Release Notes - Rev. C

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

Release 8.9R2

These release notes accompany release 8.9R2. 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.

Alcatel-Lucent Enterprise

Contents

Related Documentation

These release notes should be used in conjunction with OmniSwitch AOS Release 8 User Guides. The following are the titles of the user guides that apply to this release.

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

U-Boot and FPGA Requirements

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

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

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

OmniSwitch 6360 - AOS Release 8.9.107.R02 (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

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
OS6360-P10A (904324-90)	8.8.2.R03	8.8.2.R03 8.9.85.R02[4]	0.1	0.1
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
OS6360-PH24	8.7.149.R02	8.7.30.R03[2] 8.9.85.R02[4]	0.12	0.12
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
OS6360-PH48	8.8.114.R01	8.8.114.R01 8.9.85.R02[4]	0.12	0.12

1. FPGA version 0.17 is REQUIRED to address issues CRAOS8X-26370 and CRAOS8X-25033.
2. Optional uboot update for CRAOS8X-24464, ability to disable/authenticate uboot access.
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.

OmniSwitch 6465 - AOS Release 8.9.107.R02 (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

1. FPGA version 0.7 is optional to address issue CRAOS8X-12042.
2. U-boot 8.7.2.R02 is optional to address UBIFS error issues CRAOS8X-4813/13440.
3. Optional uboot update for CRAOS8X-24464, ability to disable/authenticate uboot access.
4. Optional uboot update to support boot from USB feature.
5. Highly recommended to address the NAND flash corruption issue (CRAOS8X_35470).

OmniSwitch 6560 - AOS Release 8.9.107.R02 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6560-24Z24	8.5.22.R01	8.7.2.R02[3] 8.7.30.R03[7]	0.7	0.8[5]
OS6560-P24Z24	8.4.1.23.R02	8.7.2.R02[3] 8.7.30.R03[7]	0.6	0.7[1] 0.8[5]
OS6560-24Z8	8.5.22.R01	8.7.2.R02[3] 8.7.30.R03[7]	0.7	0.8[5]
OS6560-P24Z8	8.4.1.23.R02	8.7.2.R02[3] 8.7.30.R03[7]	0.6	0.7[1] 0.8[5]
OS6560-24X4	8.5.89.R02	8.7.2.R02[4] 8.7.30.R03[7] 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]	0.6	0.7[1] 0.8[5]
OS6560-P48Z16 (all other PNs)	8.5.97.R04	8.7.2.R02[3] 8.7.30.R03[7]	0.3	0.6[2] 0.7[6]
OS6560-48X4	8.5.97.R04	8.7.2.R02[4] 8.7.30.R03[7] 8.9.85.R02[8]	0.4	0.7[2] 0.8[6]
OS6560-P48X4	8.5.97.R04	8.7.2.R02[4] 8.7.30.R03[7] 8.9.85.R02[8]	0.4	0.7[2] 0.8[6]
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]

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

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).

OmniSwitch 6570M - AOS Release 8.9.107.R02 (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]	0.11	0.11
OS6570M-12D	8.9.25.R02	8.9.25.R02 8.9.92.R02[1]	0.11	0.11
OS6570-U28	8.9.25.R02	8.9.25.R02 8.9.92.R02[1]	0.11	0.11

1. Adds support for Gowin CPLD.

OmniSwitch 6860(E) - AOS Release 8.9.107.R02 (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 8.9.107.R02 (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.

Hardware	Minimum ONIE	Current ONIE	Minimum CPLD	Current CPLD
Note: These models use the **Uosn.img** image file.				

OmniSwitch 6865 – AOS Release 8.9.107.R02 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6865-P16X	8.3.1.125.R01	8.7.2.R02[2] 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 8.9.107.R02 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
CMM (if XNI-U12E support is not needed)	7.2.1.266.R02	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 8.9.107.R02 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
CMM (if XNI-U12E support is not needed)	7.3.2.134.R01	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 8.9.107.R02 (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 8.9.107.R02 (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 8.9.107.R02 (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]
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 1 - 6.0

Hardware	Minimum ONIE	Current ONIE	Minimum CPLD	Current CPLD
			CPLD 2 - 6.0 CPLD CPU - 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 8.9.107.R02 (GA)

Hardware	Minimum Coreboot-uboot	Current Coreboot-uboot	Minimun Control FPGA	Current Control FPGA	Minimum/ Current Power FPGA
OS99-CMM	8.3.1.103.R01	8.3.1.103.R01 8.7.30.R03[1]	2.3.0	2.3.0	0.8
OS9907-CFM	8.3.1.103.R01	8.3.1.103.R01	-	-	-
OS9907-CFM2	8.9.X	8.9.X	-	-	-
OS99-GNI-48	8.3.1.103.R01	8.3.1.103.R01 8.8.152.R01[2]	1.2.4	1.2.4 1.2.5[2]	0.9
OS99-GNI-P48	8.3.1.103.R01	8.3.1.103.R01 8.8.152.R01[2]	1.2.4	1.2.4 1.2.5[2]	0.9
OS99-XNI-48 (903753-90)	8.3.1.103.R01	8.3.1.103.R01 8.8.152.R01[2]	1.3.0	1.3.0 1.5.0[2]	0.6
OS99-XNI-48 (904049-90)	8.6.261.R01	8.6.261.R01 8.8.152.R01[2]	1.4.0	1.4.0 1.5.0[2]	0.7
OS99-XNI-U48 (903723-90)	8.3.1.103.R01	8.3.1.103.R01 8.8.152.R01[2]	2.9.0	2.9.0 2.11.0[2]	0.8
OS99-XNI-U48 (904047-90)	8.6.261.R01	8.6.261.R01 8.8.152.R01[2]	2.10.0	2.10.0 2.11.0[2]	0.8
OS99-GNI-U48	8.4.1.166.R01	8.4.1.166.R01 8.8.152.R01[2]	1.6.0	1.6.0 1.7.0[2]	0.2
OS99-CNI-U8	8.4.1.20.R03	8.4.1.20.R03 8.8.152.R01[2]	1.7	1.7 1.9[2]	N/A
OS99-XNI-P48Z16	8.4.1.20.R03	8.4.1.20.R03 8.8.152.R01[2]	1.4	1.4 1.6[2]	0.6
OS99-XNI-U24	8.5.76.R04	8.6.261.R01 8.8.152.R01[2]	1.0	2.9.0 2.11.0[2]	0.8
OS99-XNI-P24Z8	8.5.76.R04	8.6.261.R01 8.8.152.R01[2]	1.1	1.4.0 1.6.0[2]	0.7
OS99-XNI-U12Q	8.6.117.R01	8.6.117.R01 8.8.152.R01[2]	1.5.0	1.5.0 1.6.0[2]	N/A
OS99-XNI-UP24Q2	8.6.117.R01	8.6.117.R01 8.8.152.R01[2]	1.5.0	1.5.0 1.6.0[2]	N/A

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

[IMPORTANT] *MUST READ*: AOS Release 8.9R2 Prerequisites and Deployment Information

General Information

- Early availability features are available in AOS and can be configured. However, they have not gone through the complete AOS validation cycle and are therefore not officially supported.
- Please refer to the Feature Matrix in Appendix A for detailed information on supported features for each platform.
- Prior to upgrading please refer to Appendix D for important best practices, prerequisites, and step-by-step instructions.
- Some switches that ship from the factory will default to VC mode (requiring a vcboot.cfg configuration file) and attempt to run the automatic VC, automatic remote configuration, and automatic fabric protocols. Please note that since the switches default to VC mode, automatic remote configuration does not support the downloading of a 'boot.cfg' file, only the 'vcboot.cfg' file is supported.
- Some switches may ship from the factory with a diag.img file. This file is for internal switch diagnostic purposes only and can be safely removed.

Note: None of the ports on the OS6865 or OS6465 models default to auto-vfl so automatic VC will not run by default on newly shipped switches. However, automatic remote configuration and automatic fabric will run by default. The OS9900 does not support automatic VC mode, only static VC mode is supported.

- Switches that ship from the factory will have the *Running Configuration* set to the **/flash/working** directory upon the first boot up. By default, the automatic VC feature will run and the vcboot.cfg and vcsetup.cfg files will be created in the **/flash/working** directory but not in the **/flash/certified** directory which results in the *Running Configuration* not being certified. This will result in the *Running Configuration* being set to the **/flash/certified** directory on the next reboot. Additionally, on the next reboot the switch will no longer be in the factory default mode and will have a chassis-id of 1 which could cause a duplicate chassis-id issue if the switch is part of a VC. To set the switch back to the factory defaults on the next reboot perform the following:

```
-> rm /flash/working/vcboot.cfg
-> rm /flash/working/vcsetup.cfg
-> rm /flash/certified/vcboot.cfg
-> rm /flash/certified/vcsetup.cfg
```

- The OS6560-P48Z16 (903954-90) supports link aggregation only on the 1G/2.5G multigig and 10G ports (33-52). The 1G ports (ports 1-32) do not support link aggregation (CRAOSX-1766). Linkagg configuration on unsupported ports in 85R1/841R03 config file will be removed internally from software during upgrade reboot. Oversized frames will not be dropped on ingress of ports 1-32 (CRAOS8X-20939).

