

Release Notes - Rev. D

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

Release 8.8R1

These release notes accompany release 8.8R1. These release notes provide important information on individual software features and hardware modules. Since much of the information in these release notes is not included in the hardware and software user manuals, it is important that you read all sections of this document before installing new hardware or loading new software.

Note: A new 8.8R1 GA build number (8.8.153.R01) is being released on some platforms to address a possible issue when upgrading to AOS Release 8.8R1. Please see [New 8.8R1 GA Release Build](#) for details and recommendations prior to upgrading.

Contents

Contents 2

Related Documentation 3

System Requirements 4

[IMPORTANT] *MUST READ*: AOS Release 8.8R1 Prerequisites and Deployment Information 10

Licensed Features 13

ALE Secure Diversified Code 14

New / Updated Hardware Support and Guidelines 15

New Software Features and Enhancements 17

Open Problem Reports and Feature Exceptions 26

Hot-Swap/Redundancy Feature Guidelines 28

Technical Support 31

Appendix A: Feature Matrix 33

Appendix B: MACsec Platform Support 42

Appendix C: SPB L3 VPN-Lite Service-based (Inline Routing) / External Loopback Support / BVLAN Guidelines 43

Appendix D: General Upgrade Requirements and Best Practices 46

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

Appendix F: ISSU - OmniSwitch Chassis or Virtual Chassis 53

Appendix G: FPGA / U-boot Upgrade Procedure 56

Appendix H: Fixed Problem Reports 59

Appendix I: Installing/Removing Packages 69

Related Documentation

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

- OmniSwitch 6360 Hardware User Guide
- OmniSwitch 6465 Hardware User Guide
- OmniSwitch 6900 Hardware User Guide
- OmniSwitch 6560 Hardware User Guide
- OmniSwitch 6860 Hardware User Guide
- OmniSwitch 6865 Hardware User Guide
- OmniSwitch 9900 Hardware User Guide
- OmniSwitch AOS Release 8 CLI Reference Guide
- OmniSwitch AOS Release 8 Network Configuration Guide
- OmniSwitch AOS Release 8 Switch Management Guide
- OmniSwitch AOS Release 8 Advanced Routing Configuration Guide
- OmniSwitch AOS Release 8 Data Center Switching Guide
- OmniSwitch AOS Release 8 Specifications Guide
- OmniSwitch AOS Release 8 Transceivers Guide

System Requirements

Memory Requirements

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

Platform	SDRAM	Flash
OS6360	1GB	1GB
OS6465	1GB	1GB
OS6560	2GB	2GB
OS6560-24X4/P24X4	1GB	1GB
OS6860(E)	2GB	2GB
OS6860N	4GB	32GB
OS6865	2GB	2GB
OS6900-X Models	2GB	2GB
OS6900-T Models	4GB	2GB
OS6900-Q32	8GB	2GB
OS6900-X72	8GB	4GB
OS6900-V72/C32	16GB	16GB
OS6900-C32E	8GB	64GB
OS6900-X48C6/T48C6/X48C4E	8GB	32GB
OS9900	16GB	2GB

U-Boot and FPGA Requirements

The software versions listed below are the MINIMUM required, except where otherwise noted. Switches running the minimum versions, as listed below, do not require any U-Boot or FPGA upgrades but it's recommended to upgrade to the current 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 8.8.152R01 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6360-10	8.7.149.R02	8.7.30.R03 ²	0.11	0.11
OS6360-P10	8.7.149.R02	8.7.30.R03 ²	0.11	0.11
OS6360-24	8.7.149.R02	8.7.30.R03 ²	0.15	0.17 ¹
OS6360-P24	8.7.149.R02	8.7.30.R03 ²	0.15	0.17 ¹

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6360-P24X	8.7.149.R02	8.7.30.R03 ²	0.12	0.12
OS6360-PH24	8.7.149.R02	8.7.30.R03 ²	0.12	0.12
OS6360-48	8.7.149.R02	8.7.30.R03 ²	0.15	0.17 ¹
OS6360-P48	8.7.149.R02	8.7.30.R03 ²	0.15	0.17 ¹
OS6360-P48X	8.7.149.R02	8.7.30.R03 ²	0.12	0.12

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

OmniSwitch 6465 - AOS Release 8.8.152.R01 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6465-P6	8.5.83.R01	8.7.2.R02 ² 8.7.30.R03 ³ 8.8.33.R01 ⁴	0.10	0.10
OS6465-P12	8.5.83.R01	8.7.2.R02 ² 8.7.30.R03 ³ 8.8.33.R01 ⁴	0.10	0.10
OS6465-P28	8.5.89.R02	8.7.2.R02 ² 8.7.30.R03 ³ 8.8.33.R01 ⁴	0.5	0.7 ¹
OS6465T-12	8.6.117.R01	8.7.2.R02 ² 8.7.30.R03 ³ 8.8.33.R01 ⁴	0.4	0.4
OS6465T-P12	8.6.117.R01	8.7.2.R02 ² 8.7.30.R03 ³ 8.8.33.R01 ⁴	0.4	0.4
OS6465-P12 (ENH-240)	8.8.33.R01	8.8.33.R01	0.5	0.5

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

OmniSwitch 6560 - AOS Release 8.8.152.R01 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6560-24Z24	8.5.22.R01	8.7.2.R02 ³ 8.7.30.R03 ⁷	0.7	0.8 ⁵
OS6560-P24Z24	8.4.1.23.R02	8.7.2.R02 ³ 8.7.30.R03 ⁷	0.6	0.7 ¹ 0.8 ⁵
OS6560-24Z8	8.5.22.R01	8.7.2.R02 ³ 8.7.30.R03 ⁷	0.7	0.8 ⁵

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6560-P24Z8	8.4.1.23.R02	8.7.2.R02 ³ 8.7.30.R03 ⁷	0.6	0.7 ¹ 0.8 ⁵
OS6560-24X4	8.5.89.R02	8.7.2.R02 ⁴ 8.7.30.R03 ⁷	0.4	0.4
OS6560-P24X4	8.5.89.R02	8.7.2.R02 ⁴ 8.7.30.R03 ⁷	0.4	0.4
OS6560-P48Z16 (903954-90)	8.4.1.23.R02	8.7.2.R02 ³ 8.7.30.R03 ⁷	0.6	0.7 ¹ 0.8 ⁵
OS6560-P48Z16 (all other PNs)	8.5.97.R04	8.7.2.R02 ³ 8.7.30.R03 ⁷	0.3	0.6 ² 0.7 ⁶
OS6560-48X4	8.5.97.R04	8.7.2.R02 ⁴ 8.7.30.R03 ⁷	0.4	0.7 ² 0.8 ⁶
OS6560-P48X4	8.5.97.R04	8.7.2.R02 ⁴ 8.7.30.R03 ⁷	0.4	0.7 ² 0.8 ⁶
OS6560-X10	8.5.97.R04	8.7.2.R02 ⁴ 8.7.30.R03 ⁷	0.5	0.8 ²

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

OmniSwitch 6860(E) - AOS Release 8.8.152.R01 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6860/OS6860E (except U28/P24Z8)	8.1.1.70.R01	8.7.30.R03 ²	0.9	0.10 ¹
OS6860E-U28	8.1.1.70.R01	8.7.30.R03 ²	0.2	0.2
OS6860E-P24Z8	8.4.1.17.R01	8.7.30.R03 ²	0.5	0.7 ¹

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 8.8.153.R01 (GA)

Hardware	Minimum ONIE	Current ONIE	Minimum FPGA	Current FPGA
OS6860N-U28	2019.05.00.10	2019.05.00.10	12	12
OS6860N-P48Z			12	12
OS6860N-P48M			11	11
O6860N-P24M	2019.05.00.11	2019.05.00.11	2	2

Hardware	Minimum ONIE	Current ONIE	Minimum FPGA	Current FPGA
OS6860N-P24Z	2019.05.00.11	2019.05.00.11	2	2
Note: These models use the Uosn.img image file.				

