

Release Notes - Rev. A

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

Release 8.9R3

These release notes accompany release 8.9R3. 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.

Contents

Contents 2

Related Documentation..... 3

System Requirements 4

[IMPORTANT] *MUST READ*: AOS Release 8.9R3 Prerequisites and Deployment Information 11

Licensed Features 14

ALE Secure Diversified Code..... 16

New / Updated Hardware Support and Guidelines 17

8.9R3 New Feature and Enhancements 18

Open Problem Reports and Feature Exceptions 27

Hot-Swap/Redundancy Feature Guidelines..... 29

Technical Support..... 32

Appendix A: Feature Matrix 34

Appendix B: MACsec Platform Support 43

Appendix C: SPB L3 VPN-Lite Service-based (Inline Routing) / External Loopback Support / BVLAN Guidelines 44

Appendix D: General Upgrade Requirements and Best Practices 47

Appendix E: Standard Upgrade - OmniSwitch Standalone or Virtual Chassis 52

Appendix F: ISSU - OmniSwitch Chassis or Virtual Chassis 54

Appendix G: FPGA / U-boot Upgrade Procedure..... 57

Appendix H: CPLD Upgrade Procedure for ONIE-Based Devices..... 60

Appendix I: Fixed Problem Reports 62

Appendix J: Installing/Removing Packages 83

Appendix K: Fixed CVEs 85

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 Requirements

Memory Requirements

The following are the standard shipped memory configurations. Configuration files and the compressed software images—including web management software (WebView) images—are stored in the flash memory.

Platform	SDRAM	Flash
OS6360	1GB	1GB
OS6465	1GB	1GB
OS6560	2GB	2GB
OS6560-24X4/P24X4	1GB	1GB
OS6570M	2GB	8GB
OS6860(E)	2GB	2GB
OS6860N	4GB	16GB
OS6865	2GB	2GB
OS6900-X Models	2GB	2GB
OS6900-T Models	4GB	2GB
OS6900-Q32	8GB	2GB
OS6900-X72	8GB	4GB
OS6900-V72/C32	16GB	16GB
OS6900-X48C6/T48C6/X48C4E/T24C2/X24C2	8GB	32GB ¹
OS6900-V48C8/C32E	8GB	64GB ¹
OS9900	16GB	2GB
1. Size of physical memory. Partitioned to 16GB flash memory.		

U-Boot and FPGA Requirements

The software versions listed below are the **MINIMUM** required, except where otherwise noted. Switches running the minimum versions, as listed below, do not require any U-Boot or FPGA upgrades but it's recommended to upgrade to the current version to address any known issues. Use the '**show hardware-info**' command to determine the current versions.

Switches not running the minimum version required should upgrade to the latest U-Boot or FPGA that is available with this AOS release software available from Service & Support.

Please refer to the [Upgrade Instructions](#) section at the end of these Release Notes for step-by-step instructions on upgrading your switch.

OmniSwitch 6360 - AOS Release 8.9.221.R03 (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

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
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
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 uboot update for CRAOS8X-24464, ability to disable/authenticate uboot 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 8.9.221.R03 (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	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		
OS6465T-P12	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
OS6465-P12 (ENH-240)	8.8.33.R01	8.8.33.R01 8.9.85.R02 ⁵	0.5	0.5
<p>1. FPGA version 0.7 is optional to address issue CRAOS8X-12042.</p> <p>2. U-boot 8.7.2.R02 is optional to address UBIFS error issues CRAOS8X-4813/13440.</p> <p>3. Optional uboot update for CRAOS8X-24464, ability to disable/authenticate uboot access.</p> <p>4. Optional uboot update to support boot from USB feature.</p> <p>5. Highly recommended to address the NAND flash corruption issue (CRAOS8X_35470).</p>				

OmniSwitch 6560 - AOS Release 8.9.221.R03 (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
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
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
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
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
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

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
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
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

1. FPGA version 0.7 is optional to address issue CRAOS8X-7207.
2. FPGA versions are optional to address issue CRAOS8X-16452.
3. U-boot 8.7.2.R02 is optional to address eUSB issue CRAOS8X-13819.
4. U-boot 8.7.2.R02 is optional to address UBIFS error issues CRAOS8X-4813/13440.
5. FPGA version 0.8 is optional to address issue CRAOS8X-22857.
6. FPGA versions 0.7 and 0.8 are optional to support 1588v2.
7. Optional uboot update for CRAOS8X-24464, ability to disable/authenticate uboot access.
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 uboot version for these models.

OmniSwitch 6570M - AOS Release 8.9.221.R03 (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	0.11	0.11
OS6570M-12D	8.9.25.R02	8.9.25.R02 8.9.92.R02 ¹ 8.9.139.R03 ³	0.11	0.11
OS6570-U28	8.9.25.R02	8.9.25.R02 8.9.92.R02 ¹ 8.9.139.R03 ³	0.11	0.11 0.12 ²

1. Adds support for Gowin CPLD.
2. Addresses power supply interrupt issue.
3. Addresses CRAOS8X-40924 for disabling uboot access.

OmniSwitch 6860(E) - AOS Release 8.9.221.R03 (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

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

OmniSwitch 6860N - AOS Release 8.9.221.R03 (GA)

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

1. Addresses CRAOS8X-29731/30471 - OS6860N power supply issue.
Note: These models use the Uosn.img image file.

OmniSwitch 6865 - AOS Release 8.9.221.R03 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6865-P16X	8.3.1.125.R01	8.7.2.R02 ² 8.7.30.R03 ³ 8.8.33.R01 ⁴	0.20	0.25 ¹
OS6865-U12X	8.4.1.17.R01	8.7.2.R02 ² 8.7.30.R03 ³ 8.8.33.R01 ⁴	0.23	0.25 ¹
OS6865-U28X	8.4.1.17.R01	8.7.2.R02 ² 8.7.30.R03 ³ 8.8.33.R01 ⁴	0.11	0.14 ¹

1. FPGA versions 0.25 and 0.14 are optional for the fast and perpetual PoE feature support.
 2. U-boot 8.7.2.R02 is optional to address eUSB issue CRAOS8X-13819.
 3. Optional uboot update for CRAOS8X-24464, ability to disable/authenticate uboot access.
 4. Optional uboot update to support boot from USB feature.
Note: CRAOS8X-4150 for the OS6865-U28X was fixed with FPGA version 0.12 and higher.

OmniSwitch 6900-X20/X40 - AOS Release 8.9.221.R03 (GA)

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

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

OmniSwitch 6900-T20/T40 - AOS Release 8.9.221.R03 (GA)

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

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

OmniSwitch 6900-Q32 - AOS Release 8.9.221.R03 (GA)

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

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

OmniSwitch 6900-X72 - AOS Release 8.9.221.R03 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
CMM	7.3.4.31.R02	8.6.189.R02 ¹ 8.7.30.R03 ²	0.1.10	0.1.11 ¹

1. FPGA version 0.1.11 and U-boot version 8.6.189.R02 are optional to address CRAOS8X-11118.
2. Optional uboot update for CRAOS8X-24464, ability to disable/authenticate uboot access.

OmniSwitch 6900-V72/C32/C32E/X48C6/T48C6/X48C4E/V48C8/T24C2/X24C2- AOS Release 8.9.221.R03 (GA)

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

Hardware	Minimum ONIE	Current ONIE	Minimum CPLD	Current CPLD
OS6900-X48C4E	2019.05.00.10	2019.05.00.10	CPLD 1 - 3 CPLD 2 - 2 CPLD 3 - 3 CPU CPLD - N/A	CPLD 1 - 3 CPLD 2 - 2 CPLD 3 - 3 CPU CPLD - 2.14 ¹
OS6900-V48C8	2020.02.00.01	2020.02.00.01	CPLD 1 - 2 CPLD 2 - 3 CPLD 3 - 2	CPLD 1 - 2 CPLD 2 - 3 CPLD 3 - 2
OS6900-T24C2	2019.08.00.03	2019.08.00.03	CPLD 1 - 2.0 CPLD 2 - 2.0 CPLD CPU - 6.0	CPLD 1 - 2.0 CPLD 2 - 2.0 CPLD CPU - 6.0
OS6900-X24C2	2019.08.00.03	2019.08.00.03	CPLD 1 - 6.0 CPLD 2 - 6.0 CPLD CPU - 6.0	CPLD 1 - 6.0 CPLD 2 - 6.0 CPLD CPU - 6.0

1. Optional CPU CPLD update to address CRAOS8X-30098.

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

OmniSwitch 9900 - AOS Release 8.9.221.R03 (GA)

Hardware	Minimum Coreboot-uboot	Current Coreboot-uboot	Minimum Control FPGA	Current Control FPGA	Minimum/Current Power FPGA
OS99-CMM	8.3.1.103.R01	8.3.1.103.R01 8.7.30.R03 ¹	2.3.0	2.3.0	0.8
OS99-CMM2	8.9.183.R03	8.9.183.R03	1.4.0	1.4.0	1.2.0
OS9907-CFM	8.3.1.103.R01	8.3.1.103.R01	-	-	-
OS9907-CFM2	8.9.X	8.9.X	-	-	-
OS99-GNI-48	8.3.1.103.R01	8.3.1.103.R01 8.8.152.R01 ²	1.2.4	1.2.4 1.2.5 ²	0.9
OS99-GNI-P48	8.3.1.103.R01	8.3.1.103.R01 8.8.152.R01 ²	1.2.4	1.2.4 1.2.5 ²	0.9
OS99-XNI-48 (903753-90)	8.3.1.103.R01	8.3.1.103.R01 8.8.152.R01 ²	1.3.0	1.3.0 1.5.0 ²	0.6
OS99-XNI-48 (904049-90)	8.6.261.R01	8.6.261.R01 8.8.152.R01 ²	1.4.0	1.4.0 1.5.0 ²	0.7
OS99-XNI-U48 (903723-90)	8.3.1.103.R01	8.3.1.103.R01 8.8.152.R01 ²	2.9.0	2.9.0 2.11.0 ²	0.8
OS99-XNI-U48 (904047-90)	8.6.261.R01	8.6.261.R01 8.8.152.R01 ²	2.10.0	2.10.0 2.11.0 ²	0.8
OS99-GNI-U48	8.4.1.166.R01	8.4.1.166.R01 8.8.152.R01 ²	1.6.0	1.6.0 1.7.0 ²	0.2
OS99-CNI-U8	8.4.1.20.R03	8.4.1.20.R03 8.8.152.R01 ²	1.7	1.7 1.9 ²	N/A

Hardware	Minimum Coreboot-uboot	Current Coreboot-uboot	Minimum Control FPGA	Current Control FPGA	Minimum/Current Power FPGA
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	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 uboot update for CRAOS8X-24464, ability to disable/authenticate uboot access. 2. Optional Uboot/FPGA update for CMM2 and OS9912 compatibility.					

[IMPORTANT] *MUST READ*: AOS Release 8.9R3 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.

- Beginning in August 2022 ALE will begin placing QR codes on physical products as well as the corrugated shipping boxes, the QR codes allow for additional information such as MAC addresses to be included. To allow time for customers and partners to adjust to the new barcodes there will be a 6 to 12 month transition period that will include both the QR code and the linear style barcodes. After the transition period ends only the QR codes will be included.

Deprecated Features / Functionality Changes

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

AOS Release 8.5R4
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 8.6.R1. Commands entered using the CLI must use the new 'ipv6 dhcp guard vlan vlan-id' format of the command. The old format will still be accepted if present in a vcboot.cfg to preserve backwards compatibility.
IP Helper - The 'ip helper' commands have been deprecated in 8.6R1 and replaced with 'ip dhcp relay'. The old format will still be accepted if present in a vcboot.cfg to preserve backwards compatibility.
SAA - The vlan-priority and drop-eligible parameters have been deprecated from all SAA commands beginning in 8.6R1.
MACsec is now supported on ports 33-48 of the 6560-(P)48X4. CRAOS8X-7910 was resolved in 8.6R1.
AOS Release 8.6R2
Distributed ARP - Beginning 8.6R2 distributed ARP is no longer supported.
WRED - Beginning in 8.6R2 WRED is no longer supported.
QoS - Beginning in 8.6R2 the 'qos dscp-table' command is no longer supported.
NTP - The ntp parameter for the 'ip service source-ip' command was deprecated in 8.5R4. Support has been added back in 8.6R2.
AOS Release 8.7R1
MACsec - Static mode is not supported on OS6860N.
Transceivers - Beginning in AOS release 8.7R1 an error message will be displayed when the unsupported QSFP-4X25G-C transceiver is inserted on an OS99-CNI-U8 module.
SPB - Beginning in 8.7.R01 the default number of BVLANS created via Auto Fabric is reduced from 16 to 4. This new default value is only applicable to factory default switches running 8.7R1 with no vcboot.cfg file. Upgrading to 8.7.R1 will not change the number of configured BVLANS in an existing configuration. See Appendix 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. - 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) - 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.

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 6900	
Data Center Features		
DCB (PFC,ETS,DCBx)	Yes	
FIP Snooping	Yes	
FCoE VXLAN	Yes	
Note: Supported on OS6900-X20/X40/T20/T40/Q32/X72 models.		

Licensed Features	License Required							
	OS6360	OS6465	OS6560	OS6570M	OS6860	OS6860N	OS6900	OS9900
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
Licenses Features	
CPE Test Head	Yes
PPPoE-IA	Yes
Ethernet OAM	Yes
SAA	Yes
Link OAM	Yes
VLAN Stacking	Yes
DPA	Yes
Hardware Loopback	Yes
IPMVLAN	Yes
Note: Starting in 8.9R1 the features above require a Metro license.	

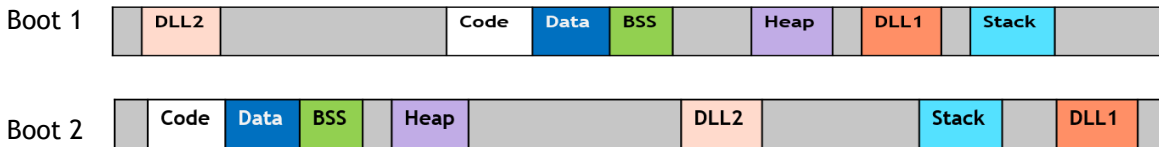
ALE Secure Diversified Code

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

ALE secure diversified code employs multiple techniques to identify vulnerabilities such as software architecture reviews, source code analysis (using both manual techniques and automated tools), vulnerability scanning tools and techniques, as well as analysis of known vulnerabilities in third party code.

Software Diversification

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



Please contact customer support for additional information.

New / Updated Hardware Support and Guidelines

The following new hardware features are being introduced in this release.

OS99-CMM2

The OS99-CMM2 Chassis Management Module (CMM) manages system functions in the OS9912 chassis and provides four (4) 100G QSFP28 uplink ports.

OS9912-CFM

OmniSwitch 9912 Chassis Fabric Module (CFM).

OS9912-CHAS

OmniSwitch 9912 Chassis is a 12 slot 17.25 RU chassis with:

- 12 - CMM and NI Slots (Slot 1 and 2 are reserved for CMMs with integrated 4 ports of QSFP28)
- 4 - CFM - (Bays marked CFM3 and CFM4 are inactive; reserved for future use)
- 3 - Fan Tray Slots
- 4 - Power Supplies Slots
 - OS99-PS-A - 3000W AC Power Supply
 - OS99-PS-D - 2500W DC Power Supply

Note: The OS9912 does not support a Virtual Chassis configuration (VC of 1 Only).