  Note: OS6560-P48Z16 (all other PNs) - This is a new version of the OS6560-P48Z16 which does not have the limitations mentioned above. The model number (OS6560-P48Z16) remains the same for both versions, only the part number can be used to differentiate between the versions.

- Improved Convergence Performance
  Faster convergence times can be achieved on the following models with SFP, SFP+, QSFP+, and QSFP28 ports with fiber transceivers.

  Exceptions:
  - Copper ports or ports with copper transceivers do not support faster convergence.
  - OS6865-P16X and OS6865-U12X ports 3 and 4 do not support faster convergence.

  - VFL ports do not support faster convergence.
  - Splitter ports (i.e. 4X10G or 4X25G) do not support faster convergence.

- MACsec Licensing Requirement
  Beginning in 8.6R1 the MACsec feature requires a site license, this license can be generated free of cost. After upgrading, the feature will be disabled until a license is installed. There is no reboot required after applying the license.

- SHA-1 Algorithm - Chosen-prefix attacks against the SHA-1 algorithm are becoming easier for an attacker[1]. 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: - 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. - 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.

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

	License Required							
	OS6360	OS6465	OS6560	OS6570M	OS6860	OS6860N	OS6900	OS9900
Licensed Features								
MACsec (OS-SW-MACSEC)	N/A	Yes	Yes	N/A	Yes	Yes	Yes[3]	Yes
10G support (OS6560-SW-PERF)	N/A	N/A	Yes[1]	N/A	N/A	N/A	N/A	N/A
10G support (OS6360-SW-PERF)	Yes[2]	N/A	N/A	N/A	N/A	N/A	N/A	N/A
10G support (OS6570-SW-PERF4)	N/A	N/A	N/A	Yes[4]	N/A	N/A	N/A	N/A

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
Note: Starting in 8.9R1 the following features require a Metro license.	

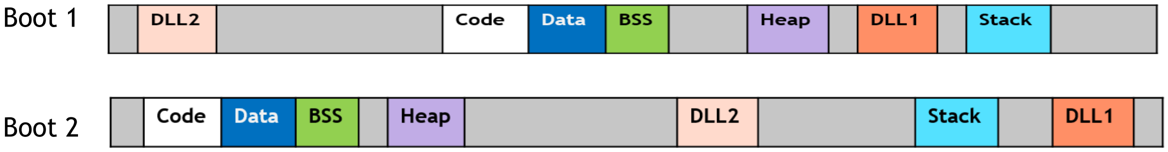
ALE Secure Diversified Code

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

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

Software Diversification

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



Please contact customer support for additional information.

New / Updated Hardware Support and Guidelines

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

OmniSwitch 6860N Expansion Modules

The following expansion modules for the OS6860N-P24M and OS6860-P48M are being built with a new i2C switch component and require a minimum 8.9R2 AOS release. They will contain a sticker indicating the minimum release required.

- OS68-XNI-U4
- OS68-QNI-U2
- OS68-VNI-U4

The following products are being built with a new CPLD component and require a minimum 8.9R2 AOS release. They will contain a sticker indicating the minimum release required.

- OS6360
- OS6570M

OmniSwitch 6360-P24/P48 - PoE Firmware 3.55

The OS6360-P24 and OS6360P-48 models are now shipping with PoE firmware version 3.55.

Transceivers

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

- SFP-25G-ESR – 25-Gigabit optical transceiver (SFP28). Supports link lengths of 300m on OM4 multimode fiber cables. LC connector type.

New Software Features and Enhancements

The following software features are being introduced in this release, subject to the feature exceptions and problem reports described later in these release notes.

8.9R2 New Feature/Enhancements Summary

Feature	OmniSwitch Platform
Management Features	
Alarm Relay Enhancement	6465
Metro Features	
CPE Enhancement	6570M
Metro Ethernet Enhancements	6465T
Security Feature	
Minimum Password Length of at Least 16 Characters (Default Mode)	All
NIS Certification - Salt Value Generated 1000 Rounds	All
NIS Certification - Minimum Password Length of at Least 16 Characters (Enhanced Mode)	All
NIS Certification - Password Policy Enhancement	All
NIS Certification – WebView Key Encryption with AES128	All
JITC - Configurable Concurrent Sessions (FTP, SSH, Telnet, HTTP/HTTPS)	All
JITC – Fully Disabled Kernel	All
Service Features	
Layer 3 Connectivity CVLAN in VLAN Stacking	6465, 6560, 6570M, 6860, 6860N, 6865, 6900, 6900-V72/C32/X48C6/T48C6/X48C4E/V48C8/C32E/X24C2/T24C2

Management Features

Alarm Relay Enhancement

On reload of the switch, the alarm status and output alarm is set based on the current alarm input. Additionally, the alarm status and alarm output are automatically updated to reflect a change in the alarm input.

The following CLI commands are associated with this feature:

- **alarm in**
- **alarm out**

Metro Related Features

CPE Enhancement

CPE test head feature is supported on the OS6570M beginning in 8.9R2. Supports 8 tests profile in a Testoam group simultaneously and supports storing the Testoam statistics in a flash file.

The following CLI commands are associated with this feature:

- **test-oam**

Metro Ethernet Enhancements

Metro Ethernet related features are now supported on the OS6465T.

Security Features

Minimum Password Length of at Least 16 Characters (Default Mode)

The minimum password size range has been changed to 1-30 characters. Previously it was 1-14.

The following CLI commands are associated with this feature:

- **user password-size min**

NIS Certification - Salt Value Generated 1000 Rounds

The update to the salt value is made to satisfy the NIS certification requirements in 8.9R2. As per the changes the encrypted password is generated by hashing the salt value and plain text combination 1000 rounds instead of one round previously.

- The existing or old user account must be migrated to the new database and the user must change the password for this encryption to apply.
- On downgrade to a previous AOS version, the users created on new database will not be usable.

NIS Certification - Minimum Password Length of at Least 16 Characters (Enhanced Mode)

The minimum password size range can be configured between 1 and 20 characters in Enhanced (secureadmin) mode.

The following CLI commands are associated with this feature:

- **aaa switch-access mode enhanced**

- **user password-size min**

NIS Certification - Password Policy Enhancement

This update allows for the restriction of three or more identical, consecutive characters while setting the password. By default this policy is enabled in the Enhanced (secureadmin) mode.

The following CLI commands are associated with this feature:

- **aaa switch-access mode enhanced**
- **user password-policy cannot-contain-consecutive-characters {enable | disable}**

NIS Requirements - WebView Key Encryption with AES128

The Webview private key “default_WebViewCert.pem” is now encrypted using AES128 encryption.

JITC - Configurable Concurrent Sessions (FTP, SSH, Telnet, HTTP/HTTPS)

Configure concurrent session limits for FTP, SSH, Telnet and HTTP/HTTPS. Access is refused if the number of sessions exceeds the configured session-limit.

- FTP: 1 – 4 (Default 4)
- SSH: 1 – 8 (Default 8)
- Telnet: 1 – 6 (Default 6)
- HTTP/HTTPS: 1 – 32 (Default 32)

The following CLI commands are associated with this feature:

- **session {ftp | ssh | telnet | http} session-limit <num>**

JITC - Fully Disabled Kernel

Kernel access for the software running on the network products is fully disabled when the switch mode is JITC. The “su” command is blocked when the switch mode is configured in JITC mode preventing access to the root account. The “su” command is allowed for other modes of switch operation.

The following CLI commands are associated with this feature:

- **aaa jitc admin-state enable**

Service Features

Layer 3 Connectivity CVLAN in VLAN Stacking

This feature supports L3 connectivity on management VLAN through UNI port. To configure L3 connectivity in management VLAN through UNI port, the following must be configured.

- UNI port must be bound to a SAP profile with CVLAN tag as ‘translate’.
- Configured CVLAN and SVLAN for the UNI port must be same as the management VLAN in which management traffic should flow.