OmniSwitch 6865 - AOS Release 8.8.152.R01 (GA)

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

OmniSwitch 6900-X20/X40 - AOS Release 8.8.152.R01 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
CMM (if XNI-U12E support is not needed)	7.2.1.266.R02	8.7.30.R03 ¹	1.3.0/1.2.0	1.3.0/2.2.0
CMM (if XNI-U12E support is needed)	7.2.1.266.R02	8.7.30.R03 ¹	1.3.0/2.2.0	1.3.0/2.2.0
1. Optional uboot update for CRAOS8X-24464, ability to disable/authenticate uboot access.				

OmniSwitch 6900-T20/T40 - AOS Release 8.8.152.R01 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
CMM (if XNI-U12E support is not needed)	7.3.2.134.R01	8.7.30.R03 ¹	1.4.0/0.0.0	1.6.0/0.0.0
CMM (if XNI-U12E support is needed)	7.3.2.134.R01	8.7.30.R03 ¹	1.6.0/0.0.0	1.6.0/0.0.0
1. Optional uboot update for CRAOS8X-24464, ability to disable/authenticate uboot access.				

OmniSwitch 6900-Q32 - AOS Release 8.8.152.R01 (GA)

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

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

OmniSwitch 6900-X72 - AOS Release 8.8.152.R01 (GA)

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

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

OmniSwitch 6900-V72/C32/C32E - AOS Release 8.8.153.R01 (GA)

Hardware	Minimum ONIE	Current ONIE	Minimum CPLD	Current CPLD
OS6900-V72	2017.08.00.01	2017.08.00.01	CPLD 1 - 0x5 CPLD 2 - 0x6 CPLD 3 - 0x8	CPLD 1 - 0x5 CPLD 2 - 0x6 CPLD 3 - 0x8
OS6900-C32	2016.08.00.03	2018.11.00.02	CPLD 1 - 0xA CPLD 2 - 0xB CPLD 3 - 0xB	CPLD 1 - 0xA CPLD 2 - 0xB CPLD 3 - 0xB
OS6900-C32E	2020.02.00.01	2020.02.00.01	CPLD 1 - 0xD CPLD 2 - 0x9 CPLD 3 - 0x9	CPLD 1 - 0xD CPLD 2 - 0x9 CPLD 3 - 0x9

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

OmniSwitch 6900-X48C6/T48C6/X48C4E/V48C8- AOS Release 8.8.153.R01 (GA)

Hardware	Minimum ONIE	Current ONIE	Minimum CPLD	Current CPLD
OS6900-X48C6	2019.08.00.01	2019.08.00.01	CPLD 1 - 0x2 CPLD 2 - 0x2 CPLD 3 - 0x2	CPLD 1 - 0x2 CPLD 2 - 0x2 CPLD 3 - 0x2
OS6900-T48C6	2019.08.00.01	2019.08.00.01	CPLD 1 - 0x2 CPLD 2 - 0x2 CPLD 3 - 0x4	CPLD 1 - 0x2 CPLD 2 - 0x2 CPLD 3 - 0x4
OS6900-X48C4E	2019.05.00.10	2019.05.00.10	CPLD 1 - 0x3 CPLD 2 - 0x2 CPLD 3 - 0x3	CPLD 1 - 0x3 CPLD 2 - 0x2 CPLD 3 - 0x3
OS6900-V48C8	2020.02.00.01	2020.02.00.01	CPLD 1 - 0x2 CPLD 2 - 0x3 CPLD 3 - 0x2	CPLD 1 - 0x2 CPLD 2 - 0x3 CPLD 3 - 0x2

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

OmniSwitch 9900 - AOS Release 8.8.152.R01 (GA)

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

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

[IMPORTANT] *MUST READ*: AOS Release 8.8R1 Prerequisites and Deployment Information

General Information

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

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

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

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

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

Note: OS6560-P48Z16 (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 SFP, SFP+, QSFP+, and QSFP28 ports with fiber transceivers.

The following exceptions do not support faster convergence:

- Copper ports or ports with copper transceivers.
- OS6865-P16X and OS6865-U12X ports 3 and 4.
- VFL ports.
- Splitter ports (i.e. 4X10G or 4X25G).

- 25G uplink ports with 1G transceivers on the OS6860N, OS68-VNI-U4 expansion module, and ports 41-48 on the OS6900-X48C4E.
- **MACsec Licensing Requirement**
Beginning in 8.6R1 the MACsec feature requires a site license, this license can be generated free of cost. After upgrading, the feature will be disabled until a license is installed. There is no reboot required after applying the license.
- **SHA-1 Algorithm - Chosen-prefix attacks against the SHA-1 algorithm are becoming easier for an attacker¹.** For this reason, we will be disabling the "ssh-rsa" public key signature algorithm by default in an upcoming AOS release. The better alternatives include:
 - The RFC8332 RSA SHA-2 signature algorithms rsa-sha2-256/512. These algorithms have the advantage of using the same key type as "ssh-rsa" but use the safer SHA-2 hash algorithms. RSA SHA-2 is enabled in AOS.
 - The RFC5656 ECDSA algorithms: ecdsa-sha2-nistp256/384/521. These algorithms are supported in AOS by default.

To check whether a server is using the weak ssh-rsa public key algorithm, for host authentication, try to connect to it after disabling the ssh-rsa algorithm from ssh(1)'s allowed list using the command below:

```
-> ssh strong-hmacs enable
```

If the host key verification fails and no other supported host key types are available, the server software on that host should be upgraded.

1. "SHA-1 is a Shambles: First Chosen-Prefix Collision on SHA-1 and Application to the PGP Web of Trust" Laurent, G and Peyrin, T (2020) <https://eprint.iacr.org/2020/014.pdf>

- With the continuous goal of preserving the environment in addition to the AOS software being preloaded on the switch and available on the Business Portal, we have begun removing the software access card previously included in the switch ship kit. For additional information or if in need of special assistance, please contact Service & Support.