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. Refer to [OS9900 Uboot/FPGA](#) for additional information.

Note: The OS99-XNI-U12Q, OS99-XNI-UP24Q2, OS99-XNI-P24Z8 and OS99-XNI-P48Z16 modules are not supported in an OS9912 chassis.

OS99-CNI-U20

Contains twenty (20) 40/100G QSFP28 ports. Ports 13-20 support splitter functionality of either 4X10G or 4X25G.

OS6570M-12/12D

Revised OS6570M-12 (904390-90) and OS6570M-12D (904391-90) models will begin shipping with a hardware change that will allow for IEEE 1588 V2 support in a future AOS Release. **Note:** These revised models are also supported in AOS release 8.9R2.

SFP-DUAL-MM-N

The existing part SPG-DR-FX-CDFC-AL2 is being replaced with part SPG-DR-FX-CDFD-AL2. The existing SPG-DR-FX-CDFC-AL2 will continue to work with all AOS releases. However, SPG-DR-FX-CDFD-AL2 requires a minimum of AOS release 8.9R3.

SFP-10G-T

The existing parts 903866-90 (HW Rev. -43 and -53) are being replaced with part 903866-90 (HW Rev. A53). The existing 903866-90 (HW Rev. -43 and -53) will continue to work with all AOS releases. However, 903866-90 (HW Rev. A53) requires a minimum of AOS release 8.9R3.

SFP-GIG-T

The existing SFP-GIG-T transceiver is being replaced with an updated transceiver. The existing part will continue to work with all AOS releases. The serial number format of the new part is "APxxxxxxxx" and requires a minimum of AOS release 8.9R3.

8.9R3 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
Management Features	
X.509 Certificate Support - Switch Supplicant	All
Lanpower Delayed Start	6360, 6465, 6560
Authentication Trap Mode	All
Layer 3 Features	
Separate Routing Table and Default Gateway on EMP-Port	All
VRF - Device Profiling	6860(E), 6860N, 6865
VRF Names / Firewall Contexts	6860(E), 6860N, 6865, 6900 (all), 9900
Service Features	
L2 Customer to Customer Isolation Over SPB (PVLAN on SAP)	OS6860(E), OS6860N, OS6900-C32/V72/X48C6/X48C4E/V48C8/X24C2 /T24C2
SPB L3VPN Route-tag Support	6860(E), 6860N, 6865, 6900 (all), 9900
Hybrid SAP and Bridge Port	6860(E), 6860N, 6865, 6900 (all), 9900
MPLS	
MPLS	6860N
MPLS Licensing - Site and Node based Licensing for MPLS	6860N
Other Features	
DHCPv6 Option 37 and 18	All
Virtual Chassis of 8	6360 (all 24/48 port models)
IP Multicast VLAN (IPMVLAN)	6465, 6560, 6570M
MEF 3.0 Compliance	6560-24X4, 6560-P48X4, 6465T-12, 6570M-U28,6570M-12
Port Mirroring - Sessions and Destination Ports	6860(E), 6860N, 6865, 6900 (all)
Port Mirroring - Remote Over Linkagg	6560
Dynamic ARP Inspection Support with DHCP Snooping	6465, 6560, 6570M
Hardware Loopback Scalability Support	6465
Parity Features	
ERPv2 Support	6360
TDR	6360, 6465 and 6560.
1588v2 End-to-End Transparent Clock	OS6860N, 6900-V72/C32/X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2

Management Features

X.509 Certificate Support - Switch Supplicant

OmniSwitch now includes a feature that allows the switch to be authenticated as a supplicant device using X.509 certificates. Customers can either download their custom X.509 certificates or use default ALE X.509 certificates for switch authentication.

If the switch does not pass authentication, it will be placed in Restricted mode. The switch will only transition out of the restricted state when it successfully completes the authentication process. Ability to download and manage the customer X.509 certificate on switch without removing the default ALE certificates. Use this downloaded X.509 certificate for 802.1x authentication of the switch itself as a supplicant.

Lanpower Delayed Start

This enhancement delays the enabling of lanpower on PoE ports until after the Ethernet ports are enabled and the system has stabilized. A delay from 120 to 600 seconds can be configured. FPoE and PPoE are not supported when delayed start is enabled.

The following CLI commands are associated with this feature:

- **lanpower slot *chassis/slot* delayed-start [enable seconds *num* | disable]**
- **show lanpower slot *chassis/slot* all status [all | delayed-start]**

Authentication Trap Mode

The OmniSwitch can be configured to send both a standard and private authentication trap.

- If mode is set to **standard** (default): only the standard *authenticationFailure* notification will be sent.
- If mode is set to **private**: only *alaAuthenticationFailure* notification failure will be sent.
- If mode is set to **both**: *authenticationFailure* and *alaAuthenticationFailure* notifications will be sent.

The *alaAuthenticationFailure* includes the IP address of the client causing the authentication failure.

The following CLI commands are associated with this feature:

- **snmp authentication-trap mode {standard | private | both}**

Layer 3 Features

Separate Routing Table and Default Gateway on EMP-Port

This feature allows for applying an ACL on the EMP port of the switch. It enables policy-based routing on the EMP ports. The configuration is enabled using the **empacl** policy-list type.

Note: In this release the support is added only for IP condition in PBR policy rule.

The following condition and action are supported in this release:

- Policy condition with Source IPv4 and Destination IPv4 addresses
- Policy action with PBR

Only a single **empacl** policy list with multiple policy rules is supported.

The following CLI commands are associated with this feature:

- **policy list *list_name* type empacl**

VRF Device Profiling

This enhancement makes device profiling VRF aware by supporting the *vrf-name* parameter when starting iot-profiler.

The following CLI commands are associated with this feature:

- **appmgr start iot-profiler** *vrf-name*

VRF Names / Firewall Contexts

This enhancement allows VRF names to be 32 characters long and contain letters, minus signs and numbers.

The following CLI commands are associated with this feature:

- **vrf create** *vrf-name*

Service Features

L2 Customer to Customer Isolation Over SPB (PVLAN on SAP) / SPB E-Tree Services

E-TREE services provide rooted multipoint connectivity (P2MP) between UNIs (SAPs) of an SPBm service. In the current release, E-TREE services with Leaf SAPs is supported.

With this implementation, the traffic ingressing on the SAPs of a BEB (say BEB-1) of a service created with E-TREE option is sent out with MAC-in-MAC (MIM) encapsulation on network port to the remote BEB. On BEB-2, a service with same ISID value is created as an E-LAN service (without E-TREE option). The MIM port traffic (originating on BEB-1 for service E-TREE ISID) into the BEB-2, egress out on SAPs of the service with corresponding ISID value.

- E-Tree feature on an SPB service can be configured by enabling ‘e-tree’ option while creating the service.
- E-Tree feature on UNP created services can be configured by enabling ‘e-tree’ option on the UNP profile while creating the profile.

The following CLI commands are associated with this feature:

- **service** *service_id*[-*service_id2*] **spb isid** *instance_id*[-*instance_id2*] **bvlan** *bvlan_id*[:*x*] [**e-tree** {**enable** | **disable**}]
- **show service ports**
- **show service**
- **unp profile** *profile_name* **map service-type** **spb tag-value** {**0** | **ALL** | *outer_qtag:all* | *qtag* | *outer_qtag:inner_qtag*} **isid** *instance_id* **bvlan** *bvlan_id* [**e-tree**]
- **show unp profile map**

SPB L3VPN Route-tag Support

AOS functionality of advertising SPB L3VPN routes is extended to exchange and inject the route-tag field to be carried across the SPB-ISIS network. This feature will be supported on all the platforms which support SPB-ISIS. Functionality will be supported in two components: IPRM/GRM and ISIS SPB.

The following CLI commands are associated with this feature:

- **show sppb ipvpn route-table**

Hybrid SAP and Bridge Port

Hybrid access port feature allows a single port to function both as an access port and a bridging port. Hybrid configured port can be understood as a bridge port with a default VLAN and tagged VLAN for bridging and the user can configure SAPs for services with mapped tagged VLANs.

Features that are currently supported in both in VLAN and service domain will be supported in VLAN domains only on the hybrid access port. Features that are not supported on the service access port will continue to be not supported on the hybrid access port as well.

The following CLI commands are associated with this feature:

- **service access {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} hybrid {enable | disable} [description port_description]**
- **show service access**

MPLS Features

Multiprotocol Label Switching (MPLS)

MPLS is a label switching technology that provides the ability to set up connection-oriented paths over a connectionless IP network. MPLS sets up a specific path for a sequence of packets. The packets are identified by a label inserted into each packet. This implementation of MPLS provides the network architecture that is needed to set up a Virtual Private LAN Service (VPLS). VPLS allows multiple customer sites to transparently connect through a single bridging domain over an IP/MPLS-based network. The MPLS architecture provided is based on the Label Distribution Protocol (LDP). The LDP consists of a set of procedures used by participating Label Switching Routers (LSRs) to define Label Switched Paths (LSPs), also referred to as MPLS tunnels. These tunnels provide the foundation necessary to provision VPLS.

OmniSwitch implementation of VPLS supports the following:

- VPLS using LDP signaling
- VPLS using BGP signaling

MPLS is a licensed feature in AOS. MPLS is packaged into a Debian package, which can be installed or removed independently on the switch. To configure MPLS in AOS, it is required to install the MPLS package using Package Manager commands. Upon installing the MPLS package, MPLS process is loaded. The LDP and BGP modules will be loaded only after the load commands - **mpls load ldp**, and **ip load bgp**.

Also, it is required to install Site-based or Node-based license for MPLS interface to be up and running.

The following CLI commands are associated this feature:

MPLS commands -

- **mpls interface**
- **show mpls**
- **show mpls interface**
- **show mpls ftn-table**
- **show mpls ilm-table**
- **show mpls forwarding-table**
- **show mpls vpls mesh**

MPLS LDP Commands -

- `mpls ldp admin-state`
- `mpls ldp`
- `mpls ldp interface admin-state`
- `mpls ldp interface`
- `mpls ldp session-protection`
- `mpls ldp graceful-restart`
- `show mpls ldp`
- `show mpls ldp interface`
- `show mpls ldp neighbor`
- `show mpls ldp session`
- `show mpls ldp session rx-addresses`
- `show mpls ldp session rx-labels`
- `show mpls ldp session tx-labels`

MPLS BGP Commands -

- `ip bgp max-neighbors`
- `show ip bgp`
- `ip bgp neighbor activate l2vpn-vpls`
- `show ip bgp neighbors`
- `ip bgp address-family l2vpn-vpls`
- `show ip bgp l2vpn-vpls`
- `show ip bgp l2vpn-vpls path`

MPLS VPLS commands -

- `service vpls`
- `service description`
- `service vlan-xlation`
- `service admin-state`
- `show service`
- `show service ports`
- `show service spb sap`
- `show service debug-info`
- `show service info`
- `show service l3vpn profile`
- `service sap`
- `service sdp vpls`
- `service bind-sdp`
- `show service sdp`
- `show service sdp vpls`
- `show service bind-sdp`
- `show service bind-sdp l2gre`
- `show service bind-sdp vpls`
- `show service mesh-sdp`
- `show service vpls mesh-sdp`

MPLS Source Learning Commands -

- `mac-learning flush domain vpls`

- **show mac-learning**
- **show mac-learning domain all**
- **show mac-learning domain vpls**

Site and Node Based Licensing for MPLS

MPLS (Multiprotocol Label Switching) is supported on AOS switches as a dynamically installable software (Debian) package. To configure MPLS in AOS, it is required to install the MPLS package using Package Manager commands.

For MPLS interface to be up and running, every network node that runs MPLS will require to be licensed. Such licenses will be generated on the ALE Customer or Business Portal. Two types of licenses are supported:

Two types of licenses are supported:

- **Site-based license** - The Site-based licenses can be used as a floating or a shared license up to a maximum of four network nodes, without being bound to the hardware. For licensing, a network node can be a standalone switch or a virtual chassis of up to eight units. Site license eliminates the need to support expiry, revocation, or transfer attributes on the switch client. All these are handled by the site license server. Switch identification can be done using serial numbers and system MAC addresses, and so on.
- **Node-based license** - The Node-based licenses are specific to any MPLS node, not bound to the hardware, and are not tied to the Node's Serial Number, MAC addresses, and so on. For licensing, an MPLS node can be a standalone of a Virtual Chassis of up to eight units.

The SILOS (Site Local Licensing Server) is available as a ALE Debian software package that runs on a switch or a virtual chassis acts as a server issuing the site or node licenses to the sites and nodes. SWLIC (Switch Local Licensing client) runs on every MPLS-enabled switch in the network and acts as a client getting the site or node licenses from the SILOS.

To install the licenses, download the site or node licenses generated on the ALE portal to the SILOS switch. To enable the site or node license in the SILOS, the customer must use the current ALE license portal to generate the license and install it manually using the SILOS management configuration commands.

The following CLI commands are associated with this feature:

- **license server**
- **license server apply**
- **license server remove**
- **license client**
- **license client remove**
- **show license-server**
- **show license-server info**
- **show license-server usage**
- **show license-client info**

Note: A customer may purchase multiple site or node licenses to support more than four MPLS network switches.

Other Features

DHCPv6 Option 37, 18 Support

The OmniSwitch now supports the configuration of Option 18 and Option 37 information on the DHCPv6 relay. Options 18 and 37 serve the purpose of providing additional information to the DHCPv6 server, enabling it to identify the DHCPv6 client and assign an appropriate IPv6 address.

Option 18, known as the interface-ID option, signifies the interface index of the port through which the DHCPv6 client messages are received. Option 37, known as the remote-ID option, provides the host details that the DHCPv6 server can utilize to assign IP addresses, prefixes, and other configuration parameters specifically tailored for the client.

The following CLI commands are associated with this feature:

- `ipv6 dhcp relay interface-id prefix prefix_name`
- `ipv6 dhcp relay remote-id format { base-mac | system-name | vlan | user-string string | interface-alias | auto-interface-alias | disable}`
- `ipv6 dhcp relay remote-id enterprise-number num`
- `show ipv6 dhcp relay`
- `show configuration snapshot dhcpv6-relay`

Virtual Chassis of 8

This enhancement allows all OS6360-24/48 port models to support of VC of 8 elements.

IP Multicast VLAN (IPMVLAN)

IP Multicast VLAN (IPMV) is an innovative feature for service providers delivering residential voice and video services. It involves the creation of separate dedicated VLANs built specifically for multicast traffic distribution. These distribution VLANs connect to the nearest multicast router and support multicast traffic only.

Service providers have to separate users using these VLANs. This has to be done along with the distribution of broadcast media through IP Multicast across these VLANs without a router in the distribution L2 switch. To achieve this, the distribution L2 switch needs to perform IGMP snooping (that is, allow the switch to "listen in" on the IGMP conversation between hosts and routers) as well as distribute multicast traffic from one multicast distribution VLAN to many customer ports.

A distribution multicast VLAN that switches into customer ports is invisible to the customer to avoid packet duplication across the trunk. Furthermore, some service providers use QinQ on the provider ports to tag the multicast distribution VLAN with a distinct outer VLAN tag. The customer ports can either be tagged or untagged. However, the multicast traffic always has to be tagged. This process requires one or more separate multicast distribution VLANs. These distribution VLANs connect to the nearest multicast router and are used for multicast traffic only.