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-32090	When the isam port is tagged, and untagged traffic passes through the port, there is traffic loss seen because the port discards traffic.	There is no known workaround at this time.
CRAOS8X-30045	High convergence is seen when a linkagg is disabled. Root cause of the issue is that linkagg disable is applied slower causing mac-move to be triggered first compared to mac-flush. This issue is only particular only when linkagg is disabled through CLI, if individual links of the linkagg are down then convergence is proper.	Admin link-down individual ports of the linkagg before linkagg disable or instead of linkagg disable.
CRAOS8X-36426	OS6570M is not supported in OVC.	There is no known workaround at this time.

Hardware / Transceivers

CR	Description	Workaround
CRAOS8X-31402	On an OS6900-X48C6/T48C6, port 52 or 53 (100GDAC) flaps while trying to bring 100G optical link on the neighbor port 52 or 53 respectively. This behavior is observed regardless of uplink or VFL link on port 52 or 53.	To avoid this link flap, it is recommended to use only 100G DACs OR 100G optical transceivers on both ports -52&53.
CRAOS8X-32089	Traffic Loss seen above 8 Gbps speed on the XS-010S-Q,XGS PON ONT,1x10GE transceiver (3FE49327AA).	There is no known workaround at this time.
CRAOS8X-33243	On an OS6900-Q32/X72 the maximum limit of VFI field in L2 table in Broadcom chipset is 4096, so only 4096 (4k) services are supported on these platform.	There is no known workaround at this time.
CRAOS8X-34219	With CFM2 and XNI-U48 board, port recovery after violation takes an additional 2 mins with WTR of 15 seconds.	There is no known workaround at this time.
CRAOS8X-35816	OS6570-U28 – SFP-10G-T supports only 10G peer links. Link will be down when peer speed is either 1G or 100M. If peer 1G or 100M is left connected rapid port toggles may be seen locally which may also result in the port not recovering even when set back to 10G.	Configure peer as 10G, port will operate as expected.
CRAOS8X-36381	OS6570M-U28 - It is possible with the SFP-GIG-T when speed is configured to 10M, multiple admin disable/enable toggles can cause port instability (including false local linkup and no traffic through port). Issue is only seen with repeated consecutive	A reboot of the switch is required to recover from this issue.

	local admin disable/enable toggles. Issue is not seen with 1G and 100M speed configurations.	
CRAOS8X-36440	OS6570-U28 - Port 25 with SFP-10G-T may see a local only linkup or a LED up with link down when peer side is admin-toggled repeatedly.	There is no known workaround at this time.
CRAOS8X-36589	OS6570M-U28 - SFP-100-BX-U/D may have a linkup without cable on some random ports. Port number and number of ports displaying issue appear to vary by switch (ranging from none up to two ports). Normal operation is expected when cable is inserted.	There is no known workaround at this time.
CRAOS8X-36726	OS6570M-U28 - On intermittent reload or powercycles, ports 1~20 may display a small burst of CRC errors at time of port bring up. These CRC errors are not continuous and non-incrementing.	There is no known workaround at this time.
CRAOS8X-36752	OS6570M-U28 - Activity LEDs on ports 25~30 may be less noticeable or appear to be solid if the traffic rate on the port is less than wire rate. (10G if 10G SFP, 1G if 1G SFP). Issue is more evident as traffic rate lowers on the port.	There is no known workaround at this time.

Layer 2 / Multicast

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

Layer 3

PR	Description	Workaround
CRAOS8X-33472	When BGP peering sessions operate over an IPv6 TCP connection between two OS9900s it has been observed that there could be intermittent flapping of BGP session due to loss of TCP synchronization between the BGP routers. An error log could be observed as follows: <Timestamp> : bgp_0 tcp ERR message: <Timestamp> OS9900 vrfId 0: [<peer description>,<AS>] Bad marker rcvd! Aborting peer session.	There is no known workaround at this time.

	The BGP peering session will get re-established, with no manual intervention necessary and the routing table will be restored. This behavior/symptom has not been observed on BGP peering sessions between OS9900 and OS6900/OS6860N switches. This behavior/symptom is isolated to IPv6 BGP peer sessions and has not been observed on IPv4 BGP sessions. Impact of behavior: BGP IPv6 peering session toggles and restores with above error log output. This could result in temporary network route convergence. Switch logs will attempt to capture the loss of synchronization, if possible.	

QoS

PR	Description	Workaround
CRAOS8X-4424	With color-only policy action configured, egress queue is not honoring the color marking and packets drops are observed and expected traffic rate is not achieved.	There is no known workaround at this time.
CRAOS8X-10498	Configuring maximum ingress bandwidth (i.e. qos port 1/1/3 maximum ingress-bandwidth 80M) doesn't work after vc-takeover and reload. It gets overwritten by default ingress-bandwidth of a port.	Configure ingress-bandwidth through "interfaces port c/s/p ingress-bandwidth mbps <num> burst <num>" instead of "qos port c/s/p maximum ingress-bandwidth <num>".
CRAOS8X-33587	On an OS9900, ingress bandwidth ratelimiting fails when ratelimiting is configured with more than 32G for a 40G port.	There is no known workaround at this time.

Security

PR	Description	Workaround
CRAOS8X-34758	On an OS9900, port violation recovery sometimes takes additional 5 seconds.	There is no known workaround at this time.

Service Related

PR	Description	Workaround
CRAOS8X-37414	"tcamni main ERR" error messages seen in console while trying to remove the CVLAN association with VSTK SAP.	Remove the vlan stacking configuration, enter 'qos 'apply, and reconfigure vlan stacking.

CRAOS8X-12513	When 2048 IGMP groups were sent over SPB service, only 1025 IGMP groups were received with 1024 SAPs per service configured on the edge switch. Seen with large amount of SAPs (>1K) configured on same port.	Distribute SAPs across different ports.

Virtual Chassis

PR	Description	Workaround
CRAOS8X-35788	In OS6570M Virtual Chassis switches, Outward loopback cannot loopback the traffic correctly with the interchanged Source and Destination Mac Address when Outward loopback is configured on one NI and Test Traffic coming in other NI	There is no known workaround at this time.

Hot-Swap/Redundancy Feature Guidelines

Hot-Swap Feature Guidelines

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

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

Existing Expansion Slot	Hot-Swap/Hot-Insert compatibility
Empty	
OS68-XNI-U4	OS68-XNI-U4
OS68-VNI-U4	OS68-VNI-U4
OS68-QNI-U2	OS68-QNI-U2
OS68-CNI-U1	OS68-CNI-U1

OS6860N-P48M Hot-Swap/Insertion Compatibility

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

OS6900 Hot-Swap/Insertion Compatibility

Existing Slot	Hot-Swap/Hot-Insert compatibility
Empty	All modules can be inserted
OS99-CMM	OS99-CMM
OS9907-CFM	OS9907-CFM

OS99-GNI-48	OS99-GNI-48
OS99-GNI-P48	OS99-GNI-P48
OS99-XNI-48	OS99-XNI-48
OS99-XNI-U48	OS99-XNI-U48
OS99-XNI-P48Z16	OS99-XNI-P48Z16
OS99-CNI-U8	OS99-CNI-U8
OS99-GNI-U48	OS99-GNI-U48
OS99-XNI-U24	OS99-XNI-U24
OS99-XNI-P24Z8	OS99-XNI-P24Z8
OS99-XNI-U12Q	OS99-XNI-U12Q
OS99-XNI-UP24Q2	OS99-XNI-UP24Q2

OS9900 Hot-Swap/Insertion Compatibility

Hot-Swap Procedure

The following steps must be followed when hot-swapping modules.

1. Disconnect all cables from transceivers on module to be hot-swapped.
2. Extract all transceivers from module to be hot-swapped.
3. Extract the module from the chassis and wait approximately 30 seconds before inserting a replacement.
4. Insert replacement module of same type. For a CMM wait approximately 15 to 20 minutes after insertion.
5. Follow any messages that may displayed.
6. Re-insert all transceivers into the new module.
7. Re-connect all cables to transceivers.
8. Hot-swap one CFM at a time. Please ensure all fan trays are always inserted and operational. CFM hot-swap should be completed with 120 seconds.

VC Hot-Swap / Removal Guidelines

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

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

Fast/Perpetual PoE Unlike Power Supply Swapping

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

1. Disable fpoe and ppoe (Only needs to be executed if lanpower is started).

2. Save and synchronize the configuration.
3. Swap the power supplies.
4. Reload chassis.
5. Start lanpower.
6. Enable fpoe and ppoe as required.
7. Save and synchronize the configuration.

Technical Support

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

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

Internet: Customers with service agreements may open cases 24 hours a day via the support web page. Upon opening a case, customers will receive a case number and may review, update, or escalate support cases on-line. Please specify the severity level of the issue per the definitions below. For fastest resolution, please have hardware configuration, module types and version by slot, software version, and configuration file available for each switch.

