"> • Concurrent access to the BCM Sdk port type data structure during a link scan speed change configuration. • Returning Service Access Point details without proper cleanup creates an issue state. 🔒 Click for Additional Information
Case: 00738590 CRAOS8X-44265	Summary: 6465: PoE status "denied" for Watchnet MPIX-40IRPTZAI camera model Explanation: The Watchnet MPIX-40IRPTZAI camera model consistently displays a "Denied" status when connected to the OS6465-P6 switch across all ports. The PD is failing while class detection before assigning power. <i>OS6465 swlogd lpNi LanNi INFO: Port 1/1/1 FAULT State change 1b to 43 desc: Port is off: Class Error (Illegal class)</i> As an enhancement, the following debug has to be applied in OS6465 model running in 8.10.R01 to power up the Camera which failed with Illegal class. <i>debug lanpower slot 1/1 config ignore-class-error enable</i> 🔒 Click for Additional Information
Case: 00754049 CRAOS8X-45829	Summary: TCam NI task restarted[Failed App /bin/tcamnid] while executing tech-support-eng complete







	<p>Explanation: When there are more IP entries in the network group, OS9900's RuleIdx cannot progress to the next iteration.</p> <p>When the command "show tcam utilization resource "all-resources" active" is executed while generating tech-support-eng complete, the tcam NI task is restarted.</p> <p> Click for Additional Information</p>
<p>Case: 00752480 CRAOS8X-45639</p>	<p>Summary: 2XOS6560-24X4: Chassis-2 going to Failure-shutdown after upgrading to AOS 8.9R04.</p> <p>Explanation: When FIP configuration is enabled, FIPS mode in master and slave are not synchronized: Master have the FIP mode enabled; however, slave is missed to set the mode which is causing algorithms mismatch between ssh client and server.</p> <p>This issue is seen only in the AOS 8.9.94.R04 code.</p> <p>When FIP-mode is enabled:</p> <p>1) SSH between Master to slave will not work in the switches OS6360/OS6465/OS6560/OS9900/OS6570M [Normal switch SSH will work without any issues].</p> <p>2) If we upgrade VC from any code to 8.9.R04 with FIP mode enabled in the switches (OS6360/OS6465/OS6560/OS9900,6570M), VC won't be formed.</p> <p>The workaround is documented in 8.9.R04 release notes.</p> <p> Click for Additional Information</p>
<p>Case: 00754707 CRAOS8X-45930</p>	<p>Summary: ARP is learnt in incorrect service when MAC is learnt in correct service.</p> <p>Explanation: It has been confirmed that the issue is with the display; there will be no functional impact.</p> <p>While displaying "show arp", it is using the "Virtual Port" details which was updated with the most recent service ID.</p> <p>The fix approach is to use the variable in "ipmcm" which already knows the correct ISID value when using "show arp".</p> <p> Click for Additional Information</p>
<p>Case: 00743364 CRAOS8X-44533</p>	<p>Summary: Interface speed 1G,10G accepted in 25G speed port which causes the port not to come up in 25G speed</p> <p>Explanation:</p> <ul style="list-style-type: none"> • Speed 100M, 1G, and 10G will not be accepted when 25G SFP is connected to the port group.