The multicast traffic only flows from the distribution VLAN to the customer VLAN. Customer-generated multicast traffic flows only through the customer VLANs so that the multicast router can control the distribution of such traffic.

The IPMV feature works in both the Enterprise and the VLAN Stacking environment. The ports are classified as VLAN Stacking ports and Legacy ports (fixed ports/tagged ports).

The following CLI commands are associated with this feature:

- `ipmvlan`
- `show vlan ipmvlan`
- `spantree vlan`
- `mac-learning vlan`

- **ipmvlan ctag**
- **ipmvlan address**
- **ipmvlan sender**
- **ipmvlan receiver**
- **ip multicast static-group**
- **show ipmvlan**
- **show ipmvlan config**
- **show ipmvlan port-config**
- **show ipmvlan address**
- **show ipmvlan c-tag**

MEF 3.0 Compliance

MEF 3.0 compliance is being added to OmniSwitch. MEF 3.0 is a set of standards aimed at accelerating the deployment and delivery of dynamic networking services across a global network. E-Line (EPL and EVPL) and E-LAN (EP-LAN and EVP-LAN) are supported on OmniSwitch. E-Tree (EP-Tree, EVP-Tree), E-Access (A E-Line). and E-Transit (T E-Line) of MEF 3.0 are not supported.

- OS6560-24X4
- OS6560-P48X4
- OS6465T-12
- OS6570M-U28
- OS6570M-12

Port-mirroring Sessions and Destination Ports

The following port mirroring enhancements have been made on the 6860(E), 6860N, 6865, 6900 (all) in 8.9R3. The same destination port can be used in different port mirroring sessions and the maximum port-mirroring sessions has been increased from 2 to 4.

Note the following:

- There is a limit of 4 Mirror-to-port (MTP) indexes.
- Bi-directional counts as two MTP indexes for each destination port in the session.
- If a destination port is configured on multiple sessions and has the same source port mirror direction as those sessions the MTP index will only be counted once.

The following CLI commands are associated with this feature:

- **port-mirroring source destination**

Port Mirroring - Remote Over Linkagg

Remote port mirroring over a link aggregate is now supported on the OS6560.

The following CLI commands are associated with this feature:

- **port-mirroring destination linkagg**

Dynamic ARP Inspection Support with DHCP Snooping

Dynamic ARP Inspection (DAI) serves as a security feature for validating the authenticity of Address Resolution Protocol (ARP) packets in a network. This capability can be used to prevent certain types of "man-in-the-

middle" attacks. DAI is implemented by combining both DHCP snooping and IP source filtering capabilities on the OmniSwitch.

The following CLI commands are associated with this feature:

- **dhcp-snooping vlan admin-state**
- **dhcp-snooping binding admin-state**
- **dhcp-snooping port trust**
- **dhcp-snooping ip-source-filter admin-state**
- **dhcp-snooping ip-source-filter dynamic-arp-inspection admin-state**
- **show dhcp-snooping ip-source-filter**

Hardware Loopback Scalability Support on OS6465

The capability to accommodate 12 Inward and 2 outward loopback profiles in OS6465 is introduced in this release. These 14 hardware loopback profiles can be simultaneously operational within OS6465. The allocation of TCAM resources dynamically occurs when the loopback profiles are activated and is released when all loopback resources are deactivated. This dynamic allocation ensures efficient TCAM resource utilization across various TCAM clients.

Parity Features

ERPV2 Support

This enhancement adds support for ERPv2 on the OS6360.

The following CLI commands are associated with this feature:

- **erp-ring**

Time Domain Reflectometry (TDR)

This enhancement adds TDR support on the OS6360, OS6465 and OS6560. Support is added for 1G RJ-45 copper ports only.

Note the following limitations:

- Not supported for OS6560-(P)24Z8/(P)24Z24/P48Z16 2.5G ports.
- Not supported on OS6360-P24X/PH24/P48X/PH48 10G combo ports.
- Length is displayed only for faulty cables. Cable length is not displayed for a good working cable.

The following CLI commands are associated with this feature:

- **interfaces chassis/slot/port tdr enable**

1588v2 End-to-End Transparent Clock

This enhancement adds support for Precision Time Protocol (1588v2) End-to-End (E2E) Transparent Clock (TC) support on the OS6860N, OS6900-V72/C32/X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2.

The following CLI commands are associated with this feature:

- **interfaces ptp admin-state {enable | disable}**

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-41205	Wireless client connecting to the Stellar AP with an SSID mapped to a Tunnel which is getting terminated on the GTTS switch are not getting the IP address. The issue is seen only when the loopback0 IP and the gateway IP is in the same Subnet. However the issue is sporadic and is not seen every time.	To avoid this issue, change the loopback0 IP and make sure its not in the same subnet of the Gateway IP.
CRAOS8X-41329	On an OS9912 the maxpower (watts) displays incorrect values in webview when lanpower is turned off.	Use the CLI to show the accurate power consumption value when lanpower is stopped.
CRAOS8X-41650	The 'show update fpga-cpld cmm 1/1 power' CLI command displays an error on the OS9900 chassis.	Use the 'show module long' command.
CRAOS8X-41961	On an OS9912 the 'lanpower maxpower' configuration may be missing after a reload or vc-takeover.	There is no known workaround at this time.
CRAOS8X-39126	When hot-swapping an OS9912-CFM traffic drop from 2 to 60 seconds may be seen.	There is no known workaround at this time.
CRAOS8X-41742	On an OS9912, fabric link down status may be seen during a CMM hot swap. The link will automatically recover but some packet loss may be seen.	There is no known workaround at this 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-41322	On an OS9912 the PoE firmware is not able to be updated using Webview.	Use the CLI to update the PoE firmware.
CRAOS8X-41538	On an OS9912 intermittent NI power-good failures may be seen after a reload for CNI-U20, CNI-U8, XNI-U48 modules.	There is no known workaround at this time.
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 disconnected or remove the transceiver.
CRAOS8X-37543	On an OS6465 "ALARM IN TRAP is OFF" & "ALARM IN TRAP is ON" traps are duplicated everytime the alarm is created.	There is no known workaround at this time.

CRAOS8X-3877	On 6900 and 6900-V72, untagged packets are mirrored as tagged traffic when when monitored port is across VC chassis. On standalone switch monitored egress traffic is tagged.	Use port mirroring.
CRAOS8X-27368	On an OS9900, when linkagg port is admin disabled, a forwarding database flush is issued for that particular port which is resulting in flushing MACs on other fixed port which a unrelated to the linkagg.	There is no known workaround at this time.
CRAOS8X-41625	On an OS9912 EMP IP details are still available even after removing the CMM from the slot with the status showing as UP.	There is no known workaround at this time.
CRAOS8X-40728	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. 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. 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.	There is no known workaround at this time.
CRAOS8X-23137	When a 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.
Hardware / Transceivers		
CRAOS8X-37513	SFP-10G-T (Methode SP7053-ALU) is not supported on OS6900-X48C4E.	There is no known workaround at this time.
CRAOS8X-37852	On some OS6360, OS6465, and OS6560 OmniSwitch models with Dragonite PoE firmware the error message "Dragonite Firmware download failed" may be seen causing PoE to become inoperable.	Rebooting the switch will, in some cases, allow the firmware to be downloaded properly and allow PoE to function. This issue is fixed in 8.9R3. See CR37852 .
CRAOS8X-41611	OS99-CNI-U8 with 4x25G DAC cable link does not come up for certain lanes.	Use the QSFP-100G-SR4 fiber transceiver with 4X25G capability.
CRAOS8X-40689	Fake link on OS6570M-U28 and OS6570M-12 10G ports with SFP-10G-CWDM and SFP-10G-BX-U40/D40 on peer admin toggles.	Reconnecting the cable may fix the issue. If not, hot-swap the transceiver.

CRAOS8X-35256	On 6860N 25G ports, the SFP-10G-GIG-SR/LR transceiver links up only at 10G and unable to config to 1G speed.	If 1G speed is required, use single speed Gigabit transceivers.
Layer 3		
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.
QoS/Security		
CRAOS8X-40989	On an OS99-XNI-P24Z8 the dynamic MACsec port status is down after a reload.	Toggle the MACsec admin state on the port.
CRAOS8X-4424	With a color-only policy action configuration, egress queues are not honoring the color marking and packet drop is observed and expected traffic rate is not achieved.	There is no known workaround at this time.
CRAOS8X-40948	On an OS6900 with QMR configured, if the policy server is reloaded the switch is unable retrieve more than approximately 200 quarantined MAC addresses from OmniVista.	There is no known workaround at this time.
Virtual Chassis		
CRAOS8X-41365	On an 6860N, 6900, or 9900 in some rare cases the EMP interface may not come up after a reload.	Toggle the interface from the root prompt: -> su -> ifconfig eth2 down -> ifconfig eth2 up

Hot-Swap/Redundancy Feature Guidelines

Hot-Swap Feature Guidelines

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

- When connecting or disconnecting a power supply to or from a chassis, the power supply must first be disconnected from the power source.
- For the OS6900-X40 wait for first module to become operational before adding the second module.
- All NI module extractions must have a 30 second interval before initiating another hot-swap activity. CMM module extractions should have between a 15 and 20 minute interval.
- All new module insertions must have a 5 minute interval AND the LEDs (OK, PRI, VC, NI) have returned to their normal operating state.

Existing Expansion Slot	Hot-Swap/Hot-Insert compatibility
Empty	
OS68-XNI-U4	OS68-XNI-U4
OS68-VNI-U4	OS68-VNI-U4

OS68-QNI-U2	OS68-QNI-U2
OS68-CNI-U1	OS68-CNI-U1

OS6860N-P48M Hot-Swap/Insertion Compatibility

Existing Expansion Slot	Hot-Swap/Hot-Insert compatibility
Empty	OS-XNI-U12, OS-XNI-U4
OS-XNI-U4	OS-XNI-U12, OS-XNI-U4
OS-XNI-U12	OS-XNI-U12, OS-XNI-U4
OS-HNI-U6	OS-HNI-U6
OS-QNI-U3	OS-QNI-U3
OS-XNI-T8	OS-XNI-T8
OS-XNI-U12E	OS-XNI-U12E

OS6900 Hot-Swap/Insertion Compatibility

Existing Slot	Hot-Swap/Hot-Insert compatibility
Empty	All modules can be inserted
OS99-CMM	OS99-CMM
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 be displayed.
6. Re-insert all transceivers into the new module.
7. Re-connect all cables to transceivers.
8. Hot-swap one CFM at a time. Please ensure all fan trays are always inserted and operational. CFM hot-swap should be completed with 120 seconds.

VC Hot-Swap / Removal Guidelines

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

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

Fast/Perpetual PoE Unlike Power Supply Swapping

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

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

Technical Support

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

Country	Supported Language	Toll Free Number
France, Belgium, Luxembourg	French	+800-00200100
Germany, Austria, Switzerland	German	
United Kingdom, Italy, Australia, Denmark, Ireland, Netherlands, South Africa, Norway, Poland, Sweden, Czech Republic, Estonia, Finland, Greece, Slovakia, Portugal	English	
Spain	Spanish	
India	English	+1 800 102 3277
Singapore	English	+65 6812 1700
Hong-Kong	English	+852 2104 8999
South Korea	English	+822 519 9170
Australia	English	+61 2 83 06 51 51
USA	English	+1 800 995 2696
Your questions answered in English, French, German or Spanish.	English French German Spanish	+1 650 385 2193 +1 650 385 2196 +1 650 385 2197 +1 650 385 2198
Fax: +33(0)3 69 20 85 85 Email: 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+ with exceptions & GPLv2+ with exceptions & LGPLv2+ & BSD	: /flash/foss/gpl-3.0.txt + /flash/foss/gpl-2.0.txt + /flash/foss/lgpl-2.1.txt + /flash/foss/bsd1.txt
openvswitch	: 2.12.0	: Apache License 2.0	: /flash/foss/Apache-License-2.0.txt

The Alcatel-Lucent name and logo are trademarks of Nokia used under license by ALE. To view other trademarks used by affiliated companies of ALE Holding, visit: www.al-enterprise.com/en/legal/trademarks-copyright. All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Neither ALE Holding nor any of its affiliates assumes any responsibility for inaccuracies contained herein. © Copyright 2023 ALE International, ALE USA Inc. All rights reserved in all countries.

Appendix A: Feature Matrix

The following is a feature matrix for AOS Release 8.9R3.

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	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	8.6R1	8.7R1	8.6R1
Automatic Remote Configuration Download (RCL)	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	Y	8.6R2	8.7R1	Y
Automatic/Intelligent Fabric	8.7R2	8.5R1	Y	8.9R2	Y	8.7R2	Y	Y	Y	Y	Y
Automatic VC	8.7R2	N	Y	8.9R2	Y	8.7R1	Y	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	8.7R1	8.6R2	N	N
Console Disable	8.7R2	8.6R2	8.6R2	8.9R2	8.6R2	8.7R1	8.6R2	8.6R2	8.6R2	8.7R1	8.6R2
Dying Gasp	N	Y	Y	N	Y	8.7R1	Y	N	N	N	N
Dying Gasp (EFM OAM / Link OAM)	N	8.6R1	8.6R1	N	8.6R1	8.7R1	8.6R1	N	N	N	N
EEE support	Y	8.9R1	8.9R1	8.9R2	Y	8.7R1	Y	Y	Y	Y	Y
Embedded Python Scripting / Event Manager	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	Y	8.7R2	8.7R2	Y
IP Managed Services	N	N	N	N	Y	8.7R1	Y	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	8.7R1
In-Band Management over SPB	N	N	N	N	8.5R4	8.7R1	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4
ISSU	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	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	8.8R1
NAPALM Support	8.7R2	8.5R1	8.5R1	8.9R2	8.5R1	8.7R1	8.5R1	8.5R1	8.7R2	8.7R2	N
NTP - Version 4.2.8.p11.	8.7R2	8.5R4	8.5R4	8.9R2	8.5R4	8.7R1	8.5R4	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	8.7R3
OpenFlow	N	N	N	N	Y	N	N	Y	N	N	N
OV Cirrus - Zero touch provisioning	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	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	8.5R4	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	8.5R4	8.7R1	8.5R4