Deprecated Features / Functionality Changes

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

AOS Release 8.5R4
EVB - Beginning in 8.5R4, support for EVB is being removed. Any switches with an EVB configuration cannot be upgraded to 8.5R4 or above.
NTP - Beginning with AOS Release 8.5R4, OmniSwitches will not synchronize with an unsynchronized NTP server (stratum 16), as per the RFC standard. Existing installations where OmniSwitches are synchronizing from another OmniSwitch, or any other NTP server which is not synchronized with a valid NTP server, will not be able to synchronize their clocks. The following NTP commands have been deprecated: - ntp server synchronized - ntp server unsynchronized
AOS Release 8.6R1
DHCPv6 Guard - Configuration via an IPv6 interface name is deprecated in 8.6R1. Commands entered using the CLI must use the new 'ipv6 dhcp guard vlan vlan-id' format of the command. The old format will still be accepted if present in a vcboot.cfg to preserve backwards compatibility.
IP Helper - The 'ip helper' commands have been deprecated in 8.6R1 and replaced with 'ip dhcp relay'. The old format will still be accepted if present in a vcboot.cfg to preserve backwards compatibility.
SAA - The vlan-priority and drop-eligible parameters have been deprecated from all SAA commands beginning in 8.6R1.

MACsec is now supported on ports 33-48 of the 6560-(P)48X4. CRAOS8X-7910 was resolved in 8.6R1.
AOS Release 8.6R2
Distributed ARP - Beginning 8.6R2 distributed ARP is no longer supported.
WRED - Beginning in 8.6R2 WRED is no longer supported.
QoS - Beginning in 8.6R2 the 'qos dscp-table' command is no longer supported.
NTP - The ntp parameter for the 'ip service source-ip' command was deprecated in 8.5R4. Support has been added back in 8.6R2.
AOS Release 8.7R1
MACsec - Static mode is not supported on OS6860N.
Transceivers - Beginning in AOS release 8.7R1 an error message will be displayed when the unsupported QSFP-4X25G-C transceiver is inserted on an OS99-CNI-U8 module.
SPB - Beginning in 8.7.R01 the default number of BVLANS created via Auto Fabric is reduced from 16 to 4. This new default value is only applicable to factory default switches running 8.7R1 with no vcboot.cfg file. Upgrading to 8.7.R1 will not change the number of configured BVLANS in an existing configuration. See Appendix B for additional information.
AOS Release 8.7R2
There are new default user password polices being implemented in 8.7R2. This change does not affect existing users. <ul style="list-style-type: none"> - cannot-contain-username: enable - min-uppercase: 1 - min-lowercase: 1 - min-digit: 1 - min-nonalpha: 1
The OmniSwitch 6360 does not contain a real-time clock. <ul style="list-style-type: none"> - It is recommended to use NTP to ensure time synchronization on OS6360s. - When the switch is reset, the switch will boot up from an approximation of the last known good time. - When the switch is powered off it cannot detect the time left in the powered off state. When it boots up it will have the same time as when the switch was last powered off.
AOS Release 8.7R3
The Kerberos Snooping is not supported in bridge mode in this release.
AOS Release 8.8R1
Unsupported commands (Part of AOS 88R1 but not supported) <ul style="list-style-type: none"> - mrp interconnect - show mrp interconnect - clear mrp interconnect

New 8.8R1 GA Release Build to Address Possible EEPROM Issue

Description	There is a possibility for EEPROM corruption on certain devices when performing the initial upgrade to 8.8.152.R01. The issue has currently only been seen on a small number of OS6860N devices. Out of an abundance of caution 8.8.152.R01 will be replaced with 8.8.153.R01 in order to address the issue. This is only an upgrade issue and does not have any feature impact.
Platforms Affected	OS6860N, OS6900-V72/C32/C32E/X48C6/T48C6/X48C4E/V48C8 (No other platforms are affected and 8.8.152.R01 will remain the GA build)
Recommendation	For those that have not yet upgraded to 8.8R1 there is no issue, using build 8.8.153.R01 addresses the issue. For those that have upgraded to 8.8.152.R01 there is no issue for the platforms already upgraded. However, if a unit is introduced into a VC with an AOS release prior to 8.8R1 there is a chance of seeing the issue when the unit is automatically upgraded to 8.8.152.R01. Therefore it's recommended to upgrade to 8.8.153.R01 before incorporating any units into a VC. For those planning to upgrade to 8.8R1, please use 8.8.153.R01.

Licensed Features

The table below lists the CAPEX licensed features in this release and whether or not a license is required for the various models.

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

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

ALE Secure Diversified Code

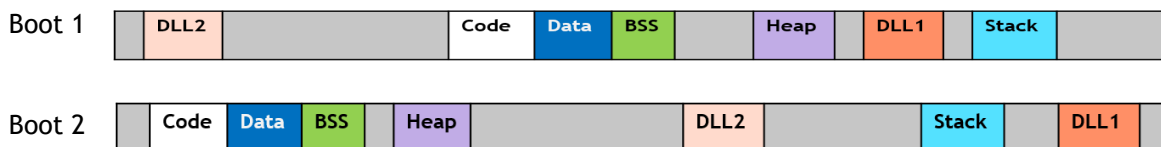
Alcatel-Lucent Enterprise provides network equipment that is hardened in conjunction with an independent 3rd party organization. ALE secure diversified code promotes security and assurance at the network device level using independent verification and validation of source code and software diversification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

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

Software Diversification

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

ASLR



Please contact customer support for additional information.

New / Updated Hardware Support and Guidelines

The following new hardware is being introduced in this release.

OS6900-C32E

Fixed configuration chassis in a 1U form factor with:

- Thirty-two (32) 40G/100G QSFP28 ports
- Two (2) 10G SFP+ ports (Not currently supported)
- USB port
- RJ-45 console port
- Front-to-rear or rear-to-front cooling
- AC or DC power supply
- Supports a VC of 6

OS6860N-P24Z

Fixed configuration chassis in a 1U form factor with:

- Twelve (12) 10/100/1000 Base-T 802.3bt PoE (60W) ports
- Twelve (12) 100M/1G/2.5G/5G Base-T 802.3bt PoE (95W) ports
- Two (2) QSFP28 VFL ports
- Four (4) SFP28 (1G/10G/25G) ports
- USB port
- RJ-45 console port
- EMP port
- 600W or 920W AC power supply

OS6860N-P24M

Fixed configuration chassis in a 1U form factor with:

- Twenty-four (24) 100M/1G/2.5G/5G/10G Base-T 802.3bt PoE (95W) ports
- Two (2) QSFP28 VFL ports
- One (1) uplink module slot
- USB port
- RJ-45 console port
- EMP port
- 600W, 920W, or 2000W AC power supply

OS6465-P12 (ENH-240)

Fixed configuration industrial chassis in a 1U form factor with a PoE budget up to 240W:

- Eight (8) - 10/100/1000 BaseT 802.3at PoE+ ports (Four ports support 60W HPOE)
- Four (4) - SFP 100/1000FX ports
- USB port
- RJ-45 console port
- Two (2) Alarm connectors (1-input, 1-output)

OS6465-BPN-X

Din-mountable, AC power supply providing both system and up to 240W of PoE power.

Note: *This power supply has not been submitted for validation to meet the industrial certification requirements.*

Transceivers

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

- **QSFP-100G-ER4** - 100-Gigabit optical transceiver (QSFP28). Supports link length of 40km over single-mode fiber. LC connector.