Severity 1 - Production network is down resulting in critical impact on business—no workaround available.

Severity 2 - Segment or Ring is down or intermittent loss of connectivity across network.

Severity 3 - Network performance is slow or impaired—no loss of connectivity or data.

Severity 4 - Information or assistance on product feature, functionality, configuration, or installation.

Third Party Licenses and Notices

Legal Notices applicable to any software distributed alone or in connection with the product to which this document pertains, are contained in files within the software itself located at: **/flash/foss.**

The following is in addition to the information found in the **/flash/foss/Legal_Notice.txt** file.

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

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

openvswitch : 2.12.0 : Apache License 2.0 : /flash/foss/Apache-License-2.0.txt

Appendix A: Feature Matrix

The following is a feature matrix for AOS Release 8.9R2.

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	N
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
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	8.8R1[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
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	N	N	Y	8.7R1	Y	Y	8.7R2	8.7R2	8.6R1
RMON	8.7R2	8.5R1	Y	8.9R2	Y	8.8R2	Y	Y	8.8R2	8.8R2	N

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
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	N	N	N	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	N	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
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											
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

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
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											
CPE Test Head	N	8.6R1	8.9R1 Metro	8.9R2	N	N	N	N	N	N	N
Ethernet Loopback Test	N	N	8.9R1 Metro	8.9R2	8.6R1	8.7R1	8.6R1	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
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	N	Y	Y (X72/Q32)	N	N	N
1588v2 Peer-to-Peer Transparent Clock	N	8.8R2	8.7R2	N	N	N	N	N	N	N	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	N	8.7R1	8.7R1	N	N	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
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

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
L2 GRE Tunnel Access (Edge) (bridge ports)	N	N	Y	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-P24/P24Z8	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
Fast 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
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.

Appendix B: MACsec Platform Support

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

MACsec Support (MACsec site license required)	
OmniSwitch 9900	
OS99-CMM	4X10G mode only (Static mode only)
OS99-GNI-48/P48	10M/100M/1G ports
OS99-XNI-48/P48	10G ports (Static mode only)
OS99-XNI-U48	10G ports (Static mode only)
OS99-XNI-P48Z16	1G/2.5G/5G/10G (16x) 1G/10G (32x)
OS99-GNI-U48	1G ports
OS99-XNI-U24	10G ports (Static mode only)
OS99-XNI-P24Z8	1G/2.5G/5G/10G (8x) 1G/10G (16x)
OS99-XNI-U12Q	10G / 4x10G Uplink (Static mode only)
OS99-XNI-UP24Q2	10G(Fiber)/4x10G Uplink (Static mode only) 10G (Copper) (Static mode only)
OS99-CNI-U8	Not Supported
OmniSwitch 6900	
OS6900-X48C4E	Dynamic mode only on all ports. Supports 256-bit key length.
OmniSwitch 6860(E)	
OS6860(E)	All models support MACsec on 10G ports.
OS6860E-P24	1G/10G ports.
OS6860E-P24Z8	1G/10G ports (not supported on 2.5G ports).
OmniSwitch 6860N	Dynamic mode only. All OS6860N models support 256-bit key length.
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.R1
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:
                                                              Services  Num    Tandem
Root Bridge
BVLAN   ECT-algorithm     In Use  mapped    ISIDS  Multicast  (Name : MAC Address)
-------+-----------------+-------+---------+------+----------+-------------------------------
---------
  4000  00-80-c2-01       YES     YES           5  SGMODE
  4001  00-80-c2-02       NO      NO            0  SGMODE
```

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

Appendix 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 chassid-id 1 is the Master, the Slave with chassis-id 2 will reload with the new image files. When Slave chassis-id 2 has rebooted and rejoined the VC, the Slave with chassis -id 3 will reboot and rejoin the VC. Once the Slaves are complete they are now using the new image files. The Master chassis is now rebooted which causes the Slave chassis to become the new Master chassis. When the original Master chassis reloads it comes back as a Slave chassis. To restore the role of Master to the original Master chassis the current Master can be rebooted and the original Master will takeover, re-assuming the Master role.

Modular Chassis - The chassis will first verify that it is in a state that will allow a successful ISSU upgrade. It will then copy the image and configuration files of the ISSU specified directory to the secondary CMM and reload the secondary CMM which becomes the new primary CMM. The old primary CMM becomes the secondary CMM and reloads using the upgraded code. As a result of this process both CMMs are now running with the upgraded code and the primary and secondary CMMs will have changed roles (i.e., primary will act as secondary and the secondary as primary). The individual NIs can be reset either manually or automatically (based on the NI reset timer).

Supported Upgrade Paths and Procedures

The following releases support upgrading using ISSU. All other releases support a Standard upgrade only.

Platform	AOS Releases Supporting ISSU to 8.9R2 (GA)
OS6360	8.9.73.R01 (Major GA) 8.8.56.R02 (Minor GA) 8.8.152.R01 (Major GA) 8.7.98.R03 (Minor GA) 8.7.252.R02 (Major GA)
OS6360-P10A	8.9.73.R01 (Major GA) 8.8.8.R03 (Minor GA) – Note: Uses same image file as other OS6360 platforms.
OS6465	8.9.73.R01 (Major GA) 8.8.56.R02 (Minor GA) 8.8.152.R01 (Major GA) 8.7.98.R03 (Minor GA) 8.7.252.R02 (Major GA)
OS6560	8.9.73.R01 (Major GA) 8.8.56.R02 (Minor GA) 8.8.152.R01 (Major GA) 8.7.98.R03 (Minor GA) 8.7.252.R02 (Major GA)
OS6570M	8.9.63.R02 (Major GA)
OS6860(E)	8.9.73.R01 (Major GA) 8.8.56.R02 (Minor GA) 8.8.152.R01 (Major GA) 8.7.98.R03 (Minor GA) 8.7.252.R02 (Major GA)
OS6860N*	8.9.73.R01 (Major GA) 8.8.56.R02 (Minor GA) 8.8.153.R01 (Major GA)
OS6865	8.9.73.R01 (Major GA) 8.8.56.R02 (Minor GA) 8.8.152.R01 (Major GA) 8.7.98.R03 (Minor GA) 8.7.252.R02 (Major GA)
OS6900	8.9.78.R01 (Major GA) 8.8.56.R02 (Minor GA) 8.8.152.R01 (Major GA) 8.7.98.R03 (Minor GA) 8.7.252.R02 (Major GA)
OS6900-V72/C32/ X48C6/T48C6/X48C4E/V48C8*	8.9.78.R01 (Major GA) 8.8.56.R02 (Minor GA) 8.8.153.R01 (Major GA) 8.8.152.R01 (Major GA)

OS9900	8.9.78.R01 (Major GA) 8.8.56.R02 (Minor GA) 8.8.152.R01 (Major GA) 8.7.98.R03 (Minor GA) 8.7.252.R02 (Major GA) **Note**: ISSU is currently not supported on an OS9900 VC-of-1.
*ISSU is not supported to 8.9.R01 from any release prior to an 8.8.R01 build. This is due to improvements made by transitioning from software on chip (SoC) to software development kit (SDK) APIs that were implemented in 8.8.R01. ISSU functionality will be supported for all future releases from 8.8R1 and above.	

8.9R2 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
                                 Address             Address
Chas  MAC-Address          Local IP              Remote IP          Status
-----+-------------------+---------------------+-------------------+-------------
1       e8:e7:32:b9:19:0b  127.10.2.65        127.10.1.65       Connected
```

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

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

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

```
6900-> rm –r /flash/issu_dir
```

6. Log out of the Slave chassis:

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

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

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

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

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

9. Upgrade the image files using ISSU:

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

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

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

This indicates that the ISSU is completed

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

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

```
6900-> debug show virtual-chassis topology
Local Chassis: 1
Oper                                        Config   Oper                      System
Chas  Role         Status              Chas ID  Pri   Group  MAC-Address        Ready
-----+------------+-------------------+--------+-----+-------+------------------+-------
1     Master        Running             1        100   19     e8:e7:32:b9:19:0b  Yes
2     Slave         Running             2        99    19     e8:e7:32:b9:19:43  Yes
```