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
OV Cirrus - Managed	8.7R2	8.5R4	8.5R4	8.9R2	8.5R4	8.7R1	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4
OVSDB	N	N	N	N	N	N	N	8.7R1 (X72/Q32)	8.7R1	N	N
Package Manager	8.7R2	8.6R2	8.6R2	8.9R2	8.6R2	8.7R1	8.6R2	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	8.6R1	8.7R1	8.6R1
Remote Chassis Detection (RCD)	N	N	N	N	8.6R2	8.7R1	N	Y	N	8.7R1	Y
SAA	8.7R2	8.5R1	8.9R1 Metro	8.9R2	Y	8.7R2	Y	Y	8.7R1	8.7R1	Y
SAA SPB	N	N	N	N	Y	8.7R2	Y	Y	8.7R1	8.7R1	8.6R2
SAA UNP	N	Y	N	N	Y	N	Y	Y	N	N	N
SNMP v1/v2/v3	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	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	8.8R1
Uboot Enable/Disable/Authenticate	8.7R3	8.7R3	8.7R3	8.9R2	8.7R3	N	8.7R3	8.7R3	N	N	8.7R3
UDLD	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	Y	N	X48C4E	EA
USB Disaster Recovery	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1 (onie)	Y	Y	8.7R1 (onie)	8.7R1 (onie)	Y
USB Flash (AOS)	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	Y	N	N	N
Virtual Chassis (VC)	8.7R2	8.5R2	Y	8.9R2	Y	8.7R1	Y	Y	8.5R2	8.7R1 (except X48C4E model)	Y (9907) N (9912)
Virtual Chassis Split Protection (VCSP)	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
VRF	N	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
VRF - IPv6	N	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
VRF - DHCP Client	N	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Web Services & CLI Scripting	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	Y	8.7R1	8.7R1	Y
Layer 3 Feature Support											
ARP	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
BFD	N	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
BGP	N	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
DHCP Client / Server	8.7R2	8.6R1	Y	8.9R2	Y	8.7R1	Y	Y	8.5R4	8.7R1	Y

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

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

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

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
802.1p / DSCP priority mapping	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
IPv4	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
IPv6	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	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	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	8.5R2	8.7R1	8.5R2
Groups - Port	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Groups - MAC	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Groups - Network	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Groups - Service	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Groups - Map	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Groups - Switch	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Ingress/Egress bandwidth limit	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Per port rate limiting	N	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	N
Policy Lists	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	Y	8.7R1	8.7R1	Y
Policy Lists - Egress	N	N	N	N	Y	8.7R1	Y	Y	8.7R1	8.7R1	N
Policy based routing	N	N	N	N	Y	8.7R1	Y	Y	8.6R2	8.7R1	EA
Tri-color marking	N	N	N	N	Y	8.7R1	Y	Y	N	N	N
QSP Profiles 1	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
QSP Profiles 2/3/4	N	N	N	QSP-2 Only	Y	QSP-2 only	Y	Y	QSP-2 only	QSP-2 only	N
QSP Profiles 5	8.7R2	8.5R1	Y	N	8.7R1	8.7R1	8.7R1	8.7R1 (X72)	N	N	Y
RoCEv2	N	N	N	N	N	N	N	N	8.7R2	N	N
Custom QSP Profiles	8.7R2	Y	Y	8.9R2	Y	Y	Y	X72 only (EA)	Y	Y	Y
GOOSE Messaging Prioritization	N	8.7R1	N	N	N	N	8.7R1	N	N	N	N
Metro Ethernet Features											

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6900	6900- V72/ C32	6900- X48C6/ T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
CPE Test Head	N	8.6R1	8.9R1 Metro	8.9R2	N	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	N
Ethernet Services (VLAN Stacking)	N	8.5R1	8.9R1 Metro	8.9R2	Y	8.7R2	Y	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	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	N
PPPoE Intermediate Agent	N	8.6R1	8.9R1 Metro	8.9R2	N	N	8.6R1	N	N	N	N
1588v2 End-to-End Transparent Clock	N	8.5R1	8.7R2	N	Y	8.9R3	Y	Y (X72/Q32)	8.9R3	8.9R3	N
1588v2 Peer-to-Peer Transparent Clock	N	8.8R2	8.7R2	N	N	N	N	N	N	N	N
1588v2 Across VC	N	N	N	N	N	N	N	8.5R2 (X72)	N	N	N
Access Guardian / Security Features											
802.1x Authentication	8.7R2	8.5R2	Y	8.9R2	Y	8.7R1	Y	Y	8.7R1	8.7R1	Y
Access Guardian - Bridge	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	Y	8.6R1	8.7R1	Y
Access Guardian - Access	N	N	N	N	Y	8.7R1	Y	Y	8.5R4	8.7R1	Y
Application Fingerprinting	N	N	N	N	N	N	N	Y	N	N	N
Application Monitoring and Enforcement (Appmon)	N	N	N	N	Y	8.7R2	N	N	N	N	N
ARP Poisoning Protection	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
BYOD - COA Extension support for RADIUS	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	8.62	8.6R2	8.7R1	Y
BYOD - mDNS Snooping/Relay	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	8.62	8.6R2	8.7R1	Y
BYOD - UPNP/DLNA Relay	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	8.62	8.6R2	8.7R1	Y
BYOD - Switch Port location information pass-through in RADIUS requests	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	8.62	8.6R2	8.7R1	Y
Captive Portal	8.7R2	8.5R4	Y	8.9R2	Y	8.7R1	Y	8.62	8.6R2	8.7R1	Y
IoT Device Profiling	8.7R2	8.5R2	8.5R2	8.9R2	8.5R2	8.7R1	8.5R2	8.5R2	8.6R1	8.7R1	8.5R2
IoT Device Profiling (IPv6)	8.7R2	8.7R1	8.7R1	8.9R2	8.7R1 ⁶	8.9R3	8.7R1 ⁶	8.7R1	8.9R3	8.9R3	8.7R1
Directed Broadcasts - Control	8.7R2	8.5R2	8.5R2	8.9R2	8.5R2	8.7R1	8.5R2	8.5R2	8.7R1	8.7R1	Y

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6900	6900- V72/ C32	6900- X48C6/ T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
Interface Violation Recovery	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	Y	8.7R1	8.7R1	Y
Kerberos Snooping (services)	8.7R2	Y	8.6R2	N	8.6R2	Y	8.6R2	8.6R2	8.6R2	Y	8.6R2
L2 GRE Tunnel Access (Edge) (bridge ports)	N	N	Y	N	Y	8.9R1	Y	8.6R1 ³	N	N	Y
L2 GRE Tunnel Access (Edge) (access ports)	N	N	N	N	8.6R1	8.9R1	8.6R1	8.6R1	8.7R1	8.7R2	8.6R1
L2 GRE Tunnel Aggregation	N	N	N	N	Y	8.9R1	Y	Y ³	8.7R1	8.7R2	Y
Learned Port Security (LPS)	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	Y	8.5R4	8.7R1	Y
MACsec ⁴	N	8.5R1	8.5R4	N	Y	8.7R1	N	N	N	X48C4E	8.5R2
MACsec MKA Support ⁴	N	8.5R2	8.5R4	N	8.5R2	8.7R1	N	N	N	X48C4E	8.5R2
MACsec on Network Port for SPB/L2GRE/VxLAN	N	N	N	N	8.9R1 (6860E)	8.9R1	N	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	8.7R2
RADIUS - RFC-2868 Support	8.7R2	8.5R4	8.5R4	8.9R2	8.5R4	8.7R1	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4
Role-based Authentication for Routed Domains	N	N	N	N	8.5R4	8.7R1	8.5R4	8.5R4	8.6R1	8.7R1	8.5R4
Storm Control (flood-limit)	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	Y	Y	8.7R1	Y
Storm Control (Unknown unicast with action trap/shutdown)	N	N	N	N	Y	N	Y	Y	N	N	N
TACACS+ Client	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	Y	8.6R1	8.7R1	Y
TACACS+ command based authorization	8.7R2	N	N	8.9R2	Y	8.7R1	Y	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	8.7R3
PoE Features											
802.3af and 802.3at	8.7R2	8.5R1	Y	N	Y	8.7R1	Y	N	N	N	Y
802.3bt	8.7R2	Y	8.6R2	N	N	8.7R1	N	N	N	N	N
Auto Negotiation of PoE Class-power upper limit	8.7R2	8.5R1	Y	N	Y	8.7R1	Y	N	N	N	Y
Display of detected power class	8.7R2	8.5R1	Y	N	Y	8.7R1	Y	N	N	N	Y
LLDP/802.3at power management TLV	8.7R2	8.5R1	Y	N	Y	8.7R1	Y	N	N	N	Y
HPOE support	8.7R2 (95W)	8.5R1 (60W)	Y (95W)	N	Y (60W)	8.7R1 (95W)	Y (75W)	N	N	N	Y (75W)
Time Of Day Support	8.7R2	8.5R1	Y	N	Y		Y	N	N	N	Y
Perpetual PoE	8.7R2	N	N	N	Y	Y	Y	N	N	N	N

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
Fast PoE	8.7R2	N	N	N	Y	Y	Y	N	N	N	N
Delayed Start	8.9R3	8.9R3	8.9R3	N	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	Y	N	N	N
Data Center Bridging (DCBX/ETS/PFC)	N	N	N	N	N	N	N	Y	N	N	N
EVB	N	N	N	N	N	N	N	N	N	N	N
FCoE / FC Gateway	N	N	N	N	N	N	N	Y	N	N	N
VXLAN ⁵	N	N	N	N	N	8.8R1	N	Q32/X72	8.5R3	8.8R1	N
VM/VXLAN Snooping	N	N	N	N	N	N	N	Y	N	N	N
FIP Snooping	N	N	N	N	N	N	N	Y	N	N	N

Notes:
 1. OS6560 supports stub area only.
 2. See protocol support table in Appendix C.
 3. Not supported on 6900-T20/T40/X20/X40.
 4. Site license required beginning in 8.6R1.
 5. L2 head-end only on OS6900-V72/C32.
 6. HTTP IPv6 only supported on OS6860(E) and OS6865

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	Not Supported
OmniSwitch 6900	
OS6900-X48C4E	Dynamic mode only on all ports. Supports 256-bit key length.
OmniSwitch 6860(E)	
OS6860(E)	All models support MACsec on 10G ports.
OS6860E-P24	1G/10G ports.
OS6860E-P24Z8	1G/10G ports (not supported on 2.5G ports).
OmniSwitch 6860N	
OS6860N-U28	SFP (1-24), SFP+ (25-28) and SFP28 (31-34) ports
OS6860N-P48Z	SFP28 (51-54) ports
OS6860N-P48M	- Expansion modules (Not supported on any 4X10G splitter transceivers). - Multi-rate Gigabit Ports (37-48)
OS6860N-P24Z	SFP28 (27-30) ports
OS6860N-P24M	- Expansion modules (Not supported on any 4X10G splitter transceivers) - Multi-rate Gigabit Ports (1-24)
OmniSwitch 6560	
OS6560-P24X4/24X4	- Ports 1-24 (Static and Dynamic modes) - Ports 25-30 (Not Supported)
OS6560-P48X4/48X4	- Ports 1-48 (Static and Dynamic modes) - Ports 49-52 (Dynamic mode only) - Ports 53-54 (Not Supported)
OS6560-P48Z16 (904044-90 only)	- Ports 1-32 (Static and Dynamic Modes) - Ports 33-48 (Static and Dynamic modes) - Ports 49-52 (Dynamic mode only) - Ports 53-54 (Not Supported)
OS6560-X10	- Ports 1-8 (10G ports only. Dynamic mode only) - Ports 9-10 (Not Supported)
OmniSwitch 6465	
	- OS6465-P28 - supported on all ports except ports 27 and 28.

	- OS6465T-12 and OS6465T-P12 - Not supported on ports 11 and 12. - All other models support MACsec on all ports.
--	---

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

Guidelines

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

Inline Routing Support							
	OmniSwitch 9900	OmniSwitch 6900-V72/C32 (Front panel port)	OmniSwitch 6900-T48C6/X48C6	OmniSwitch 6900-X48C4E/V48C8	OmniSwitch 6900-C32E	OmniSwitch 6860N	OmniSwitch 6900-X/T24C2
IPv4 Protocols							
Static Routing	Y	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
RIP v1/v2	Y	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
OSPF	Y	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
BGP	Y	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
VRRP	Y	8.7R1	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
IS-IS	N	N	N	N	N	N	N
PIM-SM/DM	8.5R3	8.6R2	Y	Y	8.8R1	Y	8.9R1
DHCP Relay	8.5R3	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
UDP Relay	8.5R4	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
DVMRP	N	N	N	N	N	N	N
BFD	8.7R2	8.7R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
IGMP Snooping	Y	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
IP Multicast Headend Mode	Y	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
IP Multicast Tandem Mode	8.5R4	8.6R2	8.8R1	8.8R1	8.8R1	8.8R1	8.9R1
IPv6 Protocols							
Static Routing	8.5R4	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
RIPng	8.5R4	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
OSPFv3	8.5R4	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
BGP	8.5R4	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
VRRPv3	8.5R4	8.7R1	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
IS-IS	N	N	N	N	N	N	N
PIM-SM/DM	8.5R4	8.6R2	8.8R1	8.8R1	8.8R1	8.8R1	8.9R1
DHCP Relay	8.6R1	8.7R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
UDP Relay	8.6R1	8.7R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
BFD	8.7R2	8.7R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
IPv6 MLD Snooping	Y	8.7R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
IPv6 Multicast Headend Mode	Y	8.7R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1
IPv6 Multicast 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	OmniSwitch 6900-V72/ C32	OmniSwitch 6900-X48C6/ T48C6	OmniSwitch 6900-X48C4E	OmniSwitch 6900-V48C8	OmniSwitch 6900- X/T48C2
IPv4 Protocols									
Static Routing	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
RIP v1/v2	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
OSPF	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
BGP	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
VRRP	8.6R1	8.5R4	8.7R1	Y	8.7R1	8.7R2	8.7R2	8.7R3	8.9R1
IS-IS	Y	Y	Y	Y	Y	Y	8.7R2	8.7R3	8.9R1
PIM-SM/DM	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
DHCP Relay	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
UDP Relay	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
DVMRP	N	N	N	N	N	N	N	N	N
BFD	Y	Y	Y	Y	Y	Y	8.7R2	8.7R3	8.9R1
IGMP Snooping	8.5R4	Y	8.7R1	Y	8.6R1	8.7R1	8.7R2	8.7R3	8.9R1
IP Multicast Headend Mode	8.5R4	Y	8.7R1	Y	8.6R1	8.7R1	8.7R2	8.7R3	8.9R1
IP Multicast Tandem Mode	8.5R4	Y	8.7R1	Y	8.6R1	Y	Y	Y	8.9R1
IPv6 Protocols									
Static Routing	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
RIPng	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
OSPFv3	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
BGP	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
VRRPv3	8.5R4	8.5R4	8.7R1	Y	8.7R1	8.7R2	8.7R2	8.7R3	8.9R1
IS-IS	Y	Y	Y	Y	Y	Y	8.7R2	8.7R3	8.9R1
PIM-SM/DM	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
DHCP Relay	8.6R1	8.6R1	8.7R1	8.6R1	8.6R1	8.7R1	8.7R2	8.7R3	8.9R1
UDP Relay	8.6R1	8.6R1	8.7R1	8.6R1	8.6R1	8.7R1	8.7R2	8.7R3	8.9R1
BFD	Y	Y	Y	Y	Y	Y	8.7R2	8.7R3	8.9R1
IPv6 MLD Snooping	8.5R4	Y	8.7R1	Y	Y	8.7R2	8.7R2	8.7R3	8.9R1
IPv6 Multicast Headend Mode	8.5R4	Y	8.7R1	Y	Y	8.7R2	8.7R2	8.7R3	8.9R1
IPv6 Multicast Tandem Mode	8.5R4	Y	8.7R1	Y	Y	Y	Y	Y	8.9R1

SPB BVLAN Scalability and Convergence Guidelines

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

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

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

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

```
OS6860-> show spb isis bvlans
SPB ISIS BVLANS:
```

Root Bridge						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 8.9R3 (GA)
OS6360	8.9.107.R02 (Minor GA) 8.9.73.R01 (Major GA) 8.8.56.R02 (Minor GA) 8.8.152.R01 (Major GA)
OS6360-P10A	8.9.107.R02 (Minor GA) 8.9.73.R01 (Major GA) 8.8.8.R03 (Minor GA) - Note: Uses same image file as other OS6360 platforms.
OS6465	8.9.107.R02 (Minor GA) 8.9.73.R01 (Major GA) 8.8.56.R02 (Minor GA) 8.8.152.R01 (Major GA)
OS6560	8.9.107.R02 (Minor GA) 8.9.73.R01 (Major GA) 8.8.56.R02 (Minor GA) 8.8.152.R01 (Major GA)
OS6570M	8.9.107.R02 (Minor GA) 8.9.63.R02 (Major GA)
OS6860(E)	8.9.107.R02 (Minor GA) 8.9.73.R01 (Major GA) 8.8.56.R02 (Minor GA) 8.8.152.R01 (Major GA)
OS6860N*	8.9.107.R02 (Minor GA) 8.9.73.R01 (Major GA) 8.8.56.R02 (Minor GA) 8.8.153.R01 (Major GA)
OS6865	8.9.107.R02 (Minor GA) 8.9.73.R01 (Major GA) 8.8.56.R02 (Minor GA) 8.8.152.R01 (Major GA)
OS6900	8.9.107.R02 (Minor GA) 8.9.78.R01 (Major GA) 8.8.56.R02 (Minor GA) 8.8.152.R01 (Major GA)
OS6900-V72/C32/ X48C6/T48C6/X48C4E/V48C8	8.9.107.R02 (Minor GA) 8.9.78.R01 (Major GA) 8.8.56.R02 (Minor GA) 8.8.153.R01 (Major GA) 8.8.152.R01 (Major GA)
OS9900	Due to the required changes to support the new OS9912 model, ISSU is not supported from any prior release.