- **iSFP-10G-SR** - 10-Gigabit industrial optical transceiver (SFP+). Supports link length of 30m over single-mode fiber. LC connector.
- Break-out Support
 - OS6900-T48C6 (ports 51 and 54 only)
 - OS6900-X48C6 (ports 51 and 54 only)
 - OS6900-X48C4E (ports 49-52 only)
 - OS6900-V48C8 (ports 49-56 only)
 - OS6900-C32E (ports 1-32)
 - OS6860N
 - OS68-QNI-U2 (Both ports)
 - OS68-CNI-U1
- VFL links are not supported on break-out ports.
- Break-out cables cannot be auto-detected. If break-out cables are connected the break-out mode should explicitly enabled to prevent unexpected behavior such as remote link partners having a false link up.

The table below lists new and existing transceiver support added in this release. Please refer to the Transceivers and Hardware guides for additional information.

Product	Transceiver
OS6360	SFP-GIG-BX-D20/U20/D40/U40, SFP-10G-T, SFP-10G-GIG-SR, SFP-10G-GIG-LR, 3FE46541AA (G-010S-A, GPON SFP ONT, 1xGE UNI)
OS6465	iSFP-10G-SR
OS6860N	SFP-DUAL-MM-N, SFP-DUAL-BX-D/U, QSFP-100G-ER4
OS6865	iSFP-10G-SR
OS6900	QSFP-100G-ER4
OS9900	QSFP-100G-ER4

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.

8.8R1 New Feature/Enhancements Summary

Feature	Platform
Management Features	
Console Log Redirection	All
DHCP options 2 and 12	All
Increase Authentication Server Down Re-Auth Time	All
Thin Client OmniSwitch	All
AMS Controller Redundancy	6360, 6465, 6560
Hitless Upgrade for IP Services	All
Remote NI Syslog on OS9900 (UDP/TLS)	OS9900
Allow miniboot shell access after authenticating with password. Allow user to modify this password.	6360, 6465, 6560, 6860(E), 6865, 6900 (without ONIE), 9900
Increasing re-authentication session timer from 5 mins done through TACACS+	All
USB backup improvement and Boot from USB and/or external flash	6465, 6865
Microservice Marketplace	All
WebView Refresh and Localization (French)	All
NaaS 2.0 (licensing enforcement)	All
QoS Features	
QoS on VFL Links	OS6900-X72
Introduction to Statistical Jitter	All
Service Features	
DPI over SPB	6860N
Hybrid NNI mode with VLAN Stacking and 802.1Q vlans on the same NNI port	All
OAM PDU Support for EVC MEF OAM on per- CVLAN\SVLAN basis	6465, 6865
Support for additional tag-values under unp-profile mapped to services (spb/vxlan/l2gre)	6860, 6860N, 6865, 6900 (all models) 9900
LPS over SPB	6860, 6860N, 6865, 6900 (all models) 9900
ERP - SPB Interworking for convergence	6860, 6860N, 6900 (all), 9900
Other	
MTU Handling of VXLAN Tunneled Traffic	6900, 6900-V72/C32
NIS enhancements/certifications	6560, 6860
MRP	6865
DHCPv6 guard configuration using VLAN range option	6360, 6860, 6860N, 6865, 6900 (all), 9900
Increase ARP table to 2048 for OS6560	6560
Parity Features	

Feature	Platform
VXLAN	6860N, 6900-X48C6/T48C6/X48C4E/V48C8/C32E
OSPFv3 6560	6560
Automatic Fabric	6860N
HAVLAN	6860N
Private VLANs	6860N

Management / NMS Related Features

Console Log Redirection

This functionality enables uploading of the console log(s) to the remote UDP syslog server. By default, uploading the console log to a remote syslog server is disabled. Logs will continue to be displayed on the console when this feature is enabled.

However, to enable uploading of console logs to a remote syslog server, it is mandatory to have at least one remote syslog server is configured. If there is no UDP remote syslog server configured, an error message will be displayed.

The following CLI commands are associated with this feature:

- **swlog output socket console enable**
- **show swlog**

DHCP Options 2 and 12

The time zone and the system name of the OmniSwitch is set according to the time zone (DHCP Option-2) and system name (DHCP Option-12) assigned by the DHCP server. DHCP server sets the Option-2 and Option-12 values only when they are set to their default values or they are already set by the DHCP. Once the user configures these values to non-default values, DHCP does not set them. This was an EA feature in 8.7R2.

The automatic setting of the time zone from DHCP option 2 and 12 is supported through DHCP client IP interface.

The following CLI commands are associated with this feature:

- The **show system** command shows the current time zone and current system name that is effective.
- The **show ip interface dhcp-client** output is enhanced to reflect the time zone obtained through option 2 and option 12.

Increase Authentication Server Down Re-Auth Time

The authentication server down timer range is increased to 43200 seconds from 1000 seconds.

The following CLI commands are associated with this feature:

- **unp auth-server-down-timeout *seconds***

Thin Client OmniSwitch

OmniSwitch can function as a thin client in a network. In this mode no configuration can be saved in the "Running" directory of the switch. Only the vcboot.cfg with minimal network reachability configuration is stored on the switch running directory. This mode prevents the sensitive information stored in the configuration from being tracked and enhances the switch security.

The OmniSwitch as thin client mode is configured through the activation process from the OmniVista cloud. A switch is provisioned as a ThinSwitch on the OmniVista server and the configuration is pushed to the device during the call-home process.

The activation will work with or without a DHCP server in the network. If the network is not configured with the DHCP server, the minimal network configuration for reachability to DNS server, NTP server and OVE must be configured on the OmniSwitch thin client using the CLI and saved in the vcboot.cfg file.

The following CLI commands are associated with this feature:

- No new CLI

AMS Controller Redundancy

OmniSwitch now supports broker redundancy across two separate systems. It uses the VRRP protocol to handle the broker failover. AMS redundancy consist of two switches running the VRRP protocol to interact and sync with each other to take over whenever the active broker fails.

AMS redundancy can be configured two ways:

- Manual Configuration
- Via DHCP VSO

The AMS client is configured with active broker IP address. When connectivity with the active broker is lost, it automatically reconnects with the new active broker using the same IP address.

The following CLI commands are associated with this feature:

- No new CLI

Hitless Upgrade for IP Services

The OmniSwitch package manager now includes SNMP upgrade and OpenSSH patch update. The SNMP upgrade install and removal does not require switch reboot. The Open SSH patch install and removal requires switch reboot for OS6560, OS6465 and OS6360.

The following CLI commands are associated with this feature:

- No new CLI

Remote NI Syslog on OS9900

On an OS9900 only the syslog from the CMM is transferred by the remote syslog. The NI and HOST syslog are not transferred to the remote syslog server. In 8.8R1 the syslog on NI and HOST can be configured to send their logs to the CMM. On receiving the logs, the CMM will forward the logs to the external server. The configuration is applicable only for UDP remote syslog servers.