	<ul style="list-style-type: none"> The following error message will be thrown in 8.10.R01 when trying to configure 100, 1G, or 10G speed in 25G port-group speed: interfaces port 1/1/1 speed 10000 ERROR: Configured Speed is not supported on this platform Using another port group to use 1G and 10G speed is suggested. <p> Click for Additional Information</p>
<p>Case: 00752681 CRAOS8X-45575</p>	<p>Summary: The output of “show configuration snapshot aaa” had user command output in CLI guide. CLI output is not expected to display the “user” command configuration. The users created in the switch are saved in userTable in the /flash/system folder and these users will not be printed in configuration snapshot commands.</p> <p>Explanation: Management and CLI guide documentation corrected in AOS 8.10R01 for “show configuration snapshot aaa”.</p> <p> Click for Additional Information</p>
<p>Case: 00746111 CRAOS8X-45219</p>	<p>Summary: Continuously noticing the “swlogd portmgrni library(HAL_lib) ERR: hal_port_interface_mode_get:18032 unit=0 dport=6 Unknown hostIf 18”</p> <p>Explanation: The error is seen when it is unable to get host interface for 20G interface. This issue is fixed in 8.10R01.</p> <p> Click for Additional Information</p>
<p>Case: 00750952 CRAOS8X-45460</p>	<p>Summary: DHCP snooping entry is not updated during re-IP or PXE process causes ISF to drop any ARP packets received from the new IP. As a result, clients on the ports will not have network connectivity.</p> <p>Explanation: Due to changes made to the DHCP server for printers and PXE devices to acquire IP addresses within a new range, clients are now unable to connect to the network after receiving their new IP addresses during the DHCP renewal process.</p> <p>Checking the DHCP snooping table on the switch reveals that it still displays the old IP addresses for the clients. Due to this conflict, IP source filtering is blocking packets from the new IP addresses of the clients. Disabling ISF on the VLAN/port is one of the work arounds.</p> <p> Click for Additional Information</p>
<p>Case: 00738222 CRAOS8X-44151</p>	<p>Summary: Different behavior of OID dot1qVlanFdbId than AOS6x and other vendors.</p> <p>Explanation: The OID dot1qVlanFdbId has been observed as behaving differently in AOS8x switches than AOS6x and other vendor switches.</p>

	<p>The index for all the VLANs is set as 1, instead of unique values of each VLAN IDs like other vendors.</p> <p> Click for Additional Information</p>
<p>Case: 00727549 CRAOS8X-42974</p>	<p>Summary: Multiarea SPB interoperability with Extreme switches.</p> <p>Explanation: when multiarea is enabled on Extreme SPB node, the new area configured is appended to default area 00 instead of overwriting it, in ALE SPB node. Extreme detects the ALE area as a loop connection and the SPB adjacency is shutdown.</p> <p> Click for Additional Information</p>
<p>Case: 00746197 CRAOS8X-44962</p>	<p>Summary: OS6900-X72: Switch uses a different "IP Inteface" for DNS Query instead of "Loopback0".</p> <p>Explanation: OS6900-X72 switch configured with service source-ip "Loopback0". Still the DNS query from the switch uses a different IP interface instead of "Loopback0" as configured.</p> <p> Click for Additional Information</p>
<p>Case: 00748200 CRAOS8X-45068</p>	<p>Summary: OS6560-P48Z16: VC-Split after the upgrade from 8.9R03 to 8.9.94.R04</p> <p>Explanation: The chassis affected are stuck in unusual boot loop and there was no login prompt even on console access. Spin locks are a synchronization mechanism which allows one process at a time to access the shared memory. OS6560 is a device with two CPU cores. During the issue state the 'spinlock backtrace tracking' got stuck and busy-locked one CPU core. This caused the other CPU to detect the stall, dump the backtrace, and hang the box.</p> <p> Click for Additional Information</p>
<p>Case: 00751395 CRAOS8X-45516</p>	<p>Summary: Mitel IP phone connected to the UNP port of OS6560-P48Z16 switch is filtered by LPS.</p> <p>Explanation: If the IP-Phone mac address is initially classified in "server-down" profile. LPS increment the bridging count of the port to 1. Later the same device is identified as IP-Phone based on LLDP info. While assigning the profile in agCmmAssignProfileToMac, the LPS Count was not decremented properly. Hence same mac was learnt in filtering as the bridge count already reached max limit of 1.</p> <p> Click for Additional Information</p>
<p>Case: 00749019 CRAOS8X-45241</p>	<p>Summary: OS6860N stops authenticating end users via RADIUS server. Access to the switch could not be established via SSH or Console prompt. Reload of switch is required to overcome this issue.</p>