8.9R3 ISSU Supported Releases

Prerequisites

These upgrade instructions require that the following conditions exist, or are performed, before upgrading. The person performing the upgrade must:

- Be the responsible party for maintaining the switch's configuration.
- Be aware of any issues that may arise from a network outage caused by improperly loading this code.
- Understand that the switch must be rebooted and network access may be affected by following this procedure.
- Have a working knowledge of the switch to configure it to accept an FTP connection through the EMP or Network Interface (NI) Ethernet port.
- Read the GA Release Notes prior to performing any upgrade for information specific to this release.
- Ensure there is a current certified configuration on the switch so that the upgrade can be rolled-back if required.
- Verify the current versions of U-Boot and FPGA. If they meet the minimum requirements, (i.e. they were already upgraded during a previous AOS upgrade) then only an upgrade of the AOS images is required.
- Depending on whether a standalone chassis or VC is being upgraded, upgrading can take from 5 to 20 minutes. Additional time will be needed for the network to re-converge.
- The examples below use various models and directories to demonstrate the upgrade procedure. However, any user-defined directory can be used for the upgrade.
- If possible, have EMP or serial console access to all chassis during the upgrade. This will allow you to access and monitor the VC during the ISSU process and before the virtual chassis has been re-established.
- Knowledge of various aspects of AOS directory structure, operation and CLI commands can be found in the Alcatel-Lucent OmniSwitch User Guides. Recommended reading includes:
 - Release Notes - for the version of software you're planning to upgrade to.
 - The AOS Switch Management Guide
 - Chapter - Getting Started
 - Chapter - Logging Into the Switch
 - Chapter - Managing System Files
 - Chapter - Managing CMM Directory Content
 - Chapter - Using the CLI
 - Chapter - Working With Configuration Files
 - Chapter - Configuring Virtual Chassis

Do not proceed until all the above prerequisites have been met. Any deviation from these upgrade procedures could result in the malfunctioning of the switch. All steps in these procedures should be reviewed before beginning.

Switch Maintenance

It's recommended to perform switch maintenance prior to performing any upgrade. This can help with preparing for the upgrade and removing unnecessary files. The following steps can be performed at any time prior to a software upgrade. These procedures can be done using Telnet and FTP, however using SSH and SFTP/SCP are recommended as a security best-practice since Telnet and FTP are not secure.

1. Use the command **'show system'** to verify current date, time, AOS and model of the switch.

```
6900-> show system
System:
Description: Alcatel-Lucent OS6900-X20 8.6.289.R01 GA, July 14, 2019.,
Object ID: 1.3.6.1.4.1.6486.801.1.1.2.1.10.1.1,
Up Time: 0 days 0 hours 1 minutes and 44 seconds,
Contact: Alcatel-Lucent, http://alcatel-lucent.com/wps/portal/enterprise,
Name: 6900,
Location: Unknown,
Services: 78,
Date & Time: MON AUG 12 2019 06:55:43 (UTC)
Flash Space:
Primary CMM:
Available (bytes): 1111470080,
Comments : None
```

2. Remove any old `tech_support.log` files, `tech_support_eng.tar` files:

```
6900-> rm *.log
6900-> rm *.tar
```

3. Verify that the `/flash/pmd` and `/flash/pmd/work` directories are empty. If they have files in them check the date on the files. If they are recently created files (<10 days), contact Service & Support. If not, they can be deleted.

4. Use the **'show running-directory'** command to determine what directory the switch is running from and that the configuration is certified and synchronized:

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

If the configuration is not certified and synchronized, issue the command **'write memory flash-synchro'**:

```
6900-> write memory flash-synchro
```

6. If you do not already have established baselines to determine the health of the switch you are upgrading, now would be a good time to collect them. Using the `show tech-support` series of commands is an excellent way to collect data on the state of the switch. The `show tech support` commands automatically create log files of useful `show` commands in the `/flash` directory. You can create the tech-support log files with the following commands:

```
6900-> show tech-support
6900-> show tech-support layer2
6900-> show tech-support layer3
```

Additionally, the **'show tech-support eng complete'** command will create a TAR file with multiple tech-support log files as well as the SWLOG files from the switches.

```
6900-> show tech-support eng complete
```

It is a good idea to offload these files and review them to determine what additional data you might want to collect to establish meaningful baselines for a successful upgrade.

- If upgrading a standalone chassis or VC using a standard upgrade procedure please refer to [Appendix E](#) for specific steps to follow.
- If upgrading a VC using ISSU please refer to [Appendix F](#) for specific steps to follow.

Appendix E: Standard Upgrade - OmniSwitch Standalone or Virtual Chassis

These instructions document how to upgrade a standalone or virtual chassis using the standard upgrade procedure. Upgrading using the standard upgrade procedure consists of the following steps. The steps should be performed in order:

1. Download the Upgrade Files

Go to the Service and Support website and download and unzip the upgrade files for the appropriate model and release. The archives contain the following:

- OS6360 - Nosa.img
 - Refer to [Appendix G](#) for recommended/required FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6465 - Nos.img
 - Refer to [Appendix G](#) for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6560 - Nos.img
 - Refer to [Appendix G](#) for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6860 - Uos.img
 - Refer to [Appendix G](#) for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6860N - Uosn.img
 - Refer to [Appendix H](#) for recommended CPLD upgrades. AOS must be upgraded prior to upgrading the CPLD.
- OS6865 - Uos.img
 - Refer to [Appendix G](#) for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6900 - Tos.img
 - Refer to [Appendix G](#) for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6900-V72/C32/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
-----+-----+-----+-----
Tos.img          8.9.107.R02     239607692 Alcatel-Lucent OS

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

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

5. Certify the Software Upgrade

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

```
OS6900-> copy running certified

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

Appendix 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.
- 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 - Tos.img
 - Refer to [Appendix G](#) for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6900-V72/C32/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
```

Chas	MAC-Address	Local IP	Remote IP	Status
1	e8:e7:32:b9:19:0b	127.10.2.65	127.10.1.65	Connected

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

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

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

```
6900-> rm -r /flash/issu_dir
```

6. Log out of the Slave chassis:

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

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

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

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

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

9. Upgrade the image files using ISSU:

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

During ISSU `'show issu status'` gives the respective status (pending, complete, etc)

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

This indicates that the ISSU is completed

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

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

```
6900-> debug show virtual-chassis topology
Local Chassis: 1
Oper
Chas  Role      Status      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
-----+-----+-----+-----
Tos.img      8.9.107.R02 239607692 Alcatel-Lucent OS
```