The following CLI commands are associated with this feature:

- `swlog host output socket {enable | diable}`
- `swlog ni slot <chassis/slot> output socket {enable | disable}`
- `show swlog`

Miniboot Shell Access with Authentication

The AOS bootloader (uboot) provides access to system parameters, with which boot images and system variables can be manipulated by any user having physical/console access to the switch, which can cause security related issues. With this feature, an option is provided to disable access to uboot shell. When the option is disabled, any keypress at AOS boot does not allow access to the uboot shell. AOS images are booted with the pre-set parameters. When the Uboot access is enabled, Uboot shell can be accessed with any key-press at AOS boot.

U-boot Access Recovery: When the U-boot access is disabled, any key-press at AOS boot does not allow access to U-boot shell. AOS images are booted with the pre-set parameters. If the AOS images are not valid or corrupted, switch goes to no response state, where only watch-dog reboots are possible. U-boot cannot start AOS and recover options cannot be used, as these options need U-boot access. In this case, the switch must be returned to the factory for repair as it cannot be recovered by the admin user.

The OmniSwitch allows for securing the Uboot with the Uboot password authentication. When Uboot authentication is enabled the Uboot shell can be accessed only after authenticating with the password. The password authentication is not enabled by default. It needs to be enabled by the administrator.

Uboot Password Recovery: The Uboot password cannot be modified at the Uboot prompt. Only the admin user can modify or set the password using the Uboot authentication command. If the user forgets the password, user can continue to normal AOS boot. The admin user can then modify or reset the Uboot password. If the flash is corrupt and Uboot fails to start AOS with the password enabled and the password is forgotten, the switch must be returned to the factory for repair.

The following CLI commands are associated with this feature:

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

Increase Re-authentication Session Timer Through TACACS+

The switch can now be configured for reauthentication for all the TACACS+ sessions by setting the timeout interval for reauthentication.

The following CLI commands are associated with this feature:

- **session reauthentication**
- **show session config**

USB backup Improvements and Boot from USB and/or External Flash

This is an enhancement to the USB backup functionality that will copy all necessary files to the backup location to allow the switch to boot from the backup. At boot-up, if boot loader detects a USB connected with a specific signature file and an AOS image, it will attempt to boot AOS from the USB. If not the switch shall continue to boot from flash.

The following CLI commands are associated with this feature:

- **usb backup bootable**

Microservice Marketplace

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

The following “pkgmgr” CLI commands are changed:

- **pkgmgr/appmgr commit** is changed to **write memory**
- **pkgmgr list** is changed to **show pkgmgr**
- **appmgr start** has new **argument** keyword.
- **appmgr list** is replaced by **show appmgr**

WebView Refresh and Localization

WebView is now available in French.

The following CLI commands are associated with this feature:

- **No new CLI**

Network as a Service 2.0 - License Enforcement

Network as a Service is an innovative subscription model for network solutions. Organizations can now purchase network infrastructure like hardware, licenses, applications, management tools and managed services through subscriptions as opposed to perpetual contracts. Network infrastructure can be deployed quickly and scaled instantly according to their business needs.

OmniSwitch now supports NaaS by providing "Connectivity as a Service" for all LAN switches for which it must have NaaS connectivity license and connectivity to ALE License Activation Server.

OmniSwitch provides the following license models:

- Node Locked Permanent/Perpetual License: this license is locked to the serial number of the switch and is permanent.
- Node Locked Subscription License: this license is locked to the serial number of the switch with a start and end date for license validity.

The following CLI commands are associated with this feature:

- **naas license call-home interval**
- **naas license call-home interval now**
- **naas license apply file**
- **show naas-agent status**
- **show naas license.**

Qos Features

QoS on VFL Links

QSP profile 5 is supported on VFL Links on the OS6900-X72.

Introduction to Statistical Jitter

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

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

The following CLI commands are associated with this feature:

- **saa jitter-calculation enhanced**
- **show saa**

Service Features

DPI over Services

This feature provides AppMon support on Service access ports as well as Service network ports on the OmniSwitch 6860N platforms.

The following CLI commands are associated with this feature:

- No new CLI

Hybrid NNI Mode with VLAN Stacking and 802.1Q VLANs on the same NNI Port

Any standard (non-service) VLAN can now be assigned to NNI ports as the default VLAN (untagged) or as an 802.1Q tagged VLAN. This allows customers to configure 802.1q services, QinQ service, and untagged services using the same uplink NNI port.

There is no new CLI to support this feature, but the NNI port can be configured as Untagged or tagged port of a VLAN using the existing `vlan members port | linkagg untagged` and `vlan members port | linkagg tagged` commands. Similarly, it is now allowed to configure an interface configured with standard VLAN and 802.1q VLAN as NNI port using the following CLI:

- **ethernet-service svlan <vlanid> NNI <port <chassis/slot/port-port> | linkagg <linkagg-linkagg**

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

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

The following CLI commands are associated with this feature:

- **cvlan** parameter added to **ethoam endpoint domain association** command.
- **ethoam endpoint ctag-priority**, **ethoam association allowed-cvlan-list** introduced.

Support for Additional Tag-values Under Unp-profile Mapped to Services (SPB/VXLAN/L2GRE)

Currently UNP allows the following tag-values to be configured on an UNP-Profile mapped to services (SPB/VXLAN/L2GRE). These tag values can be used to dynamically create a SAP when a UNP profile is mapped to a service.

- 0 (untagged),
- <vid> (single-tag),
- <vid>:<vid> (double-tag)

As part of this enhancement the following tag-values are allowed to be configured on a UNP profile mapped to a service:

- "all" (catch all - any single/double-tag)
- "<vid>:all" (outer-vid + any inner-vid)

The following CLI commands are associated with this feature:

- **unp profile map service-type tag-value [all, vid:all].**

LPS Over SPB

This enhancement allows LPS support to be extended to the service domain. LPS is supported both on Static and Dynamic SAP ports mapped to SPB services.

The following CLI commands are associated with this feature:

- **port-security sap {port | linkagg} sap**
- **show port-security sap**

ERP-SPB Interworking for Convergence

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

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

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

The following CLI commands are associated with this feature:

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

Additional Features

MTU Handling of VxLAN Tunneled Traffic

When overlay network traffic is tunneled using VxLAN the encapsulated traffic could be dropped by the service provide network if the tunneled traffic exceeds the MTU size supported by the service provider tunnel. The OmniSwitch allows the TCP Maximum Segment Size (MSS) carried in the TCP SYN/SYN-ACK frames to be configured to a value supported by the tunnel. A value in range defined below or a default size profile of sbp (1380) or ethernet (1402) can be configured.

The following CLI commands are associated with this feature:

- **service *service-id* sap {port | linkagg } tcp-mss {500-1410 | overlay-profile {spb | ethernet }}**
- **show service *service-id* sap tcp-mss**

NIS Enhancements and Certifications

As part of the NIS enhancements the OmniSwitch is pre-configured with a secured user called “secureadmin”. The **secureadmin** user login automatically enables the enhanced mode and disables the **admin** user. All the IP services are disabled by default. The required IP services must be enabled manually by the secureadmin user. The services like Telnet, SSH, FTP, SFTP, HTTP/HTTPs, Radius, SNMP, NTP will be part of the software integrity check. The software integrity check is performed on reload. The critical CLIs such as cp, mkdir, mv, rm, vi, grep, more, cat, less, head, tail and su is available only through console session.