	<p>Explanation: As part of the user authentication process, radCLI sends the Radius packet to the server. During this flow, while recomputing hash for the packet to be sent to the radius server, radCLI task got stuck in an infinite loop.</p> <p> Click for Additional Information</p>
<p>Case: 00753370 CRAOS8X-45732</p>	<p>Summary: AOS 8.x switches uses identical value in the 'Authenticator' field of "RADIUS-Request" packet.</p> <p>Explanation: "RADIUS-Request" packets from two different AOS 8.x switches seems to be using identical value in the 'Authenticator' field. The authenticator field hash is computed using a random number based on the time in seconds. In a time-synchronized network, when multiple switches try to send RADIUS-Request in the same second then there is high possibility for AOS switches to generate identical 'Authenticator' value.</p> <p> Click for Additional Information</p>
<p>Case: 00736076 CRAOS8X-43927</p>	<p>Summary: Write Memory failed! Unable to retrieve VCM configuration.</p> <p>Explanation: These errors are generated after executing the CLI command "write memory" and "write-memory flash-synchro" in the OS6560 switch. This issue is due to the TCP connection failure between the MIP_gw and the VCM.</p> <p> Click for Additional Information</p>
<p>Case: 00725556 CRAOS8X-42890</p>	<p>Summary: OS6860N: No connectivity on the service access port with UNP.</p> <p>Explanation: An OS6860N switch using SPB has a device connected via an ISID ##### via UNP on an interface but is not able to communicate with the network. SVC BCM error occurs when the access port is dynamically changed, causing the SAP port to become nonfunctional.</p> <p> Click for Additional Information</p>
<p>Case: 00733326 CRAOS8X-43637</p>	<p>Summary: OS6900 Traffic loss observed on unit-1 of VC due to missing vlan tag on SAP port.</p> <p>Explanation: The ICMP between client and server has around 98% loss.</p> <p>The SAP connected to router is holding the services along with specific vlan IDs.</p> <p>The pkt from client is reaching the server and response from server is reaching the VC and while exiting, it is not adding the respective vlan tag, hence client not receiving the response from the router.</p> <p> Click for Additional Information</p>

<p>Case: 00730642 CRAOS8X-43939</p>	<p>Summary: Authentication was failing for the clients connected to OS6560 switch on UNP 802.1x ports.</p> <p>Explanation: The issue was that the delay in Client responding to EAP request from switch. Due to no response from client, switch was resending the same request as duplicate and now client is responding with 2 replies. Switch was forwarding the first reply and for the RADUIS response from Server, switch was sending the duplicate response to server which is not supposed to be done.</p> <p> Click for Additional Information</p>
<p>Case: 00742719 CRAOS8X-44522</p>	<p>Summary: OS6860E Switch rebooted with new_cs PMD.</p> <p>Explanation: The switch has been restarted and new_cs PMD was generated.</p> <p>The reason for the crash was due to incorrect payload length dhcpv6 packet reception.</p> <p> Click for Additional Information</p>
<p>Case: 00747497 CRAOS8X-45011</p>	<p>Summary: OS9900 was upgraded to 8.9R2 and post-upgrade the QSFP-40G-LR in OS99-CNI-U8 stays down.</p> <p>Explanation: The issue is observed when the switch is upgraded to AOS 8.9R2. Once the issue is seen in the port the same SFP is moved to another port the interface comes up. If the same QSFP is moved back to the issue port, the port down is seen.</p> <p> Click for Additional Information</p>
<p>Case: 00748554 CRAOS8X-45492</p>	<p>Summary: When two 2000W Power supply the “Error reading PS EEPROM” error is seen in the switch console.</p> <p>Explanation: In AOS 8.9R04, enhancements are made to the fan algorithm, where the switch will pool the power supply for power consumption every 15 seconds. When there is a missing pooling request, the reported error is seen in the console.</p> <p> Click for Additional Information</p>
<p>Case: 00757184 CRAOS8X-46260</p>	<p>Summary: In the OS9907 model switch, while performing the failover test in the CMM of the chassis, and after the failover of the CMM you have noticed VFL ports of the Chassis are in down status, however, the interface status is up.</p> <p>Explanation: VFL port status is down after the failover test of CMM A. However, the interface status is up. The issue was not seen when the VC take-over command was used and physically the link was made down. The reboot of the whole chassis resolved the issue.</p>