11. Certify the Software Upgrade

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

```
OS6900-> 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
CRAOS8X-11118	Description	1000BaseT SFP interface up before system ready
	U-boot/FPGA Version	- U-boot version 8.6.R02.189 - FPGA version 0.1.11
	Platforms	OS6900-X72
Fast/Perpetual PoE	Description	Fast and Perpetual PoE Support
	FPGA Version	0.7 (OS6860E-P24Z8) 0.10 0.14 (OS6865-U28X) 0.25 (OS6865-P16X/U12X)
	Platforms	OS6860/OS6865
8.7R2 Release		
CRAOS8X-4813/13440	Description	Uboot unable to mount NAND flash with UBIFS errors
	U-boot Version	8.7.2.R02
	Platforms	OS6465(T), 6560-24X4/P24X4/48X4/P48X4/X10
CRAOS8X-13819	Description	Uboot unable to mount eUSB flash
	U-boot Version	8.7.2.R02
	Platforms	OS6560-24Z24/P24Z24/24Z8/P24Z8/P48Z16 (all PNs), 6865
CRAOS8X-22857	Description	OS6560-P24Z24 reloads continuously with 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	Uboot update for CRAOS8X-24464, ability to disable / authenticate uboot access.
	Uboot Version	8.7.30.R03
	Platforms	OS6360, 6465, 6560, 6860, 6865, 6900, 9900. (Not applicable for platforms that use ONIE)
8.8R1 Release		
Boot from USB	Description	Uboot update to allow switch to boot from USB.
	Uboot Version	8.8.33.R01
	Platforms	OS6465, OS6865
8.8R2 Release		
Future compatibility	Description	Uboot/FPGA update to allow future CMM2/OS9912 NI compatibility.
	Uboot/FPGA Versions	See OS9900 Table for versions.
	Platforms	9907
8.9R1 Release		
N/A	There are no Uboot/FPGA upgrade requirements in this release.	
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	Uboot fix for NAND flash bad file system block. Support of Gowin CPLD ¹
	Uboot	8.9.85.R02
	Platforms	OS6360 (All)
CPLD Support	Description	Support of Gowin CPLD ¹
	Uboot	8.9.92.R02
	Platforms	OS6570M-12/12D/U28
CRAOS8X_35470	Description	Uboot fix for NAND flash bad file system block
	Uboot/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 uboot access.
	Uboot 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

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_8405
- U-boot.8.9.R02.85.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_8405
Parse /flash/fpga_kit_8405
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.R02.85.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
No other CPLD upgrades are available or required.		
Notes:		
<ol style="list-style-type: none"> Upgrading the CPLD on ONIE-based models is only supported beginning with AOS Release 8.8.R02 and when using the AOS command procedure. Any other procedure to upgrade the CPLD may damage the switch and void the warranty. CPLD versions are compatible with previous AOS releases. Downgrading to a previous AOS release is supported: <ol style="list-style-type: none"> Backup the configuration files from previous release. Upgrade to AOS Release 8.8.R02. Upgrade the CPLD. Downgrade to previous release. (ISSU is not supported when downgrading AOS) Restore the configuration. 		

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

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

- CPLD File - *.updater

2. Ensure the configuration is certified and synchronized prior to upgrading the CPLD.

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

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




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




5. Once complete, a reboot is required. (In some cases multiple reboots may be required).






6. If the switch reboots to the 'Certified' directory use the 'reload from *running-directory* no rollback-timeout' command to reboot from the desired directory.






Appendix I: Fixed Problem Reports




The following problem reports were closed in this release.





CR/PR NUMBER	Description
<p>Case: 00671702 CRAOS8X-37499</p>	<p>Summary: The following messages are flooding the switch logs: kernel [16525.569864] alv4if_rcv: missing ifindex 400 cnt 9290 kernel [16525.569884] flow 0x0 type 0x800 port 0x11 kernel [16525.569901] dstmac 2c:fa:a2:xx:xx:xx srcmac 2c:fa:a2:yy:yy:yy kernel [16525.569918] 0x45000034 0x188b4000 0x7b062a21 0xa0807ef 0xac1fff01</p> <p>Explanation: These messages do not indicate any functionality impact. Code changes have been made so that these logs will not be displayed.</p> <p> Click for Additional Information</p>
<p>Case: 00687516 CRAOS8X-38753</p>	<p>Summary: The message "swlogd svcNi mSVC INFO: SVCN STATS Config: Op Copy Obj 3" is seen repeatedly in the switch logs.</p> <p>Explanation: The message "swlogd svcNi mSVC INFO: SVCN STATS Config: Op Copy Obj 26" is shown during service stats collection. It does not indicate any functional impact. It will be logged while collecting the stats either via the "snmpwalk" or via the <show service spb service_id counters> command. Code changes have been made to move these messages from "info" to "debug1" logging level during service stats collections.</p> <p> Click for Additional Information</p>
<p>Case: 00691563 CRAOS8X-39197</p>	<p>Summary: AOS 8.X switches are sending the pause frame with SRC MAC address 00:00:00:00:00:00</p> <p>Explanation: In AOS 8.X switches in pause frame source MAC is not correctly update with the switch chassis MAC. Changes are made to update the pause frame with source MAC as chassis MAC.</p> <p> Click for Additional Information</p>
<p>Case: 00686797 CRAOS8X-38631</p>	<p>Summary: Before captive-portal authentication, clients are unable to get IP address though MAC-authentication is successful. DHCP offer is not forwarded to these clients. This issue is noticed when UNP redirect is configured and DHCP snooping is enabled.</p> <p>Explanation: During BYOD state, that is restricted role state when the client is transitioning from mac-authenticated success to captive-portal authentication stage, the TCAM rule for Access-Guardian (AG) did not trap the DHCP discover packets which leads to TCAM rule for DHCP snooping not hit and dropped DHCP offer packets from forwarding to the client.</p>





	<p>Corrections are made to have TCAM rule for DHCP snooping to be hit and trap the DHCP discover packets correctly to forward the DHCP offer packets to the client after it is MAC-authenticated successfully before captive-portal authentication.</p> <p> Click for Additional Information</p>
<p>Case: 00679990 CRAOS8X-38140</p>	<p>Summary: In OS6860N when executing the “qos revert” command, error messages are seen.</p> <p>“Qos revert” command is used to remove all the Qos configuration which is not yet applied with “Qos apply” command.</p> <p>However, “Qos revert” command on execution gave the following error:</p> <pre>tcamni main ERR message: +++ : [tcDbError:227] : tnDbTnCounterIdxToRuleDupState:4130 Database error 19, UNIQUE constraint failed: TnCounterIdxToRule.Tcam, TnCounterIdxToRule.State, TnCounterIdxToRule.CounterIdx, TnCounterIdxToRule.ConId, TnCounterIdxToRule.SplitId +++ : [tcDbError:227] : tnDbTnCounterIdxToRuleDupState:4134 Database error 19, UNIQUE constraint failed: TnCounterIdxToRule.Tcam, TnCounterIdxToRule.State, TnCounterIdxToRule.CounterIdx, TnCounterIdxToRule.ConId, TnCounterIdxToRule.SplitId +++ : [tnResourceRevertPendingFifo:9333] : TCAM_RET_GEN_ERR +++ : [tnHandleResourceRevertPendingFifo:9527] : Invalid resourceId = 3 +++ : [tnApiResourceReqHandle:328] : TcOperRevert</pre> <p>Explanation: The 'tcamni' error messages were seen when the command was executed.</p> <p>Corrections are made to revert the Qos commands configured which is remove the Qos configuration done before applying the “Qos apply” command.</p> <p> Click for Additional Information</p>
<p>Case: 00673148 CRAOS8X-37538</p>	<p>Summary: Are Alcatel 8x switches vulnerable to CVE-2022-4203, CVE-2023-0401, CVE-2023-0216, CVE-2022-4450, and CVE-2022-4304?</p> <p>Explanation: Fix is given in AOS 8.9R03 with an upgrade of Open SSL version to 3.0.8.</p> <p> Click for Additional Information</p>
<p>Case: 00685281 CRAOS8X-38454</p>	<p>Summary: In OS6860E, the following error messages is seen when SNMP trap absorption function is in use.</p> <p>“trapmgr trapmgr_main ERR ERR: [ERROR] FUNCTION trap_system_free LINE 304”</p> <p>Explanation: When absorption traps are enabled, initially, all traps sent within a 15-second window are consolidated into one trap. However, the consolidation did not occur after the first 15 seconds had elapsed.</p>






	<p>A code fix has been provided in build 8.9.R03 to regulate SNMP traps and ensure that the consolidation continues to work correctly throughout the 15-second interval, not just within the first 15 seconds</p> <p> Click for Additional Information</p>
<p>Case: 00687567 <i>CRAOS8X-38892</i></p>	<p>Summary: Login with "secureadmin" via SSH end up in maintenance mode (su) rather than CLI.</p> <p>Explanation: A code correction has been made so that when logging in with 'secureadmin' via SSH, it will now log in to the CLI (Command Line Interface) rather than su mode</p> <p> Click for Additional Information</p>
<p>Case: 00674396 <i>CRAOS8X-37642</i></p>	<p>Summary: In AOS 8.x switches, the CLI command “show spantree vlan <vlan ID> blocking” in STP FLAT mode displays forwarding ports as blocking.</p> <p>Explanation: VLAN and VLAN ID in “show spantree” commands are to be used when the STP mode is per-vlan and it is not applicable to FLAT mode. The command to check the STP blocking state is "show Spantree ports blocking" when the switches are running in FLAT mode.</p> <p>Fix is given to provide the warning message "INACTIVE Spanning Tree Parameters for VLAN" will be added on top of the show command "show spanning tree VLAN ports blocking" output.</p> <p> Click for Additional Information</p>
<p>Case: 00697725 <i>CRAOS8X-38497</i></p>	<p>Summary: The switch rebooted and stuck in ONIE menu</p> <p>Explanation: The OS6860n_p48m_p48z_u28_maincpu_20220318.updater is a mixed CPLD, and CPU CPLD update file that cannot recognize the different CPU CPLD in the new revision hardware, hence the switch is stuck in ONIE during the upgrading process.</p> <p>Starting with AOS 8.9.R03, AOS will be able to check the CPU CPLD chip and stage correct upgrade code.</p> <p> Click for Additional Information</p>
<p>Case: 00674633 <i>CRAOS8X-37819</i></p>	<p>Summary: OS6900: OVC provision failed due to “Callhome-failure”.</p> <p>Explanation: When the OS6900 is booted up in Standalone mode, the callhome failure is noticed. This issue is fixed from 8.9R03.</p> <p> Click for Additional Information</p>
<p>Case:</p>	<p>Summary:</p>






<p>00688329 <i>CRAOS8X-38813</i></p>	<p>The OS6900-X20 switch is in version 8.7R02 and has a display issue for show spantree outputs</p> <p>Explanation: The STP port status is in forwarding status, even after disabling the STP for that port. Fix is enhanced in AOS 8.9R03 for the display issue.</p> <p> Click for Additional Information</p>
<p>Case: 00669313 00693995, 00684161, 00695181 <i>CRAOS8X-40115,</i> <i>CRAOS8X-37235</i></p>	<p>Summary: AOS 8.X switches are unable to download the configuration from SolarWinds due to a mismatch in supported algorithms and ciphers. The SolarWind was using ssh-rsa key generation, which was disabled in the AOS switch.</p> <p>Explanation: The ssh-rsa (rsa-sha2-512 & rsa-sha2-256) has been disabled by default in AOS switches until AOS 8.9R02. Fix is given to support ssh-rsa keys.</p> <p> Click for Additional Information</p>
<p>Case: 00694772 <i>CRAOS8X-39578</i></p>	<p>Summary: In CLI guide , MIB is mentioned as chasHardwareBoardTemp instead of chasNI1HardwareBoardTemp.</p> <p>Explanation: The alcatel.tree file in the AOS 8.7R02 MIBS file has the correct MIBs for "temperature" reading. The CLI guide of AOS 8.9R03 will be corrected to reflect the chasNI1HardwareBoardTemp to chasNI8HardwareBoardTemp under MIB objects section.</p> <p> Click for Additional Information</p>
<p>Case: 00694878 <i>CRAOS8X-39560</i></p>	<p>Summary: Special character "!" is not accepted in AOS 8X switches.</p> <p>Explanation: Fix is given to accept this “!” special character.</p> <p> Click for Additional Information</p>
<p>Case: 00681845 <i>CRAOS8X-38429</i></p>	<p>Summary: The SFP-GIG-BX-U/-D modules from the manufacturer "ATOP" are incompatible with the OS6900-V48C8 switches on the AOS 8.9.R02.</p> <p>Explanation: Below error message is seen in swlogs : swlogd intfNi Drv ERR: Unsupported Dual Speed SFP plugged in SFP+ cage, in port 2/1/33</p> <p>Code changes are done to make ATOP SFPs compatible for OS6900-V48C8 model.</p> <p> Click for Additional Information</p>
<p>Case:</p>	<p>Summary:</p>




<p>00676760, 00706014, 00707664, 00698967</p> <p><i>CRAOS8X-38004,</i> <i>CRAOS8X-37850</i></p>	<p>Machines that are connected to OS6560 access switches, are unable to download files of more than 80MB from the internet or inside the network in 8.9.R01</p> <p>Explanation: Incorrect TCAM rules were hit when the host traffic was received in the switch. Code changes are done in TCAM rules to avoid this issue.</p> <p> Click for Additional Information</p>
<p>Case: 00685119 <i>CRAOS8X-38587</i></p>	<p>Summary: Logs displaying erroneous messages as given below For testOam swlogd toamCmm TCAM ERR: testOamHWLBTCamCountReadOrClear(9431): chassis: 1 slot 1</p> <p>For Power supply swlogd ChassisSupervisor fpgaMgr INFO: ps change, psMask 1, PS 1 status 0 PS 2 status 1</p> <p>Explanation: For power supply, these power supply logs are displayed only when there is change in the status, but we were displaying it for all the polling intervals even if there is no change.</p> <p>For testoam logs, it's the log needed to be at the debug level, to log the details of the chassis and the slot number during the periodic counter read.</p> <p>Fix is given to display the power supply logs when there is a change. Fix is given to move the testOam log to debug level</p> <p> Click for Additional Information</p>
<p>Case: 00708190 <i>CRAOS8X-41335</i></p>	<p>Summary: TDR feature is not supported in ports 1/1/33- 1/1/48 in OS6560-P48Z16 Example: # interfaces 1/1/42 tdr enable ERROR: TDR is not supported on port (1/1/42)</p> <p>Explanation: For the switch OS6560-P48Z16, the TDR feature is not supported only in ports 1/1/33-1/1/48 and the below error message is thrown while executing this command.</p> <p>TDR is supported on 1G copper ports in 6360/6465/6560 platforms.</p> <p>OS6560_P24Z8 model does not support TDR on ports 17 to 24. OS6560_P48Z16E model does not support TDR on ports 33 to 48. OS6560_(P)24Z24 and OS6560_P48Z16 models do not support TDR. OS6360_PH24 and OS6360_P24X models do not support TDR on ports 25 and 26. OS6360_P48X model does not support TDR on ports 49 and 50.</p> <p> Click for Additional Information</p>
<p>Case: 00685098 <i>CRAOS8X-38427</i></p>	<p>Summary: FTP is not working as expected with read-only CLI/FTP credentials in AOS 8.X switches.</p> <p>Explanation:</p>






	<p>Fix is given to allow FTP of files of AOS 8X switches using read-only access for the users created in the switch.</p> <p> Click for Additional Information</p>
<p>Case: 00693942 CRAOS8X-39763</p>	<p>Summary: Getting lpcmm error in switch log.</p> <p>LanCmmMip INFO: lpalaPethPowerPolicyTableGetNext 7136: No Next Policy Found LanCmmMip WARN: lpalaPethPowerPortTableGetNext 7754: Chassis 1 Slot 1 Port 9 does not exist</p> <p>Explanation: Switch logs are filling with lpcmm warn messages. The same behavior was observed in the release 8.9.107.R02. Code changes are done in 8.9.R03 to change these logs to debug level. The unwanted logging issue will be fixed in 8.9.R03.</p> <p> Click for Additional Information</p>
<p>Case: 00681790 CRAOS8X-38207</p>	<p>Summary: The switch showed ERROR: Unable to retrieve VFC snapshot.</p> <p>Explanation: Upon executing the “show configuration snapshot” and then the “write memory flash-synchro” commands, not able to view or save the configuration of a working OS6560-48X4 switch and got the error: “ERROR: Unable to retrieve VFC snapshot”.</p> <p>The code changes were done for the optimization correction of better socket reconnection between vfc and mipgwd application.</p> <p> Click for Additional Information</p>
<p>Case: 00674864 CRAOS8X-37897</p>	<p>Summary: PS status shows the wrong airflow.</p> <p>Explanation: While inserting the PS in the running chassis with AOS 8.7.98R03, the PS was flagged with the wrong airflow (Front to Rear), however, the power supply was accepted by the chassis. If the PS is inserted without a power source connected, then the wrong airflow (Rear to Front) is detected. However, removing the PS, and re-plugging it while the Power Cord is inserted into the PS shows the correct airflow (Front to Rear).</p> <p>Fix is given to correct the PS status display of airflow.</p> <p> Click for Additional Information</p>






<p>Case: 00671192 <i>CRAOS8X-38061</i></p>	<p>Summary: Port level LLDP-Configuration is not saved in 6900-T48C6.</p> <p>Explanation: In the OS6900-T48C6 model switch the port level lldp configuration is disabled for a port after the switch reloads. Even if the configuration is saved and synchronized in the switch.</p> <p>Fix is given to retain the LLDP port configuration when saved and rebooted the switch.</p> <p> Click for Additional Information</p>