The **secureadmin** user can set a super password to allow other users to operate in config mode. The super password can be set by the **secureadmin** by using the **enable super-password** command.

The following CLI commands are associated with this feature:

- **enable super-password**

MRP

- On OS6465 MRP is only supported on standalone or VC of 1 for release 8.8.R1.
- On OS6865 MRP is supported on VC of 1 or more.

DHCPv6 Guard Configuration using VLAN Range Option

Supports DHCPv6 guard VLAN range and trusted port/linkagg range configuration. EA feature in 8.7R2.

The following CLI commands are associated with this feature:

- ipv6 dhcp guard vlan
- ipv6 dhcp guard vlan trusted

Increase ARP Table to 2048 for OS6560

The OS6560 now supports 2048 ARP entries.

The following CLI commands are associated with this feature:

- No new CLI

Parity Features

VXLAN

VXLAN gateway functionality is now supported on the OS6860N and 6900-X48C6/T48C6/V48C8/X48C4E/C32E models.

Note: The following Access Guardian features over VXLAN tunnel are EA only features.

- LPS
- Kerberos-snooping
- LTP (UNP Location/Time Policy)
- UDR (UNP user defined roles)

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-30510	After disabling break-out mode and reloading an NI in a VC, the ‘show interfaces slot’ command still displays the port with break-out ports.	This is a display issue and has no functional impact. Use the ‘show interface <chassis/slot/port> status’ or ‘show interface status’ commands.
CRAOS8X-26502	While converging due to a link/node failure in a MRP ring network, sometimes a few multicast IGMP clients are not relearned with a large number of multicast streams (>200). Clients will be relearned after the next query interval.	There is no known workaround at this time.
CRAOS8X-30411	In ‘show configuration snapshot’ some ports may show up as autoneg disabled, even though its the default configuration of the port.	There is no functional impact.
CRAOS8X-27368	On an OS9900 when linkagg port is admin disabled, fdb flush is issued for that particular port which is resulting in flushing MACs on other fixed port which is unrelated to the linkagg.	There is no known workaround at this time.
CRAOS8X-23137	When high number of VLANs are mapped to DHL links, during failover there may be some traffic loss due to delay in hardware programming.	There is no known workaround at this time.
CRAOS8X-10059	Toggling admin state of bulk of VLANs (disable/enable) very quickly may cause VPA state of the VLANs to be incorrectly stuck in blocking state (instead of forwarding).	Allow a few seconds in between toggling admin state (disable/enable) of bulk of VLANs.

Hardware / Transceivers

CR	Description	Workaround
CRAOS8X-29371	A link UP delay of 3-4 seconds is seen with the XNI-U48 module when the link between OS99-XNI-U48 and Nokia OLT flaps. The XNI-U48 takes more than 3 seconds to bring the link UP operationally. This link UP delay is also seen when the direct loopback is tested in XNI-U48. This also affects the failover when a Y cable is connected between OS99-XNI-U48 and Nokia OLT. The failover fails on Nokia EMS as Working and Protection port status is not changed automatically.	There is no known workaround at this time.
CRAOS8X-30583	The SFP-10G-T supports both 1G and 10G speeds only on the OS6900-X48C6, OS6900-V48C8, OS6900-	Manually configure the speed to 1G for the

	X48C4E and OS6860N (25G ports only). All other 8.X models support 10G speed only.	platforms that support it when using the SFP-10G-T at 1G speed.
CRAOS8X-31887	On some OmniSwitch models, disabling lanpower on an individual port (lanpower port chassis/slot/port admin-state disable) only works temporarily. The power will initially be disabled but will then be re-enabled after approximately 20 seconds. The following platforms are affected: OS6360-P24/P48, OS6465, OS6560, OS6860/E, OS6865, and OS9900. The OS6360 and OS6860N models are not affected.	Enable "capacitance-detection" on the port prior to disabling lanpower on the port. For example: -> lanpower port 1/1/23 capacitor-detection enable -> lanpower port 1/1/23 admin-state disable

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>'. 'interfaces port c/s/p ingress-bandwidth mbps <num> burst <num>'.

Service Related

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

Virtual Chassis

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

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 insertions and extractions must have a 30 second interval before initiating another hot-swap activity. CMM module extractions should have between a 15 and 20 minute interval.
- All new module insertions must have a 5 minute interval AND the LEDs (OK, PRI, VC, NI) have returned to their normal operating state.

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

OS6860N-P48M Hot-Swap/Insertion Compatibility

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

OS6900 Hot-Swap/Insertion Compatibility

Existing Slot	Hot-Swap/Hot-Insert compatibility
Empty	All modules can be inserted
OS99-CMM	OS99-CMM
OS9907-CFM	OS9907-CFM
OS99-GNI-48	OS99-GNI-48

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

OS9900 Hot-Swap/Insertion Compatibility

Hot-Swap Procedure

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

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

VC Hot-Swap / Removal Guidelines

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

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

Fast/Perpetual PoE Unlike Power Supply Swapping

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

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

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

Technical Support

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

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

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

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

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

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

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

Third Party Licenses and Notices

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

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

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

libatomic	: 1.0.0	: GPLv3+ & GPLv3+ with exceptions & GPLv2+ with exceptions & LGPLv2+ & BSD	: /flash/foss/gpl-3.0.txt + /flash/foss/gpl-2.0.txt + /flash/foss/lgpl-2.1.txt + /flash/foss/bsd1.txt
openvswitch	: 2.12.0	: Apache License 2.0	: /flash/foss/Apache-License-2.0.txt

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

Appendix A: Feature Matrix

The following is a feature matrix for AOS Release 8.8R1.

Note: Early availability features are available in AOS and can be configured. However, they have not gone through the complete AOS validation cycle and are therefore not officially supported.

Feature	6360	6465	6560	6860(E)	6860N	6865	6900	6900- V72/ C32	6900- X48C6/ T48C6/X48C4E/V48C8/C32E	9900
Management Features										
AOS Micro Services (AMS)	8.7R2	8.6R1	8.6R1	8.6R1	8.7R1	8.6R1	8.6R1	8.6R1	8.7R1	8.6R1
Automatic Remote Configuration Download (RCL)	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.6R2	8.7R1	Y
Automatic/Intelligent Fabric	8.7R2	8.5R1	Y	Y	8.7R2	Y	Y	Y	Y	Y
Automatic VC	8.7R2	N	Y	Y	8.7R1	Y	Y	8.6R2	8.7R1	N
Bluetooth - USB Adapter with Bluetooth Technology	8.7R2	8.6R2	8.6R2	Y	8.7R1	8.6R2	8.7R1	8.6R2	N	N
Console Disable	8.7R2	8.6R2	8.6R2	8.6R2	8.7R1	8.6R2	8.6R2	8.6R2	8.7R1	8.6R2
Dying Gasp	N	Y	Y	Y	8.7R1	Y	N	N	N	N
Dying Gasp (EFM OAM / Link OAM)	N	8.6R1	8.6R1	8.6R1	8.7R1	8.6R1	N	N	N	N
EEE support	Y	N	N	Y	8.7R1	Y	Y	N	N	N
Embedded Python Scripting / Event Manager	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.7R2	8.7R2	N
IP Managed Services	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Hitless Security Patch Upgrade	8.7R2	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1
In-Band Management over SPB	N	N	N	8.5R4	8.7R1	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4
ISSU	8.7R2	Y	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
NaaS	8.8R1	8.8R1	8.8R1	8.8R1	8.8R1	8.8R1	8.8R1	8.8R1	8.8R1	8.8R1
NAPALM Support	8.7R2	8.5R1	8.5R1	8.5R1	8.7R1	8.5R1	8.5R1	8.7R2	8.7R2	N
NTP - Version 4.2.8.p11.	8.7R2	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4
NTP - IPv6	8.7R3	8.7R3	8.7R3	8.7R3	8.7R3	8.7R3	8.7R3	8.7R3	8.7R3	8.7R3
OpenFlow	N	N	N	Y	N	N	Y	N	N	N
OV Cirrus - Zero touch provisioning	8.7R2	Y	Y	Y	8.7R1	Y	Y	8.7R2	8.7R2	N
OV Cirrus - Configurable NAS Address	8.7R2	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4
OV Cirrus - Default Admin Password Change	8.7R2	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4