10. Verify the Software Upgrade

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

```
OS6900-> show microcode
/flash/working
Package           Release                 Size      Description
-----------------+------------------------+--------+------------------------------------
Tos.img           8.9.107.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-> copy running certified

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

Appendix G: FPGA / U-boot Upgrade Procedure

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

CR / Feature	Summary	
CRAOS8X-12042	Description	Switch does not shutdown after crossing danger threshold temperature.
	FPGA Version	0.7
	Platforms	OS6465-P28
CRAOS8X-7207	Description	Chassis reboots twice to join a VC.
	FPGA Version	0.7
	Platforms	OS6560-P24Z24,P24Z8,P48Z16 (903954-90)
CRAOS8X-4150	Description	VC LED status behavior.
	U-boot Version	0.12
	Platforms	OS6865-U28X
8.7R1 Release		
CRAOS8X-16452	Description	Port remains UP when only SFP is connected.
	FPGA Version	- 0.6 (OS6560-P48Z16 (904044-90)) - 0.7 (OS6560-48X4, OS6560-P48X4) - 0.8 (OS6560-X10)
	Platforms	OS6560-P48Z16 (904044-90), OS6560-48X4, OS6560-P48X4, OS6560-X10
CRAOS8X-11118	Description	1000BaseT SFP interface up before system ready
	U-boot/FPGA Version	- U-boot version 8.6.R02.189 - FPGA version 0.1.11
	Platforms	OS6900-X72
Fast/Perpetual PoE	Description	Fast and Perpetual PoE Support
	FPGA Version	0.7 (OS6860E-P24Z8) 0.10 0.14 (OS6865-U28X) 0.25 (OS6865-P16X/U12X)
	Platforms	OS6860/OS6865
8.7R2 Release		
CRAOS8X-4813/13440	Description	Uboot unable to mount NAND flash with UBIFS errors
	U-boot Version	8.7.2.R02
	Platforms	OS6465(T), 6560-24X4/P24X4/48X4/P48X4/X10
CRAOS8X-13819	Description	Uboot unable to mount eUSB flash
	U-boot Version	8.7.2.R02
	Platforms	OS6560-24Z24/P24Z24/24Z8/P24Z8/P48Z16 (all PNs), 6865
CRAOS8X-22857	Description	OS6560-P24Z24 reloads continuously with 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)

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.		

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_8165
- 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_8165
Parse /flash/fpga_kit_8161
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: 1. 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. 2. CPLD versions are compatible with previous AOS releases. Downgrading to a previous AOS release is supported: a. Backup the configuration files from previous release. b. Upgrade to AOS Release 8.8.R02. c. Upgrade the CPLD. d. Downgrade to previous release. (ISSU is not supported when downgrading AOS) e. Restore the configuration.		

Note: AOS must be upgraded 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
CRAOS8X-33298 CRAOS8X-37878 CRAOS8X-37323	**Summary:** When using the OS6465-P12 (ENH-240) with the OS6465-BPN (75W) power supply PoE power is denied. **Explanation:** In AOS releases prior to 8.9.107.R02 the OS6465-P12 (ENH-240) was expecting 50V as the minimum input voltage. The OS6465-BPN power supply provides 48V input which resulted in PoE power being denied. Beginning in 8.9.107.R02 AOS accepts an input of 44V allowing the OS6465-BPN to provide PoE power.
Case: **00999999** CRAOS8X-35470	**Summary:** If there is an unexpected power loss, there may be rare cases where a write to NAND flash is not able to be completed resulting in a bad file system block to be left in the flash. This issue may affect the OS6360, OS6465, and some OS6560-(P)24X4/(P)48X4/X10 platforms. **Explanation:** The resulting bad file block may cause the reboot process to stop at uboot. In most cases the switch can be recovered by following the existing uboot recovery process documented in the 'Disaster Recovery Using a USB Flash Drive' section of the Switch Management Guide. In the rare instance that the switch cannot be recovered please contact Customer Support. The latest uboot versions provided with the 8.9R2 release fix the issue for the affected platforms. 🔒 Click for Additional Information
Case: **00647473** *CRAOS8X-35488*	**Summary:** On an OS6865-U28X switch, the external-cpu status is down and the "swlogd ChassisSupervisor external CPU Mgr INFO: External CPU unresponsive, resetting" message is seen in the switch logs. **Explanation:** This is a software issue that is fixed from AOS 8.9R02 GA. 🔒 Click for Additional Information
Case: **00588926** *CRAOS8X-31428*	**Summary:** Randomly switch is unreachable when IP Interface is bound to SPB Service Inline Routing. **Explanation:** Mixing of indexes resulted in issue state. 🔒 Click for Additional Information
Case: **00629412,** **00639281** *CRAOS8X-34143,* *CRAOS8X-34892*	**Summary:** Add in logs generated when Power Failure/Fan Failure the Chassis ID in case of Virtual Chassis. 🔒 Click for Additional Information
Case: **00643608** *CRAOS8X-35170*	**Summary:** Add logs/traps when switch running in NaaS mode is entering into grace period or degraded mode. 🔒 Click for Additional Information
Case: **00645215** *CRAOS8X-35275*	**Summary:** SSAPP main ERR: Error returned from swLogLibrarySnapShot. 🔒 Click for Additional Information

Case: **0064827** *CRAOS8X-35520*	**Summary:** Following upgrade from AOS 8.8R02 MQTT error are noticed (mqttdConnectToBroker: mqttdStartMqttClient() error). **Explanation:** IoT Profiling package is not updated during image upgrade. 🔒 Click for Additional Information
Case: **00653790** *CRAOS8X-36079*	**Summary:** Following upgrade in AOS 8.9R01 show log swlogs are truncated. 🔒 Click for Additional Information
Case: **00668683** *CRAOS8X-37194*	**Summary:** Syslog Server certificate not validated by OmniSwitch when enabling "Client Validate Certificate". **Explanation:** Certificate verification process causes this issue when both key usage and extended key usage extensions are present in the certificate 🔒 Click for Additional Information
Case: **00649663** *CRAOS8X-36430*	**Summary:** For same VLAN members, when QoS policy is applied on OS6360, member ports on the other side of OS9900 goes into blocking state. **Explanation:** While the QoS configurations are applied, the ingress STP BPDU frames are dropped in OS6360. This causes the OS6360 to become root bridge and it starts sending BPDUs to OS9900. As the OS9900 has lower STP priority, it discards the unexpected BPDUs from OS6360 and blocks the port. 🔒 Click for Additional Information
Case: **00673435** *CRAOS8X-37566*	**Summary:** For OS6560-P48Z16 model, front panel ports are not visible in GUI. **Explanation:** While accessing the GUI of the switch, front panel ports 17 and 18 were missed. Instead, 33 and 34 were duplicated twice. This is just a cosmetic bug. 🔒 Click for Additional Information
Case: **00660081** ***CRAOS8X-36612***	**Summary:** IP phone (SAMSUNG, SMT-i2205) goes to a fault state in "show lanpower slot 1/1" when it is connected particularly with OS6360 switch. **Explanation:** In 802.3bt, Class 0 devices will be considered as class 3 as the maximum port power limit is 15.4 watts. It can power on Class-0 devices as well. The 802.3BT firmware could be accepting the low current value or I-min range for powering up such legacy devices. 6360-P24/P48 supports 802.3BT but the image is not integrated for it. Only 6360-PH24 has support for 802.3BT in the code. PoE version had been upgraded from PD69200 to PD69220 that supports 802.3BT in it. 🔒 Click for Additional Information
Case: **00661090** *CRAOS8X-36696*	**Summary:** OSPF buffer overflow for jumbo packet 1500 MTU. **Explanation:** Generally, the devices AOS, Huawei, and Cisco are configured with 1500 MTU. If the OSPF packet is

	bigger than the usual packet size of 1500 bytes, the packets are fragmented. Now in the scenario, the Cisco and Huawei devices send the OSPF packet with 9200 bytes and which is sent over ethernet with MTU 1500 bytes. While doing the fragmentation the last packet is getting failed because in the AOS switches the buffer max size is 9198. OSPF will not define how the packets need to be fragmented, in some cases, OSPF packets could be up to 65535 bytes (Including the header). But in AOS device, the variable defined for the OSPF buffer is the same as the jumbo frame size (9198), which is dropping the packets. When there is a connection with OSPF neighbor routers with a huge routing table, the memory variable allocated in the Alcatel device for the OSPF is not sufficient. 🔒 Click for Additional Information
Case: **00656545** *CRAOS8X-2078*	**Summary:** In OS6900-T48C6, webview (Home-> Physical-> Chassis Mgmt->Chassis Visualization) shows incorrect port numbers for the VFL ports. **Explanation:** OS6900-T48C6 in VC of 3 and has VFL link connected to ports 1/1/51 and 1/1/54. In webview, the switch shows as if the VFL link is connected to ports 1/1/51 and 1/1/51. There is no port 1/1/54. This is a cosmetic bug. 🔒 Click for Additional Information