<p>Case: 00702651 <i>CRAOS8X-40560</i></p>	<p>Summary: The CLI command “no-autoload-vrrp command” is not documented.</p> <p>Explanation: This command will stop the auto loading of VRRP “ip load vrrp” command upon reboot of the switch.</p> <p> Click for Additional Information</p>
<p>Case: 00694188 <i>CRAOS8X-39572</i></p>	<p>Summary: When LPS is enabled on the UNP ports and the mobile tag is enabled on the profile, the incorrect VPA is assigned.</p> <p>Explanation: When LPS is enabled on the UNP port, after the classification the Profile context is removed and the user is learnt as Pseudostatic, however the switch does not check for mobile tag status before creating the VPA. This is the reason the ports are untagged. This is due to a bug in AOS. The issue is fixed in AOS 8.9 R03</p> <p> Click for Additional Information</p>
<p>Case: 00673072 <i>CRAOS8X-37507</i></p>	<p>Summary: OS6860N-P48Z : Auto-negotiation not supported with 1G fiber SFP</p> <p>Explanation: When a 1G fiber SFP is connected to a OS6860N-P48Z switch, the following error log is thrown on the console:</p> <p>Fri Feb 10 15:06:12 : intfCmm Mgr INFO message:</p> <p>+++ 1Gig SFP 2/1/51 Disable peer port auto-negotiation for proper port connection support.</p> <p> Click for Additional Information</p>
<p>Case: 00668375 <i>CRAOS8X-37255</i></p>	<p>Summary: OS6860N-P48Z: Policy rule does not match the expected traffic</p> <p>Explanation: A policy rule to match and allow traffic from specific subnets and destined to the switch is active. However, the traffic is not matched.</p>





	<p> Click for Additional Information</p>
<p>Case: 00673743 CRAOS8X-37685</p>	<p>Summary: MVRP update message to add a VLAN is discarded</p> <p>Explanation: OS6860E: Connectivity issue arising from MVRP Update message discard in VLAN Configuration</p> <p> Click for Additional Information</p>
<p>Case: 00678619 CRAOS8X-38033</p>	<p>Summary: Either INPUT or OUPUT Ifindex field is updated for OS6900-V72 in third party NMS Live interface statistics</p> <p>Explanation: According to the 8X design, unknown unicast, broadcast and multicast packets will have either the SFLOW input or output ifindex. Enhancement made to populate the Ifindex Input and Output values in standalone switches [Not in VC] for unknown unicast and broadcast packets other than multicast. Product Enhancement request should be made in order to implement the Ifindex INPUT and OUTPUT value for VC and Multicast packets.</p> <p> Click for Additional Information</p>
<p>Case: 00666832 CRAOS8X-37085</p>	<p>Summary: LPS MAC goes to filtering after unplug/replug though port-security is disabled on the port</p> <p>Explanation: Port security with "Learn-as-static" and the settings "802.1x" and "fallback to unauthorized network access" are enabled on the PC. Even after deleting the static MAC and disabling port security, MAC still displays as filtering as opposed to bridging post toggling. The reason is "The switch processes the initial EAP packet even when UNP is not configured when LPS is deactivated.</p> <p> Click for Additional Information</p>
<p>Case: 00627569 CRAOS8x-33972</p>	<p>Summary: Some PD devices connected to POE ports and using external power source will be lanpower faulty intermittently , for Underload State reason without administrators even knowing about it.</p> <p>Explanation: Thanks to a SNMP Trap generated (when Faulty lanpower port for Underload State occurs), Administrators will be able to take action (disable lanpower on the port or remove the external power source from the PD device.</p> <p> Click for Additional Information</p>
<p>Case: 00657944 CRAOS8X-36480</p>	<p>Summary: OS6900-X48C6: No link light and connection between 10GIG Copper SFP and 1GIG "Intel I219-lm" NIC.</p> <p>Explanation:</p>





	<p>In OS6900-X48C6, laptop is connected on the switch port with "SFP-10G-T". The link between the devices stays DOWN and the port LED is also DOWN. In laptop, the NIC used is 1GIG "Intel I219-lm". In phy, the switch advertises only 1000MB and 10000MB.</p> <p> Click for Additional Information</p>
<p>Case: 00660777 CRAOS8X-36651</p>	<p>Summary: OS6900-X48C6: Response to NTP Request from Slave chassis is marked as "bogus packet" by Master chassis.</p> <p>Explanation: With NTP server configured to sync time, it is noticed that the NTP request is initiated from both Master and Slave chassis to the UDP port 123. Even though the NTP request was initiated by chassis-2 (Slave), the response from the NTP server is sent to Chassis-1 (Master). So, the Master consider the response as "bogus packet" and increment the "Bogus origin" count. This issue is seen on all the AOS 8.x switches like 6900-X48C6, 6900-X72, 6860E-U28, 6860N-U28 and 6560-P48 switches.</p> <p> Click for Additional Information</p>
<p>Case: 00676964 CRAOS8X-37852</p>	<p>Summary: OS6560: PoE not delivered to end devices connected to the switch ports after the upgrade of switch from 8.9R01 to 8.9R02.</p> <p>Explanation: The PoE issue after the upgrade would be seen only if there is Dragonite Firmware download error during the switch boot up. The same issue would be noticed if the switch has PTP configuration.</p> <p> Click for Additional Information</p>
<p>Case: 00666175 CRAOS8X-37013</p>	<p>Summary: In AOS 8.x switches like OS6900-X48C6, OS6860E-U28, OS6900-X72, 6860N-U28 and 6560-P48C6, "write memory" command corrupt the LLDP configuration.</p> <p>Explanation: LLDP is configured for ports 1/1/49A, 1/1/50A and 1/1/51A; however, the switch does not save configuration related to 1/1/50A in the running configuration. Hence, after a reload the LLDP configuration for port 1/1/50A would be missing in the switch.</p> <p> Click for Additional Information</p>
<p>Case: 00669880 CRAOS8X-37320</p>	<p>Summary: Switch Temperature threshold value of OS6860E switch is too high for the power supplies connected in the switch.</p> <p>Explanation: To test the temperature threshold warning in OS6860E switches, the chassis temperature was increased by blowing hot air against it. At around 60-65 degree Celsius, the power supply is shutting down even when the switch danger threshold is between 78-93 Celsius.</p> <p> Click for Additional Information</p>






<p>Case: 00675877 CRAOS8X-37774</p>	<p>Summary: OS6900-X48C6: WARNING!!! System temperature is 83.00C, shall shut down 69.00C</p> <p>Explanation: The Danger threshold of the switch is 69 degrees Celsius. If the chassis ambient air temperature rises above the danger threshold, then the switches would generate the message <i>"WARNING!!! System temperature is 83.00C, shall shut down 69.00C"</i>. This warning message is not self-explanatory and needs change.</p> <p>The Chassis temperature warning message is corrected as <i>"WARNING!!! System temperature is 71.00C, Switch has crossed danger threshold value"</i></p> <p> Click for Additional Information</p>
<p>Case: 00676965 CRAOS8X-37899</p>	<p>Summary: OS6560: Several switches lost SNMP communication after the upgrade from 8.9R01 to 8.9R02</p> <p>Explanation: After upgrade the switches were communicating with NMS via SNMP; however, approx. 6-7 min after the first contact to NMS server the SNMP communication is lost in several switches. There were too many SNMP requests entering the switch during the issue time and there were also traps sent out from the switch at the same time. As traps sent out cost much more CPU, these trap activities could impact processing of SNMP requests making SNMP request not handled immediately and responded late.</p> <p> Click for Additional Information</p>
<p>Case: 00679387 CRAOS8X-38067</p>	<p>Summary: VC of 5x OS6560-P48Z16 failed to write the reload command to "command.log".</p> <p>Explanation: If the VC of 5x OS6560-P48Z16 is reloaded via the switch console, it took approx. 2 minutes for the switch to print the reload command in the command.log. However, if the same VC is reloaded via the SSH session, then the switch would fail to print the reload command to "command.log". Also, this issue is not replicated on standalone OS6560.</p> <p>Changes are made in the "Chassis Supervision" to return the result earlier. This would give "Session Manager" more time to write the reload command to "command.log" while it's waiting for the reload.</p> <p> Click for Additional Information</p>
<p>Case: 00681148 CRAOS8X-38150</p>	<p>Summary: High CPU utilization noticed on the Master Chassis of OS6560-P48Z16 VC due to the task 'radCli'.</p> <p>Explanation: From the slave units in the VC, ping reachability is possible to the loopback IP (127.10.1.65) of Master chassis; however, ssh/telnet connection to Master is not established. The Master Chassis with CPU spike is not accessible even via Console connection. Even though the Master Chassis failed to establish any connection, it continued to act as the Master switch for the VC.</p>






	<p>To clear the issue, Master NI is power cycled, and it joined the VC as a Slave without any issues. "vc-takeover" command is executed to promote the Chassis-1 as the Master again.</p> <p> Click for Additional Information</p>
<p>Case: 00683772 CRAOS8X-38332</p>	<p>Summary: After a reload in OS6860N-U28 switch, the SFP-GIG-T ports does not come UP.</p> <p>Explanation: In the PHY level of OS6860N-U28, port default speed (1000M) is not set if 1G copper SFP is used with 100M speed config after reloading.</p> <p> Click for Additional Information</p>
<p>Case: 00685631 CRAOS8X-38481</p>	<p>Summary: OS6900-X48C6 switch generating "Invalid QSI 40000262 QI 8" messages.</p> <p>Explanation: The switches generate these logs during an SNMP walk to the MIB "alaVfcQInstanceTable". Once the snmpwalk has reached the end of database, it returns null value and hence this is logged as INFO message in switch logs.</p> <p> Click for Additional Information</p>
<p>Case: 00685441 CRAOS8X-38546</p>	<p>Summary: OS6560-P48Z16 switch with the microcode 8.9.107.R02 is accepting the "template name" for UNP port-template with space, if double quotes are used. However, if the switch is reloaded the UNP port-template configured would be removed from the configuration.</p> <p>Explanation: UNP port-template configured in the switch with space in "template name". In running configuration, the UNP port-template name is saved without double quotes. If the switch is reloaded after saving the configuration, the above port-template is removed from the switch configuration. Also, the switch generates "vcboot.cfg.1.err" file in the flash.</p> <p> Click for Additional Information</p>
<p>Case: 00685174 CRAOS8X-38595</p>	<p>Summary: AOS 8.x switches does not retrieve any value ("0xffffffff") for the MIB "chasEntPhysModuleType"</p> <p>Explanation: AOS 8.x switches are not able to display the "moduleType" of the transceivers connected to the ports during SNMP walk. Hence the issue is noticed.</p> <p> Click for Additional Information</p>
<p>Case: 00688018 CRAOS8X-38724</p>	<p>Summary: AOS switch generate a warning while configuration flood-limit action 'shutdown' on a linkagg member port "WARNING: Cannot configure action shutdown on Linkagg member port".</p>





	<p>Explanation: In AOS switches, it is allowed to configure the flood-limit rate (for UUCAST / MCAST / BCAST) on a linkagg member port. However, there is limitation to configure action 'SHUTDOWN'. Hence, the switch abort the command and generate a warning message.</p> <p> Click for Additional Information</p>
<p>Case: 00690907 CRAOS8X-39116</p>	<p>Summary: To disable auto-fabric functionality globally for AOS 8.x switches.</p> <p>Explanation: The following CLI command “<i>auto-fabric admin-state disable remove-vc-reload</i>” remove the auto-fabric feature and would reboot the switch. During the process, instead of creating "vcboot.cfg", the switch created "boot.cfg". AOS 8.x switches are by default Virtual-Chassis and supports only "vcboot.cfg".</p> <p> Click for Additional Information</p>
<p>Case: 00691035 CRAOS8X-39123</p>	<p>Summary: OS6465-P12 switch failed to display the command-log completely.</p> <p>Explanation: It is noticed that the "show command-log" output displayed only 20 entries; however, the entries should be more than that. Also, the 20th command was not printed properly. This issue is randomly seen in the switches, and they are not replicated frequently.</p> <p>If the data is too big to write, sometimes writing to MIP get failed due to buffer overflow.</p> <p> Click for Additional Information</p>
<p>Case: 00694109 CRAOS8X-39513</p>	<p>Summary: CPE-TEST with 10GIG UNI works only if the port is Operationally UP.</p> <p>Explanation: To perform CPE-Test in OS6570M-U28, the 10GIG UNI port should be with “Operational Status” UP and “Admin-status” UP. If the 10GIG UNI port is with “Operational Status” DOWN and “Admin-status” UP, then the CPE-Test would run only with 1000M traffic and it does not run with 10000M.</p> <p> Click for Additional Information</p>
<p>Case: 00695259 CRAOS8X-39645</p>	<p>Summary: In OS6465-P28 switch, throughput on a 10GIG port during CPE-TEST is 2302MB.</p> <p>Explanation: This issue is only noticed with OS6465-P28. If the same test is performed on OS6570M, then the throughput is as expected.</p> <p> Click for Additional Information</p>
<p>Case: 00698119</p>	<p>Summary: In OS6570M, tri-Color metering is not working as expected.</p>





<p><i>CRAOS8X-40080</i></p>	<p>Explanation: The priority from the CVLAN is not configured to the SVLAN. The SVLAN uses the default priority-0 for all the traffic. So, the switch uses Queue-0 to process all the traffic and hence the QOS metering is not working as expected.</p> <p> Click for Additional Information</p>
<p>Case: 00705199 <i>CRAOS8X-40924</i></p>	<p>Summary: In OS6570M, the Uboot is disabled via CLI command; however, the switch still allows to break the boot sequence during the bootup.</p> <p>Explanation: Uboot disabled in the switch via the below CLI command and the configuration is synchronized. When the switch is reloaded for the 1st time after configuration change, as expected the switch will not allow to break the boot sequence to enter into Uboot. If the same switch is reloaded for the 2nd time, it does allow to break the boot sequence to enter into uboot.</p> <p> Click for Additional Information</p>
<p>Case: 00705198 <i>CRAOS8X-41001</i></p>	<p>Summary: In OS6570M, few of the control frames are dropped even after using the uni-profile "ieee-fwd-all".</p> <p>Explanation: The drop in control frames is noticed only with the Cisco PDU's. Also, the Cisco PDU's are dropped only by the OS6570M switches and not by any other AOS 8.x switches.</p> <p> Click for Additional Information</p>
<p>Case: 00707863 <i>CRAOS8X-41298</i></p>	<p>Summary: Command to change the 'Default' logging level in AOS 8.x switches.</p> <p>Explanation: In AOS 8.x switches, the default logging level is 'INFO'. If the logging level of an 'appid' is changed to any value other than 'INFO', then the same is printed in the switch configuration.</p> <p>A new CLI command is introduced to set the default logging level in AOS 8.x switches.</p> <p> Click for Additional Information</p>
<p>Case: 00707865 <i>CRAOS8X-41300</i></p>	<p>Summary: Support for installing 10G license based on ORDER-ID for OS6570-U28 Model.</p> <p>Explanation: The proposal is to use the existing command to apply the 10G license generated based on unique order-Id (Instead of Serial Number and MAC address). This method is used to apply 10G license only on OS6570-U28 model.</p>





	<p>There is no change required in the License Portal (LDS) for this new method. Also, this change is provided only for End Customer "Virgin Media (VM)" not to be available for other customers.</p> <p> Click for Additional Information</p>
<p>Case: 00707542 <i>CRAOS8X-41308</i></p>	<p>Summary: In AOS 8.x switches, executing the "qos reset" command makes switch CLI unresponsive for few minutes. Also, the switch does not allow user to make further changes to the QOS until the switch is reloaded.</p> <p>Explanation: "qos reset" should only reset global qos configuration like trust, dei setting and it should not impact the ACL configuration. Commands like "qos flush", "qos revert" and "qos apply" will impact the ACL config.</p> <p>Issue seen in QoS2 based platforms and this is a legacy issue. "qos reset" behaves similar to "qos flush". So, ACL configuration is flushed in qosNi on executing "qos reset".</p> <p> Click for Additional Information</p>
<p>Case: 00709041 <i>CRAOS8X-41432</i></p>	<p>Summary: After the upgrade of 6 units of OS6560-P48Z16 switches in VC from 8.9.107.R02 to 8.9.116.R02, the UNP configuration of the ports 5/1/14-48 and 6/1/1-48 were not displayed under "show configuration snapshot" output.</p> <p>Explanation: There was no "vcboot.cfg.1.err" file written during the startup process. The switch used the correct UNP-template for the users in the ports 5/1/14-48 and 6/1/1-48 even when it failed to display the configuration in the "show configuration snapshot" output.</p> <p>After the upgrade the switch has generated 'agCmm' dump. As per PMD file, there is memory crash occurred in the function "agCmmHandleEapFromNi" and the memory corruption was caused by EAPol.</p> <p> Click for Additional Information</p>