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

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

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

Feature	6360	6465	6560	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E	9900
Switch logging / Syslog	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
TDR	N	N	N	Y	N	Y	N	N	N	N
Layer 2 Feature Support										
802.1q	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
DHL	8.7R2	8.5R1	Y	Y	8.7R1	Y	N	N	N	N
ERP v2	N	8.5R1	8.5R2	Y	8.7R1	Y	Y	8.7R1	8.7R1	8.5R3
HAVLAN	N	EA	N	Y	8.8R1	Y	Y	8.6R2	8.7R1	EA
Link Aggregation (static and LACP)	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
LLDP (802.1ab)	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Loopback detection - Edge (Bridge)	8.7R2	8.5R1	Y	Y	8.7R1	Y	N	8.6R2	8.7R1	Y
Loopback detection - SAP (Access)	N	N	N	Y	8.7R1	Y	Y	8.6R2	8.7R1	Y
MAC Forced Forwarding / Dynamic Proxy ARP	8.7R2	8.7R1	N	8.6R1	N	8.6R1	N	N	N	N
MRP	N	8.7R2	N	N	N	8.7R2	N	N	N	N
Port mapping	8.7R2	Y	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	N
Private VLANs (PVLAN)	N	N	N	Y	8.7R2	Y	Y	N	8.7R2	N
SIP Snooping	N	N	N	Y	N	N	N	N	N	N
Spanning Tree (1X1, RSTP, MSTP)	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Spanning Tree (PVST+, Loop Guard)	N	Y	N	Y	Y	Y	Y	Y	Y	Y
MVRP	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R4	8.7R1	Y
SPB ²	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
SPB - Over Shared Ethernet	N	N	N	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1
SPB - HW-based LSP flooding	N	N	N	N	N	N	N	N	N	8.5R4
QoS Feature Support										
802.1p / DSCP priority mapping	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
IPv4	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
IPv6	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y

Feature	6360	6465	6560	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E	9900
Auto-Qos prioritization of NMS/IP Phone Traffic	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Auto-Qos - New MAC range	8.7R2	8.5R2	8.5R2	8.5R2	8.7R1	8.5R2	8.5R2	8.5R2	8.7R1	8.5R2
Groups - Port	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Groups - MAC	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Groups - Network	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Groups - Service	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Groups - Map	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Groups - Switch	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Ingress/Egress bandwidth limit	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
Per port rate limiting	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	N
Policy Lists	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.7R1	8.7R1	Y
Policy Lists - Egress	N	N	N	Y	8.7R1	Y	Y	8.7R1	8.7R1	N
Policy based routing	N	N	N	Y	8.7R1	Y	Y	8.6R2	8.7R1	EA
Tri-color marking	N	N	N	Y	8.7R1	Y	Y	N	N	N
QSP Profiles 1	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
QSP Profiles 2/3/4	N	N	N	Y	QSP-2 only	Y	Y	QSP-2 only	QSP-2 only	N
QSP Profiles 5	8.7R2	8.5R1	Y	8.7R1	8.7R1	8.7R1	8.7R1 (X72)	N	N	Y
Custom QSP Profiles	8.7R2	Y	Y	Y	Y	Y	X72 only (EA)	Y	Y	Y
GOOSE Messaging Prioritization	N	8.7R1	N	N	N	8.7R1	N	N	N	N
Metro Ethernet Features										
CPE Test Head	N	8.6R1	N	N	N	N	N	N	N	N
Ethernet Loopback Test	N	N	N	8.6R1	8.7R1	8.6R1	N	N	N	N
Ethernet Services (VLAN Stacking)	N	8.5R1	8.8R1	Y	8.7R2	Y	Y	8.5R4	8.7R1	N
Ethernet OAM (ITU Y1731 and 802.1ag)	N	8.5R1	N	Y	8.7R1	Y	Y	8.7R1	8.7R1	EA
EFM OAM / Link OAM (802.3ah)	N	8.6R1	8.6R1	8.5R4	8.7R2	8.5R4	N	N	N	N

Feature	6360	6465	6560	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E	9900
PPPoE Intermediate Agent	N	8.6R1	N	N	N	8.6R1	N	N	N	N
1588v2 End-to-End Transparent Clock	N	8.5R1	8.7R2	Y	N	Y	Y (X72/Q32)	N	N	N
1588v2 Peer-to-Peer Transparent Clock	N	N	8.7R2	N	N	N	N	N	N	N
1588v2 Across VC	N	N	N	N	N	N	8.5R2 (X72)	N	N	N
Access Guardian / Security Features										
802.1x Authentication	8.7R2	8.5R2	Y	Y	8.7R1	Y	Y	8.7R1	8.7R1	Y
Access Guardian - Bridge	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.6R1	8.7R1	Y
Access Guardian - Access	N	N	N	Y	8.7R1	Y	Y	8.5R4	8.7R1	Y
Application Fingerprinting	N	N	N	N	N	N	Y	N	N	N
Application Monitoring and Enforcement (Appmon)	N	N	N	Y	8.7R2	N	N	N	N	N
ARP Poisoning Protection	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
BYOD - COA Extension support for RADIUS	8.7R2	Y	Y	Y	8.7R1	Y	8.62	8.6R2	8.7R1	Y
BYOD - mDNS Snooping/Relay	8.7R2	Y	Y	Y	8.7R1	Y	8.62	8.6R2	8.7R1	Y
BYOD - UPNP/DLNA Relay	8.7R2	Y	Y	Y	8.7R1	Y	8.62	8.6R2	8.7R1	Y
BYOD - Switch Port location information pass-through in RADIUS requests	8.7R2	Y	Y	Y	8.7R1	Y	8.62	8.6R2	8.7R1	Y
Captive Portal	8.7R2	8.5R4	Y	Y	8.7R1	Y	8.62	8.6R2	8.7R1	Y
IoT Device Profiling	8.7R2	8.5R2	8.5R2	8.5R2	8.7R1	8.5R2	8.5R2	8.6R1	8.7R1	8.5R2
IoT Device Profiling (IPv6)	8.7R2	8.7R1	8.7R1	8.7R1	N	8.7R1	8.7R1	N	N	8.7R1
Directed Broadcasts - Control	8.7R2	8.5R2	8.5R2	8.5R2	8.7R1	8.5R2	8.5R2	8.7R1	8.7R1	Y
Interface Violation Recovery	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.7R1	8.7R1	Y
Kerberos Snooping (services)	8.7R2	N	8.6R2	8.6R2	N	8.6R2	8.6R2	8.6R2	N	8.6R2
L2 GRE Tunnel Access (Edge) (bridge ports)	N	N	Y	Y	N	Y	8.6R1 ³	N	N	Y
L2 GRE Tunnel Access (Edge) (access ports)	N	N	N	8.6R1	8.7R2	8.6R1	8.6R1	8.7R1	8.7R2	8.6R1
L2 GRE Tunnel Aggregation	N	N	N	Y	8.7R2	Y	Y ³	8.7R1	8.7R2	Y
Learned Port Security (LPS)	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R4	8.7R1	Y