Case: **00647353** *CRAOS8X-35535*	**Summary:** For IPv6, no warning prompt appears for non-existing VLAN. **Explanation:** In IPv4 configuration, if a VLAN does not exist, there will be a warning when configure the ipv4 address binding to that specific VLAN, but no warning when configure ipv6 interface. 🔒 Click for Additional Information
Case: **00656195** *CRAOS8X-36286*	**Summary:** The OS6465 switch is stuck in a boot loop after performing the SNMPWalk using the Zabbix tool. The PMD getting generated for alarmMgrCmm. **Explanation:** Found the parameters of function alarmMgrCmm_outputConfigGet() are causing the stack corruption. 🔒 Click for Additional Information
Case: **00555599** *CRAOS8X-27962*	**Summary:** The zcNi task failed and the VC of 4xOS6900-X72 switches are restarted with PMD file. swlogd ChassisSupervisor appMgr ALRT: Task /bin/zcNi vrf () restart failed or restart count exceeded - board restarting **Explanation:** MDNS gateway device traps the packets to the CPU and floods them to configured gateway VLAN. When there are many packets to be flooded, transmit failures were seen while sending out the packets to the packet driver from zcNi. 🔒 Click for Additional Information
Case: **00661778** *CRAOS8X-36955*	**Summary:** OS6570M is not receiving an IP address from the DHCP SERVER due to the unicast DST mac address in the OFFER Packet. **Explanation:** This is the issue with the DHCP server at the client location; Both 6x and 8x behaviors are RFC

	compliant - setting the BCAST bit is a client option, and the old DHCP server is not adhering to it in the responses sent. The packet is sent to unicast mac, which is not trapped in the CPU, prior to getting the ACK. Changes are done to Adhere DHCP-client to interop with the server in the customer network as well (which was not adhering to the RFC in this scenario). 🔒 Click for Additional Information
Case: **00650882** *CRAOS8X-35735*	**Summary:** Should throw warning message when configuring Auto-neg in an empty port as it is not supported for 1G/10G **Explanation**: It is allowed to configure Autoneg in an empty port in current AOS 8X release. From 8.9.R02, warning message has been added when configuring auto-neg in an empty port. 🔒 Click for Additional Information
Case: **00651231** *CRAOS8X-35856*	**Summary:** Requirement to reduce BYOD login/logout time and reason for the UNP user went to Blocking. **Explanation:** **To reduce the BYOD login/logout time:** More time takes to logout BYOD page. The time is based on the pause-timer configured in the UNP configuration. As per current AOS flow, there were two cycles to clear the context after logout[Minimum value: Configured pause timer, Maximum value=2Xpause-timer]. From 89R02 release, instead of waiting for 2 cycles of tier, it happens on the next immediate timeout[1 cycle, which would be less than 60secs or configured pause-timeout]. **Reason for UNP user went in BLOCK status:** Once the pause timer expires, the CP auth should be successful and the user should be moved to Active status. However, the switch does not move the user to active status and keeps in Block status even after the pause-timer is expired. The issue is that the auth profile returned from the server does not have the VLAN mapped to it and hence the user stays in block status. VLAN mapping for the UNP profile is a mandatory requirement for the CoA role change. This will also be documented in the 89R02 guides. User should not be put into a Blocking state even when there is no VLAN mapping for post auth. Changes made in the 89R02 release to send a NACK to UPAM with the error “session context not found” by keeping the user stays in Preauth profile when there is no vlan mapping for Postauth. 🔒 Click for Additional Information 🔒 Click for Additional Information
Case: **00669882** *CRAOS8X-37323*	**Summary:** OS6465H-P12 (ENH 240): Lanpower status is 'Denied' with "SDR-75-48" PSU delivering 50V Input Voltage. **Explanation**: The minimum voltage level that can be configured with BT firmware (3.xx) is 50V. OS6465H-P12 (ENH 240) is shipped with 3.54 (BT) firmware. So, this switch cannot accept any power supply which is less than 50V output. 75W watts (SDR-75-48) power supply's output voltage level is ~48V. So, this power supply is not supported on IEEE802.3BT PSEs. 🔒 Click for Additional Information

Case: **00659602** *CRAOS8X-36585*	**Summary:** OS6900-X48C6: Switch does NOT shutdown even when the chassis temperature is over danger threshold. **Explanation:** This is an expected behavior. In OS6900-X48C6 switch, we do not have any mechanism to power off the switch when the chassis ambient air temperature rises above the danger threshold. The Hardware Guide would be corrected in AOS 8.9R02 🔒 Click for Additional Information
Case: **00638474** *CRAOS8X-34837*	**Summary:** OS6465-BPN-X: Output voltage of SDR-480-48 power supply is incorrectly displayed as 48VDC instead of 54.5VDC in the Hardware Guide. **Explanation:** On the front panel label of the power supply, it is mentioned that the output is 48V and not 54.5V. This power supply is already with that label; however, the output was regulated (adjusted) by the PSU vendor to "54.5V" to meet the Alcatel Product's requirement. Also, a note is added in AOS 8.9R02 Hardware Guide of OS6465 to disregard the power supply label of SDR-480-48 with incorrect information. 🔒 Click for Additional Information
Case: **00670941** *CRAOS8X-37378*	**Summary:** OS6900-X48C6 and OS6860N: Memory usage constantly at 10%. **Explanation:** From the performance test report to increase the memory of the switch revealed that the switch memory is constantly at 10%; however, the 'top' output from SU show that the switch memory seems to be used more than 10%. This is a display bug in CLI. 🔒 Click for Additional Information
Case: **00670979** *CRAOS8X-37359*	**Summary:** OS6900-X72: Auto-negotiation stays 'Enabled' in ports 1/1/1-48 after using SFP-GIG-T. **Explanation:** If 1G SFP in configured in any of the ports between 1/1/1-48, then this would automatically change "Autoneg enable" in the ports. If the 1G SFP is removed from the port 1/1/1 the "show interface status" output would still continue to show "autoneg enabled". Also, this will not be reflected in the config even though the port is now back to 10GIG. 🔒 Click for Additional Information
Case: **00667814** *CRAOS8X-37158*	**Summary:** OS6865-P16X not disabling Optical TX when port is admin down. **Explanation:** In OS6865-P16X switch, port 1/1/1 and 1/1/2 are 10GIG by default. In this ports, if SFP-IG-LX or iSFP-GIG-LX is configured the port would negotiate properly to 1GIG. When the interface is admin DOWN, the expected value in "Output (dBm)" is "-inf"; however, the SFP continuous to display DDM 'Output' value as '-5.533'. 🔒 Click for Additional Information
Case: **00666203** *CRAOS8X-37015*	**Summary:** OS6900-X48C6: Values of MIB "entPhysicalVendorType" for "SFP_10GIG_BASE_T" and "SFP_100GBASE_CR4" were incorrectly updated as "zeroDotZero". **Explanation:** "entPhysicalVendorType" 869, 883 and 893 should give the value of "SFP_10GIG_BASE_T". And,

	“entPhysicalVendorType” 901, 904, 983 and 986 should give the value of "SFP_100GBASE_CR4". However, the switch give an incorrect value as "zeroDotZero". 🔒 Click for Additional Information
Case: **00660851** *CRAOS8X-36650*	**Summary:** OS6900-X48C6 continues to displays DDM 'Output' and 'Input' values even when the port is admin-state disabled. **Explanation:** In OS6900-X48C6 switch, SFP-10G-SR is connected. As expected, the interface ddm output display the output and Input value in dBm. When the interface is admin DOWN, the expected value in "Output (dBm)" is "-inf"; however, the switch continues to display the Tx optical power value as if the port was up (i.e. -2.55 dBm). This issue is not limited to SFP-10G-SR, it is seen with SFP-10G-LR in SM and MM. 🔒 Click for Additional Information
Case: **00660832** *CRAOS8X-36646*	**Summary:** OS6900-X48C6: power loss or the power cord removal in Power Supply is still notified with "UNPOWERED" status. **Explanation:** When there is power loss or the "power cord" from the power supply is removed, the show command output still display the power supply status as "UNPOWERED". 🔒 Click for Additional Information
Case: **00652427** *CRAOS8X-35879*	**Summary:** OS6560: Flash Between CMMs with the status "NOT SYNCHRONIZED". **Explanation:** Before making configuration changes, the status of "Flash between CMMs" is 'SYNCHRONIZED'. Performed change in configuration by introducing a new VLAN and executed "write memory". This action moved the status of "Flash between CMMs" as "Not Synchronized". This is a legacy behavior and the issue is caused due to the banner file not been copied to the slave units during synchronization. Also, this issue is not limited to OS6560 and it would be seen with all AOS 8.x switches. 🔒 Click for Additional Information
Case: **00658379** *CRAOS8X-36476*	**Summary:** OS6900-X48C6: Manufacture Date of PowerSupply is wrongly updated in CLI output and SNMP-MIB output. **Explanation:** The Manufacture Date of the power supply in the CLI output and in the SNMP-MIB output were incorrectly updated. This is due to indexing issue in eeprom manufacture date. 🔒 Click for Additional Information