	<p> Click for Additional Information</p>
<p>Case: 00719419 CRAOS8X-42883</p>	<p>Summary: The L2GRE frames are sent out with a Tag even though the uplink port on the switch is untagged.</p> <p>Explanation: The switch sends the tagged packets on an untagged uplink port toward the router, and the router drops that L2GRE packet. This is due to an incorrect VLAN check applied for L2GRE ports and is an AOS software issue.</p> <p> Click for Additional Information</p>
<p>Case: 00719419 CRAOS8X-42883</p>	<p>Summary: The L2GRE frames are sent out with a Tag even though the uplink port on the switch is untagged.</p> <p>Explanation: The switch sends the tagged packets on an untagged uplink port toward the router, and the router drops that L2GRE packet. This is due to an incorrect VLAN check applied for L2GRE ports and is an AOS software issue.</p> <p> Click for Additional Information</p>
<p>Case: 00732839 CRAOS8X-43592</p>	<p>Summary: SFP-10G-SR / 1G-SX is not detected on chassis 1 of the OS9007 VC on the OS99-XNI-U48 module.</p> <p>Explanation: The SFPs are detected on hardware however, it is not updated in the Software and thus the SFPs are not shown in “show transceiver output”.</p> <p> Click for Additional Information</p>
<p>Case: 00741744 CRAOS8X-44402</p>	<p>Summary: OS6860N: After successful authentication, all traffic on dynamic SAP port is dropped.</p> <p>Explanation: When a device is connected to a dynamic UNP port, it passes the authentication and expected UNP profile is assigned. After that all packets received on the port are not forwarded.</p> <p> Click for Additional Information</p>
<p>Case: 00733059 CRAOS8X-43674</p>	<p>Summary: OS6860E: BGP multipath feature not supported for IPv6 prefixes</p> <p>Explanation: The switch fails to load balance traffic across two equal-cost paths for IPv6 prefixes learned through BGP. This behavior is observed despite both paths appearing in the BGP table. Only one path is ultimately installed into the routing table, resulting in suboptimal traffic distribution.</p> <p> Click for Additional Information</p>

<p>Case: 00732563 CRAOS8X-43591</p>	<p>Summary: BGP policy prefix6-list to allow only the default route is not supported</p> <p>Explanation: The functionality of implementing a BGP policy prefix6-list exclusively for permitting only the default route is not currently available on Alcatel Omniswitches.</p> <p> Click for Additional Information</p>
<p>Case: 00722591 CRAOS8X-42412</p>	<p>Summary: OS6860N: Connectivity issues on Service Access Ports</p> <p>Explanation: Lack of connectivity and missing MAC address on the affected ports. Additionally, the interface counters displayed no incoming traffic. The issue is more frequent on dynamic SAP ports.</p> <p> Click for Additional Information</p>
<p>Case: 00735340 CRAOS8X-43913</p>	<p>Summary: 6900-X72 in router mode unable to route traffic to some destinations using the default gateway route.</p> <p>Explanation: An OS 6900-X72 in Router Mode receives a 0.0.0.0/0 route via OSPF but is unable to send traffic to 128.0.0.0/1 unless a more specific route is present.</p> <p>At the software level we see the default route from OSPF is learned, but at the hardware level it is not being installed. Note that this issue does not occur when the switch is in Switch Mode. This does not affect the OS 6900-V72</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. 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
uosn-mpls-v1.deb uosn-sitemgr-v1.deb uosn-siteend-v1.deb	MPLS Application and Licensing
nutanix-v1.deb	Nutanix Prism Plug-in Package
ovng-agent-v.1.10.deb	OmniVista Cirrus 10
- 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. - Applications should be stopped prior to upgrading a package.	

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.

Appendix K: Fixed CVEs

The following CVE CRs were fixed in this release.

CVE CRs	Module	CVE	NVD CVSS
CRAOS8X-44655	Linux	CVE-2024-1086	7.8
CRAOS8X-43052	zlib	CVE-2023-45853	9.8
CRAOS8X-36566	python	CVE-2022-37454	9.8
CRAOS8X-46556	openssh	CVE-2024-6387	8.1

CRAOS8X-46556

Description: The vulnerability (CVE-2024-6387) in OpenSSH is a signal handler race condition in the OpenSSH server (sshd) that occurs if a client does not authenticate within LoginGraceTime which is 600 seconds by default. An attacker can exploit this vulnerability on a device by repeatedly attempting to connect to the OpenSSH server without authenticating. Each attempt aims to trigger the SIGALRM signal handler at a precise moment when it is performing unsafe operations. The key to successful exploitation is the ability to manipulate the server's memory layout through crafted inputs, such as malformed SSH keys, which are designed to place the device memory in a state where it becomes vulnerable to corruption.

Workaround: Set "LoginGraceTime" to "0" in sshd_cfg. This disables the functionality that is used to trigger the vulnerability. AOS 8.10R1 enables the workaround by default. If the "ssh login-grace-time" is already configured to a value other than 0, it is advisable to set to "0" using "ssh login-grace-time 0" command.