<p>Case: 00688759 <i>CRAOS8X-38870</i></p>	<p>Summary: Multicast traffic gets impaired after some time, new streams do not work.</p> <p>Explanation: In a large SPB network where there are remote links that may go down and up occasionally, the SDP VP for multicast destinations behind said link get deleted and recreated.</p> <p>Due to a bug, a 16K counter would increment each time a new SDP VP was created. Once this counter reached 16K (16384) no further SDP VPs could be created in hardware. This prevented new multicast flows from working.</p> <p> Click for Additional Information</p>
<p>Case: 00666560 <i>CRAOS8X-37244</i></p>	<p>Summary: OS6860N-P48M with 10G transceiver not working on port 48.</p>






	<p>Explanation: OS6860N-P48M with 10G transceiver not working on port 48, when it is connected to Dell server. In the hardware, the MUX PHY had an EEE (Energy efficient ethernet) enabled, which seem to cause the Dell Server link to be down, and the link on the switch side to be Up but with no Rx counter increasing. Fix provided by disabling this EEE on the PHY 88E6193 (MUX Marvell Chip).</p> <p> Click for Additional Information</p>
<p>Case: 00681080 CRAOS8X-38153</p>	<p>Summary: IP multicast for a vlan fails to forward in the OS9900 switch.</p> <p>Explanation: The defensive check has been done in 89R03, such that even after the crash the IPMS traffic will be forwarded.</p> <p> Click for Additional Information</p>
<p>Case: 00703663 CRAOS8X-41084</p>	<p>Summary: 6865P16X Service configuration cannot be removed from the SAP port</p> <p>Explanation: While trying to remove the service config on the SAP port it did not remove. The switch takes the command "no service 990 sap port 1/1/6:990" with no error shown but service remains on this SAP port. Also if tried to disable service 990 and then remove it from the SAP port. The same results where the switch takes the command yet the service remains attached to the SAP port.</p> <p> Click for Additional Information</p>
<p>Case: 00650476 CRAOS8X-35701</p>	<p>Summary: UNP and LPS configured port on the OS6560-P48Z16 switch is not working with port-voilation</p> <p>Explanation: An PC connected to an IP phone ALE 8058 are seeing lpsPortViolation[555]Port-security Violation on PORT 1/1/1 : Shutting down port, during a power on off reboot or reload.</p> <p> Click for Additional Information</p>
<p>Case: 00666546 CRAOS8X-37034</p>	<p>Summary: OS6465T-12: : Log Message RCA- appMgrSendEvent: sending event to client /bin/etherNi event (69) data (2)</p> <p>Explanation: Noticed the above log messages after a power outage. A reboot of the device seems to have fixed one of the devices.</p> <p> Click for Additional Information</p>






<p>Case: 000072817 CRAOS8X-38245</p>	<p>Summary: OS6570M is not sending out Qtagg Dying Gasp frame out of NNI interface</p> <p>Explanation: When OS6570M switch running in AOS 8.9.R02 noticed that the switch is not sending dying gasp to the NMS from an NNI interface. As per the AOS 8.9.R02 release notes, the dying gasp feature is not yet supported in the OS6570 switch.</p> <p> Click for Additional Information</p>
<p>Case: 00683017 CRAOS8X-38462</p>	<p>Summary: OS6456T-12 and OS6750M Dynamic ARP Inspection not working</p> <p>Explanation: The DAI (Dynamic ARP inspection is not working. The switch is allowing a rogue "customer device" to poison another "customer device's" ARP entry in the gateway router's ARP cache.</p> <p> Click for Additional Information</p>
<p>Case: 00666546 CRAOS8X-38333</p>	<p>Summary: OS6465-T12: 802.1Q field in Dying gasp SNMP packet is missing on a outgoing SVLAN NNI interface</p> <p>Explanation: The VLAN tagged was not send by the dying gasp frame, but the normal SNMP packets do see the qtagged field.</p> <p> Click for Additional Information</p>
<p>Case: 00685773 CRAOS8X-38490</p>	<p>Summary: Wos.img FTP file transfer corruption on a OS6570M with AOS 8.9 R02</p> <p>Explanation: The Wos.img images will get corrupted using traditional FTP only with OS6570M</p> <p> Click for Additional Information</p>
<p>Case: 000071301 CRAOS8X-38628</p>	<p>Summary: Configured the speed of port group (interfaces port-group port-group-num [c/s/pg] speed 10G), reboot and lost the configuration</p> <p>Explanation: When there is a large interfaces cli and with the port group configuration, the MIB table will get full and lost the configuration.</p> <p> Click for Additional Information</p>

<p>Case: 00694795 CRAOS8X-39792</p>	<p>Summary: OS6570M 8.9.R03 development build not sending OAM frame with dying Gasp bit set to 1 during a power failure</p> <p>Explanation: 8.9.R03 development build with OS6570M not sending OAM frame with dying Gasp bit set to 1 during a power failure.</p> <p> Click for Additional Information</p>
<p>Case: 00655334 CRAOS8X-36606</p>	<p>Summary: authenticationFailure trap does not show the defaulting device information, when SNMP operations are done using wrong community map string.</p> <p>Explanation: A new CLI command has been introduced to change the authentication-trap mode.</p> <p>This enhancement is to provide a way to configure for which traps are to be sent upon having a SNMP authentication failure.</p> <p>New trap provides information of the client IP that sends wrong community string in the SNMP operation.</p> <p> Click for Additional Information</p>
<p>Case: 00673660 CRAOS8X-37562</p>	<p>Summary: While trying to upgrade a VC of two or more OS6860E/OS6860N switches from any AOS release prior to 8.9 may exhibit the VC split (Mis-License-Conf+) scenario.</p> <p>Explanation: Due to some changes done to introduce METRO license for OS6560 in 89R01, there is license mismatch detected between the VC units running between 89R01 and pre-89R01 release (88R02, 88R01, 87R03 etc).</p> <p> Click for Additional Information</p>
<p>Case: 00694272 CRAOS8X-39515</p>	<p>Summary: ATOP BIDI SFPs are not detected properly on OS6900-V48 running with AOS 8.9R01 and R02. These are ALE certified bi-directional SFPs.</p> <p>Explanation: This is an issue in OS6900-V48 code to detect the ATOP SFPs with part number "APSB43123CDL10".</p> <p> Click for Additional Information</p>
<p>Case: 00697908 CRAOS8X-39967</p>	<p>Summary: Most of the MAC addresses on a specific port where a Media switch is connected, are going to FILTERING. Port-security on the port is disabled on the port.</p> <p>Explanation: Disabling port-security does not remove other port-security configuration on the port. This causes the MAC address above the maximum number 3 to go into FILTERING.</p>

	<p> Click for Additional Information</p>
<p>Case: 00697952 <i>CRAOS8X-40119</i></p>	<p>Summary: OS6860N-P48Z - VC of 8 - Unit 3 does not initialize PoE after reboot of VC for upgrade to 8.9.109R02</p> <p>Explanation: Lanpower module on slot 3 was unable to detect the Power supply 2 due to some error in EEPROM. However, PS2 was never connected. All the units in the VC are running with one PS.</p> <p>This caused any PoE commands not to work, PoE service was not starting. Once the specific slot was reloaded again using "reload chassis-id 3 from working no rollback-timeout", PoE service started working again.</p> <p>I2C errors caused the PS not being detected for POE.</p> <p> Click for Additional Information</p>
<p>Case: 00680868 <i>CRAOS8X-38284</i></p>	<p>Summary: OS6860N - Group of four ports go down and never come back.</p> <p>Explanation: Apple PCs connected ports keep flapping whenever they go to sleeping (power nap) mode. This causes speed to change from 1000 to 100 and back and eventually interface status changes.</p> <p>This is happening across all the Apple connected ports.</p> <p> Click for Additional Information</p>
<p>Case: 00646691 <i>CRAOS8X-35595</i></p>	<p>Summary: OS9900: Mac flooding issue.</p> <p>Explanation: Mac-flooding happening in the OS9900 switch in some vlans though the destination mac-address has been learnt by the chassis. Issue resolves with mac-flush. The observed has been fixed under AOS 8.9 R03.</p> <p> Click for Additional Information</p>
<p>Case: 00661035 00661039 <i>CRAOS8X-37300</i></p>	<p>Summary: OS6465T-P12 & OS6560: APs are not powered and are in lanpower fault status and OS6560 switch reboots continuously</p> <p>Explanation: OS6465T-P12 switches, where the PoE devices are not being powered on. The <show lanpower slot 1/1> displays a PoE "fault". OS6560 switch reboots continuously for 6 times to boot up properly. The issues are related to lanpower firmware download failed issue.</p> <p>The observed has been fixed under AOS 8.9 R03.</p>

	<p> Click for Additional Information</p>
<p>Case: 00673560 CRAOS8X-37631</p>	<p>Summary: Attempting to create command alias will crash-reload the Switch.</p> <p>Explanation: Both of the following commands will crash the switch:</p> <pre>alias swt='show log swlog timestamp \$(system date) 00:00:00 less'</pre> <pre>alias swt='show log swlog timestamp `system date` 00:00:00 less'</pre> <p>Official fix would be available under AOS 8.9 R03 GA.</p> <p> Click for Additional Information</p>
<p>Case: 00668468 CRAOS8X-37850</p>	<p>Summary: The port performance goes down with AOS 8.9.73.R01 GA to a few Kb/s or 0 Kb/s.</p> <p>Explanation: While transferring files from PC to server using a file transfer tool, the speed issue was noticed as from mb/sec the speed was getting reduced to kb/sec and stops completely at some point. The observed has been fixed under AOS 8.9 R03.</p> <p> Click for Additional Information</p>
<p>Case: 00679118 CRAOS8X-37992</p>	<p>Summary: The "user-profile save" is replacing the single-quotes with double-quotes.</p> <p>Explanation: The challenge is the single-quotes vs double-quotes. The value of the alias is taken away, if this is not respected by the "user-profile save" command.</p> <pre>alias swt="show log swlog timestamp \$(system date) 00:00:00 less"</pre> <p>After a logout/login, the "alias" command will have evaluated the output/result of \$(system date) as they replace single-quotes (') with double-quotes (") to save the alias in "user-profile save" command.</p> <p>The observed has been fixed under AOS 8.9 R03.</p> <p> Click for Additional Information</p>
<p>Case: 00682432 CRAOS8X-38421</p>	<p>Summary: OS6560: ISO CLNP and CLNS protocol are not forwarded out of the switch.</p> <p>Explanation: The protocol ISO CLNP & CLNS is not working with 8.x switches. The ISO 8473/X.233 CLNP protocol traffic was ingressing the OS6560 switch however not egressing the OS6560 switches. The issue was due to the destination mac-address is matching the switch's internal rule which is used for ISIS communication.</p>

	<p>Official fix would be available under AOS 8.9 R03 GA.</p> <p> Click for Additional Information</p>
<p>Case: 00702515 <i>CRAOS8X-40511</i></p>	<p>Summary: Documentation: the link-local address is not mentioned in the guideline of the ip6 source filtering. This address is not filtered by ip6SF when the binding ipv6 table is purged.</p> <p>Explanation: An explanation that IPV6 source-filtering of link-local is not done is added to the documentation as it was missing.</p> <p> Click for Additional Information</p>
<p>Case: 00698621 <i>CRAOS8X-40046</i></p>	<p>Summary: Documentation: command to revert back to default mode is not correct.</p> <p>Explanation: Command “capability profile tcam mode dest-ipv6” to revert back to default mode is not correctly mentioned in documentation, .</p> <p> Click for Additional Information</p>
<p>Case: 00702821 <i>CRAOS8X-40549</i></p>	<p>Summary: Documentation OS6900-V48C8 : QOS policies not working with OS6900-V48C8 INLINE ROUTING Traffic.</p> <p>Explanation: QOS policies not working with OS6900-V48C8 INLINE ROUTING Traffic which is not mentioned in documentation. It will be mentioned in the guidelines that only routing with external loop back support qos policies to be applied to ingress traffic.</p> <p> Click for Additional Information</p>
<p>Case: 00664160 <i>CRAOS8X-36855</i></p>	<p>Summary: The link connected to port 1/1/49 of OS6560-P48X4 switch model is not stable when the far end is an HP switch.</p> <p>Explanation: The link connected to port 1/1/49 of OS6560-P48X4 switch model is not stable when the far end is an HP switch. Same HP switch connected to port 1/1/50 the link is stable, improvement done to avoid this interoperability behavior.</p> <p> Click for Additional Information</p>
<p>Case: 00663902 <i>CRAOS8X-36890</i></p>	<p>Summary: The switch loses IP connectivity (ssh session / icmp / snmp) over the uplink port when port-monitoring enabled.</p> <p>Explanation: The option no forward combined configured with port monitoring causes this issue. A hardware limitation is identified when port monitored packets and ip packets are used in same time.</p>

	<p> Click for Additional Information</p>
<p>Case: 00699148 CRAOS8X-40113</p>	<p>Summary: When trying to push QoS policy from OV2500 to 6560 switches. We notice “Recache failure” in OV2500 and all current QoS config are getting flushed.</p> <p>Explanation: The issue is noticed when Network group contains multiple host IPs in the same subnet range and is seen only on OS6560. The issue is fixed in AOS 8.9 R03</p> <p> Click for Additional Information</p>
<p>Case: 00663415 CRAOS8X-37921</p>	<p>Summary: OS6560 switch displays "Please Wait" message when entering the QoS command in the switch CLI.</p> <p>Explanation: The 6560 switch (8.9.73.R01) prompted a “Please wait” message when configuring QoS policies with the “From ldap” keyword. Also, It was not displaying output for show commands.</p> <p> Click for Additional Information</p>
<p>Case: 00700181 CRAOS8X-40355</p>	<p>Summary: "mis-license-config" error was seen during the switch AOS upgrade (From 8.8R01 to 8.9.R02) from OV.</p> <p>Explanation: In VC of 2xOS6860s, the chassis2 was not added as a VC member and it was stuck at a mis-license-config error during the switch AOS upgrade (From 8.8R01 to 8.9.R02) from OV. Also, noticed the same issue during the standard upgrade via SFTP.</p> <p> Click for Additional Information</p>
<p>Case: 00671624 CRAOS8X-37784</p>	<p>Summary: After changing the VPN-MTU, the service config disappears from the "show configuration snapshot" command output.</p> <p>Explanation: After changing the service VPN-MTU to non-default values (i.e., 9000, 9100), the service config disappears from the “show running configuration snapshot” command output. Even after saving the configuration, it did not reflect in the vcboot.cfg file.</p> <p> Click for Additional Information</p>
<p>Case: 00693367 CRAOS8X-39433</p>	<p>Summary: OS9907 - CMMB rebooted three times with new_cs PMD.</p> <p>Explanation: An OS9907 single chassis, with only one CMMB, running AOS 8.9.78.R01, the CMM has been restarted due to watchdog failure, and new cs PMD is generated. As the chassis is running with Single CMM, the whole chassis is rebooted.</p>

 [Click for Additional Information](#)

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
<ul style="list-style-type: none"> - 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	Description
CRAOS8X-27035	OpenVPN: Security vulnerabilities after 2.4.9 (8.7R2) CVSS 5.3
CRAOS8X-15425	Kerberos - Security Advisories after 5.1.16.1 (CVSS 7.5)
CRAOS8X-7584	zlib: Security vulnerabilities (CVSS 8.8)
CRAOS8X-9530	Security vulnerabilities in 2.0.22(CVSS 9.8)
CRAOS8X-33994	ncurses: Security vulnerabilites (CVSS: 9.8)
CRAOS8X-34254	Python: security vulnerabilities (CVSS 9.8)
CRAOS8X-26367	PCRE: CVE Security Vulnerabilities (CVSS 7.5)
CRAOS8X-33125	curl: security vulnerabilities (CVSS : 7. 5)
CRAOS8X-3523	tcpdump - Security Advisories (CVSS 7.3)
CRAOS8X-33275	openldap: security vulnerabilities (CVSS: 7.3)
CRAOS8X-34252	libxml2: security vulnerabilities (CVSS 6.5)
CRAOS8X-32693	Linux: Security vulnerabilities CVE-2022-0995 CVE-2022-1011 CVE-2022-26490 CVE-2022-27666 (CVSS 7.8)
CRAOS8X-33532	Linux: Security Vulnerability CVE-2022-1729 race in sys_perf_event_open (CVSS 7.8)
CRAOS8X-34312	Linux: Security Vulnerability CVE-2022-32250 (CVSS 7.8)
CRAOS8X-34779	Linux security vulnerabilities: CVE-2021-33656 (CVSS 7.8)
CRAOS8X-35328	Linux security vulnerabilities: CVE-2022-2588, CVE-2022-2153, CVE-2022-2586 (CVSS: 7.8)
CRAOS8X-3528	Bash - Security Advisories (CVSS 7.8)
CRAOS8X-3569	PAM - Security Advisories (CVSS 8.1)
CRAOS8X-32119	radsecproxy: security vulnerabilities (CVSS 9.4 NIS)
CRAOS8X-37456	openssl security vulnerabilities CVE-2022-4203, CVE-2022-4304, CVE-2022-4450, CVE-2023-0215, CVE-2023-0216, CVE-2023-0217, CVE-2023-0286, CVE-2023-0401 (CVSS 8.1)
CRAOS8X-36405	libxml2 security vulnerabilities CVE-2022-40303 and CVE-2022-40304 (CVSS 8.2)
CRAOS8X-35845	expat: security vulnerability CVE-2022-40674 (CVSS 9.8)
CRAOS8X-36562	expat: security vulnerability CVE-2022-43680 (CVSS 7.5)
CRAOS8X-36765	Linux security vulnerabilities CVE-2022-20422, CVE-2022-3586, CVE-2022-3621, CVE-2022-3625, CVE-2022-3629, CVE-2022-3633, CVE-2022-3635, CVE-2022-3646, CVE-2022-3649, CVE-2022-43750 (CVSS 9.8)
CRAOS8X-37802	Linux: security vulnerabilities CVE-2022-3534, CVE-2022-4842, CVE-2023-0045, CVE-2023-0210, CVE-2023-23559 (CVSS 8.0)