Case: **00657886** *CRAOS8X-36437*	**Summary:** O6900-X72: Fake link UP in "SFP-GIG-T" without any cable. **Explanation:** In OS6900-X72 switch, if "SFP-GIG-T" (or any "1000Base-T" SFP) is inserted in any port with autoneg 'Disable', the port LED would be UP without any cable. Also, the port would be operationally UP. This is a legacy behavior. 🔒 Click for Additional Information

Case: **00651019** *CRAOS8X-35872*	**Summary:** OS6900-X72: 1GIG port stays down after toggling auto-negotiation, if the peer switch is OS6900-X48C6. **Explanation:** OS6900-X68C6 does not support auto-negotiation with 1GIG transceivers. If OS6900-X48C6 and OS6900X72 switches are connected directly with 1GIG "SFP-GIG-LX", then auto-negotiation need to be disabled on peer switch. Upon disconnecting auto-negotiation, the port came UP. However, after togging the auto-negotiation the port stays DOWN. 🔒 Click for Additional Information
Case: **00648589** *CRAOS8X-35570*	**Summary:** OS6560-P24X4/P48X4: Switch time rollback to year 1970 after Warm reload. **Explanation:** OS6560 switch does not have a battery-backed RTC. It has a super-capacitor, which will allow the RTC to hold time for somewhere around 6 minutes of power-off time. Beyond that, the switch would lose anything stored in the RTC. The switch should be configured with an external NTP server, so that the time would be in sync after every reload. The switch will not keep time longer than 6 minutes (roughly) of being powered off. This is not a hardware failure, this is according to design. 🔒 Click for Additional Information
Case: **00645461** *CRAOS8X-35300*	**Summary:** OS6465T: eoamCmm LCMM_FRMWRK ERR message. **Explanation:** When polling the MIB object "dot3OamEventLogTable", the switch would check the oam module(EFM-OAM). If the database is empty or the "ethernet-oam" is not configured in the switch then the following errors “eoamCmm LCMM_FRMWRK ERR “ would be generated. There is no functional impact in the switch due to this error. 🔒 Click for Additional Information
Case: **00662660** *CRAOS8X-35136*	**Summary:** OS6860N: Mac-address not getting learnt on some UNP or SAP service configured port. **Explanation:** Broadcom sdk set wrongly the port as invalid which causes all traffic to be discarded. Removing the UNP/SAP configuration and putting a vlan configuration or rebooting the switch resolved the issue. 🔒 Click for Additional Information
Case: **00654185** *CRAOS8X-36334*	**Summary:** OS9907: When trying to change the version of ERPV1 in RPL-NODE OS9907 to ERPV2 in ring 1 with the cli command : "erp-ring 1 reset-version-fallback", the following warning message is displayed in the swlogs: "[CMM B] <Date> ConfigManager MCH WARN Send configuration failed for APPID_ERP (49/0)." **Explanation:** This harmless warning message indicates that the cli command did not apply to the CMMB.As, it does not really have any added value it will be removed in 8.9R02. 🔒 Click for Additional Information

Case: **00652554** ***CRAOS8X-35882***	**Summary:** OS6900: devices connected to UNP/dynamic SAP can't be pinged from the OS6900V48C8. **Explanation:** ARP entries for those devices were erroneous and only mentioned the port instead of a SAP entry. SAP entries were discarded once the VP number reached 8192 , because of a wrong check of VP numbering in the port API. 🔒 Click for Additional Information
Case: **00662364** *CRAOS8X-36742*	**Summary:** The OS6860N-P48M switch on boot up displays Evaluation Copy. **Explanation:** The issue was noticed in BIOS v43.0b.07.00 and the reported issue is addressed, to remove the string "Evaluation", in the later release AOS 8.9.R02. 🔒 Click for Additional Information
Case: **00659317** *CRAOS8X-36580*	**Summary:** "vcsetup.cfg does not exist, get chassisId from Chassis Supervisor!" log is filling the swlog. **Explanation:** "vcsetup.cfg does not exist, get chassisId from Chassis Supervisor!" is logged in switch after removing a running directory. Fix is part of 8.9R02 GA. 🔒 Click for Additional Information
Case: **00657959** *CRAOS8X-36586*	**Summary:** Configuring the UNP port template using the "port range" command is executed without an error, however, the configuration is not applied to the ports and not displayed in the show configuration snapshot output. **Explanation:** If any port is configured with the UNP port template, then the UNP port range command will not be applied to all the ports that are specified. The range, config would be applied up only to the specified port initially configured as port-type bridge. The code change is to display the below error to inform the user that this command is not taken in account: "ERROR: Non-UNP port(s) found in the given range" 🔒 Click for Additional Information
Case: **00655778** *CRAOS8X-36478*	**Summary:** PD devices connected to a 6465 od 6560 having lanpower disabled are still delivering PoE after a reload despite that the lanpower is disabled. **Explanation:** Dynamic Disabling lanpower/PoE feature on specific port with lanpower port 1/1/1 admin-state disable. The PoE device is still powered on after reload. 🔒 Click for Additional Information
Case: **00653355** *CRAOS8X-36374*	**Summary:** The combo port (1/1/9 or/and 1/1/10) is up configured to be at100Mb/s, full duplex, moves to 1000M full duplex after reload. **Explanation:** The combo port (1/1/9 or/and 1/1/10) is up configured to be at100Mb/s, full duplex. However, after a switch restart, the link moves to 1000Mb/s (1Gb/s) at full duplex. The opposite end is always fixed at 100Mb/s full duplex. 🔒 Click for Additional Information

Case: **00636632** *CRAOS8X-35093*	**Summary:** 6860E VC and with two destination port-mirroring config, after a period of time some packets were missing in one of the two destinations, If reconfigured the switch with only one destination packets are not mirrored. **Explanation:** This is expected for the 6860E switch two destination are not supported till 8.9R01 GA release. When using non supported scenario of two destination configuration the pmm module configured in the hardware was having the mapping of two destinations stuck. Starting from 8.9R02GA port-mirroring two destinations config will be supported on 6860E. 🔒 Click for Additional Information
Case: **00634791** *CRAOS8X-34967*	**Summary:** OS6465T-P12 virtual-chassis is not forming or is splitting because of the "Deny" of network group Switch QoS. **Explanation:** Two OS6465, Both the switches have formed the VC after the successful auto-reload. Then, after applying QoS config the switch splited because of the Deny action of network group Switch which disturb the ISIS protocol. 🔒 Click for Additional Information
Case: **00653949** *CRAOS8X-36167*	**Summary:** OS6860 switch is sending different value format of chaasis ID in SNMP. **Explanation:** Philips monitor are not able to read the SNMP response as the chassis ID is in HEX format and the LLDP chassis ID is sent as ASCII format, the SNMP will be sent as ASCI. 🔒 Click for Additional Information
Case: **00652092** *CRAOS8X-35815*	**Summary:** The CLI LLDP command for configuring the port-id subtype to use the port name, does not allow for the use of a port range even though the configuration is stored as a range when multiple adjacent ports are configured. **Explanation**: There is also a method to configure the port-id subtype chassis wide which can be used as an alternative. 🔒 Click for Additional Information
Case: **00668756** *CRAOS8X-36848*	**Summary**: Cannot configure a port as SAP service access port if an IP interface exists for the default VLAN mapped on the port. **Explanation:** Cannot configure a port as SAP service access port if an IP interface exists for the default VLAN mapped on the port. An error message is thrown while trying to configure the port. 🔒 Click for Additional Information Go to Atrium tool, Customer care Articles, find the article, and copy link from “Public URL” field.
Case: **00659520** *CRAOS8X-36848*	**Summary:** Cannot configure a port as SAP service access port if an IP interface exists for the default VLAN mapped on the port. **Explanation:** Cannot configure a port as SAP service access port if an IP interface exists for the default VLAN mapped on the port. An error message is thrown while trying to configure the port.

	🔒 Click for Additional Information Go to Atrium tool, Customer care Articles, find the article, and copy link from “Public URL” field.
Case: **00663045** *CRAOS8X-36848*	**Summary:** Cannot configure a port as SAP service access port if an IP interface exists for the default VLAN mapped on the port. **Explanation:** Cannot configure a port as SAP service access port if an IP interface exists for the default VLAN mapped on the port. An error message is thrown while trying to configure the port. 🔒 Click for Additional Information Go to Atrium tool, Customer care Articles, find the article, and copy link from “Public URL” field.
Case: **00650056** *CRAOS8X-36283*	**Summary**: No connectivity on service port. **Explanation:** Connectivity issue is observed on service access port. There is no mac-learning and all ingress traffic is discarded. 🔒 Click for Additional Information Go to Atrium tool, Customer care Articles, find the article, and copy link from “Public URL” field.
Case: **00645183** *CRAOS8X-35632*	**Summary:** Link stability issue between OS6900-V48C8 and OS6560-P48Z16 with SFP_10G_LR. **Explanation:** Link may not come UP when SPF SFP_10G_LR is used between OS6900-V48C8 and OS6560-P48Z16. The issue is random. 🔒 Click for Additional Information
Case: **00631489** *CRAOS8X-35632*	Summary: QoS policy rule does not match for some random IP addresses included in a policy network group. **Explanation**: Policy rule has been configured to allow or deny IP addresses which are in a policy network group. The policy rule does not hit for some of the IP addresses included in the group. 🔒 Click for Additional Information Go to Atrium tool, Customer care Articles, find the article, and copy link from “Public URL” field.
Case: **00658739** *CRAOS8X-36597*	**Summary:** Switch not booting up completely after power outage. **Explanation**: Upon power cycling the switches, mostly during power outages, the switch is not booting up completely and getting stuck at Marvel prompt. The reason for the issue has been found to be with UBOOT. Hence, the observed problem is a SW issue however, not related to the switch AOS, it is with UBOOT file. The observed Uboot issue has been fixed and new Uboot version file would be released along with AOS 8.9 R01 GA. 🔒 Click for Additional Information
Case: **00638000** *CRAOS8X-34802*	**Summary:** Loopback detection transmission timer not working on SAP ports. **Explanation:** When configured the loopback-detection transmission-timer to a lower value than the default

	value of 30s, the switch does not take the value into account for service access ports and service access linkaggs. The fix would be available under AOS 8.9 R02 GA. 🔒 Click for Additional Information
Case: **00664062** *CRAOS8X-36896*	**Summary:** OS6860E-P48: Lanpower drop in switch with ERR: lpRxCallbackHandler 5019: i2c Receive Sync Lost 198 199. **Explanation:** The loss in lanpower is seen when the power controller loses internal communication. The fix is available in 8.9 R02 to avoid the loss of lanpower even if the communication is lost with the controller. 🔒 Click for Additional Information
Case: **00631681** *CRAOS8X-34553*	**Summary:** Unable to get SNMP response for polled OIDs from switch or external tool for “ENTITY-MIB. **Explanation:** While trying to poll the OIDs from external tool or from switch, unable to get the SNMP response specific to “ENTITY-MIB”. 🔒 Click for Additional Information
Case: **00644564** *CRAOS8X-35228*	**Summary:** AOS 8 switch- UNP LDAP policies not persistent after the switch reload. **Explanation:** If a switch is configured with UNP ldap-policies from the OV unified policy menu; if the switch gets disconnected with OV2500 or switch reload happens, the ldap rule will not be available in the switch running configuration. 🔒 Click for Additional Information
Case: **00645657** *CRAOS8X-3543*	**Summary:** PoE stopped on one of the OS6860E VC units suddenly. **Explanation:** PoE devices on slot 1 went down abruptly. When checking the configuration, lanpower service was missing for the slot 1. Configuring lanpower service configuration for the affected slot restored the service. 🔒 Click for Additional Information
Case: **00661509** *CRAOS8X-36712*	**Summary:** Policy Based Routing QoS policy is matched for the traffic that are supposed to match the higher precedence policy rule. **Explanation:** Users from HSA network to Server network going through Core VC OS6900-V48 are unable to reach. Traceroute from HSA network IP to one of the server IPs, shows that the traffic is taking the permanent-gateway path, though it should be only allowed as per the QoS policy rule r1 (which has a higher precedence) value). Applying “QoS apply” fixes the issue temporarily. 🔒 Click for Additional Information
Case: **00638921** *CRAOS8X-35124*	**Summary:** “IP helper per-vlan mode” commands for multinetted VLANs are not converted properly to “ip

	dhcp relay interface ..” commands” via ISSU/standard upgrade from 8.4.x to 86R02 and later releases. **Explanation:** Command conversion works only for the primary IP interface of the multinetted VLAN. 🔒 Click for Additional Information
Case: **00622155** *CRAOS8X-35817*	**Summary:** MAC address is not learnt on the ports for few devices when port-security is enabled on the ports of OS6860N. **Explanation:** When the device is initially connected to the port where port-security is enabled, it does not learnt the device MAC address when the only packet it receives is DHCP DISCOVER broadcast packets. Disabling port-security makes the port to learn the MAC address for the same device with the same initial DHCP packets. 🔒 Click for Additional Information
Case: **00646495** *CRAOS8X-35423*	**Summary:** In OS6900-T48C6, during master chassis reboot, ports of slave chassis go into violation state. **Explanation:** User intended to manage switches by connecting EMP ports to the VC of 3 x OS6900-T48C6, where flood-limit configured on the ports. When the master chassis is intentionally or accidentally rebooted, ports of slave chassis go into violation state. 🔒 Click for Additional Information Click for Additional Information
Case: **00644625** *CRAOS8X-35258*	**Summary:** In OS6860N-U28, configuring long timeout in linkagg is not read into switch memory. **Explanation:** User had OS6860N switch, connecting it with the controller, and configuring the linkagg on both devices. Both controller and switch had a long timeout configured. When the switch reboots, the long-timeout configuration was getting lost from the switch. 🔒 Click for Additional Information
Case: **00656505** CRAOS8X-36319	**Summary:** OS6860N-U28 dying Gasp timestamp on the OVE is wrong could be related to the timetick from the SNMP/Dying Gasp Frame. Explanation: The OS6860N-U28 SNMP timeticks is wrong. 🔒 Click for Additional Information
Case: **00650476** *CRAOS8X-34915*	**Summary:** OS6465T-12: Not reading CISCO EFM OAM PDU dying Gasp correctly and not setting the dying Gasp bit correctly. **Explanation:** OS6465T-12: Not reading CISCO EFM OAM PDU dying Gasp correctly and not setting the dying Gasp bit correctly. The efm-oam does not appear to work correctly. With regards to the issue: (efm-oam), it is not receiving EFM OAM PDUs from the remote device even though a port monitor packet capture on the port shows that it is receiving ETH OAM PDUs, and not sending EFM OAM PDU dying Gasp correctly. OAM PDUs are send by setting DG Flag, where as in the case of power failure it is not set.

	🔒 Click for Additional Information
Case: **00639104** ***CRAOS8X-34808***	**Summary:** ARP issue QinQ over SPB using ip interface based in service. **Explanation:** Arp or icmp reply packets sent by the switch on double tagged sap association for service interface are corrupted due to double addition outer tag field in the packet. 🔒 Click for Additional Information
Case: **00638912** CRAOS8X-35064	**Summary:** OS6465T-12: SNMP Dying Gasp sometimes send to the wrong interface where the default route is pointing to **Explanation:** 6465T-12 devices sending dying gasp SNMP traps to the wrong interface when there is a power failure. 🔒 Click for Additional Information
Case: **00649094** CRAOS8X-35597	**Summary:** OS6900-V48C8: Portgroup speed changed after the reboot. **Explanation:** While the speed configuration portgroup is applied and the directories are synced, the port group speed value has changed after the reboot - 8.8R02. Fixed in 8.9R01 for a standalone unit, but the same issue was discovered in the VC unit. 🔒 Click for Additional Information
Case: **00668792** CRAOS8X-37225	**Summary:** "SORT" and "Tr" are no longer available in AOS 8.9. **Explanation:** The Sort and Tr commands are only available in the SU mode of an AOS8.X switch. In the AOS7X code, the command was available in CLI mode. 🔒 Click for Additional Information
CVEs: **CVE-2022-3786** CRAOS8X-36225	OpenSSL: version 3.0.7 to address CVE-2022-3786.

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 starting in 8.7R3. The package files are kept in the **flash/working/pkg** directory or can be downloaded from the Service & Support website.

Package	**Package Description**
MRP (mrp-v#.deb)	MRP Application
ams / ams-apps (ams-v#.deb/ams-apps-v#.deb)	AOS Micro Services Application
OVSDB (aos-ovsdb-v#.deb)	OVSDB Application
- If a package is not committed it can result in image validation errors when trying to reload the switch. - Some packages are included as part of the AOS release and do not have to be installed separately. - 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.