Feature	6360	6465	6560	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E	9900
MACsec ⁴	N	8.5R1	8.5R4	Y	8.7R1	N	N	N	X48C4E	8.5R2
MACsec MKA Support ⁴	N	8.5R2	8.5R4	8.5R2	8.7R1	N	N	N	X48C4E	8.5R2
Quarantine Manager	N	8.7R2	8.7R2	Y	8.7R2	Y	8.7R2	8.7R2	8.7R2	8.7R2
RADIUS - RFC-2868 Support	8.7R2	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4
Role-based Authentication for Routed Domains	N	N	N	8.5R4	8.7R1	8.5R4	8.5R4	8.6R1	8.7R1	8.5R4
Storm Control (flood-limit)	8.7R2	Y	Y	Y	8.7R1	Y	Y	Y	8.7R1	Y
Storm Control (Unknown unicast with action trap/shutdown)	N	N	N	Y	N	Y	Y	N	N	N
TACACS+ Client	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.6R1	8.7R1	Y
TACACS+ command based authorization	8.7R2	N	N	Y	8.7R1	Y	Y	8.7R2	8.7R2	N
TACACS+ - IPv6	8.7R3	8.7R3	8.7R3	8.7R3	8.7R3	8.7R3	8.7R3	8.7R3	8.7R3	8.7R3
PoE Features										
802.3af and 802.3at	8.7R2	8.5R1	Y	Y	8.7R1	Y	N	N	N	Y
802.3bt	8.7R2	Y	8.6R2	N	8.7R1	N	N	N	N	N
Auto Negotiation of PoE Class-power upper limit	8.7R2	8.5R1	Y	Y	8.7R1	Y	N	N	N	Y
Display of detected power class	8.7R2	8.5R1	Y	Y	8.7R1	Y	N	N	N	Y
LLDP/802.3at power management TLV	8.7R2	8.5R1	Y	Y	8.7R1	Y	N	N	N	Y
HPOE support	8.7R2 (95W)	8.5R1 (60W)	Y (95W)	Y (60W)	8.7R1 (95W)	Y (75W)	N	N	N	Y (75W)
Time Of Day Support	8.7R2	8.5R1	Y	Y		Y	N	N	N	Y
Perpetual PoE	8.7R2	N	N	Y	Y	Y	N	N	N	N
Fast PoE	8.7R2	N	N	Y	Y	Y	N	N	N	N
Data Center Features (License May Be Required)										
CEE DCBX Version 1.01	N	N	N	N	N	N	Y	N	N	N
Data Center Bridging (DCBX/ETS/PFC)	N	N	N	N	N	N	Y	N	N	N
EVB	N	N	N	N	N	N	N	N	N	N
FCoE / FC Gateway	N	N	N	N	N	N	Y	N	N	N
VXLAN ⁵	N	N	N	N	8.8R1	N	Q32/X72	8.5R3	8.8R1	N
VM/VXLAN Snooping	N	N	N	N	N	N	Y	N	N	N
FIP Snooping	N	N	N	N	N	N	Y	N	N	N
Notes:										

Feature	6360	6465	6560	6860(E)	6860N	6865	6900	6900- V72/ C32	6900- X48C6/ T48C6/X48C4E/V48C8/C32E	9900
<ol style="list-style-type: none"> 1. OS6560 supports stub area only. 2. See protocol support table in Appendix B. 3. Not supported on 6900-T20/T40/X20/X40. 4. Site license required beginning in 8.6R1. 5. L2 head-end only on OS6900-V72/C32. 										

Appendix B: MACsec Platform Support

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

MACsec Support (MACsec site license required)	
OmniSwitch 9900	
OS9900-CMM	4X10G mode only
OS9900-GNI-48/P48	10M/100M/1G ports
OS9900-XNI-48/P48	10G ports
OS9900-XNI-U48	10G ports
OS9900-XNI-P48Z16	1G/2.5G/5G/10G (16x) 1G/10G (32x)
OS99-GNI-U48	1G ports
OS99-XNI-U24	10G ports
OS99-XNI-P24Z8	1G/2.5G/5G/10G (8x) 1G/10G (16x)
OS99-XNI-U12Q	10G / 4x10G Uplink
OS99-XNI-UP24Q2	10G(Fiber)/4x10G Uplink 10G (Copper)
OS99-CNI-U8	Not Supported
OmniSwitch 6900	
OS6900-X48C4E	Dynamic mode only on all ports.
OmniSwitch 6860(E)	
OS6860(E)	All models support MACsec on 10G ports.
OS6860E-P24	1G/10G ports.
OS6860E-P24Z8	1G/10G ports (not supported on 2.5G ports).
OmniSwitch 6860N	
OS6860N-U28	SFP (1-24), SFP+ (25-28) and SFP28 (31-34) ports
OS6860N-P48Z	SFP28 (51-54) ports
OS6860N-P48M	- Expansion modules (Not supported on any 4X10G splitter transceivers). - Multi-rate Gigabit Ports (37-48)
OS6860N-P24Z	SFP28 (27-30) ports
OS6860N-P24M	- Expansion modules (Not supported on any 4X10G splitter transceivers) - Multi-rate Gigabit Ports (1-24)
OmniSwitch 6560	
OS6560-P24X4/24X4	- Ports 1-24 (Static and Dynamic modes) - Ports 25-30 (Not Supported)
OS6560-P48X4/48X4	- Ports 1-48 (Static and Dynamic modes) - Ports 49-52 (Dynamic mode only) - Ports 53-54 (Not Supported)
OS6560-P48Z16 (904044-90 only)	- Ports 1-32 (Static and Dynamic Modes) - Ports 33-48 (Static and Dynamic modes) - Ports 49-52 (Dynamic mode only) - Ports 53-54 (Not Supported)
OS6560-X10	- Ports 1-8 (10G ports only. Dynamic mode only) - Ports 9-10 (Not Supported)
OmniSwitch 6465	
	- OS6465-P28 - Supported on all ports except ports 27 and 28. - OS6465T-12 and OS6465T-P12 - Not supported on ports 11 and 12. - All other models support MACsec on all ports.

--	--

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

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

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

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
IPv4 Protocols								
Static Routing	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3
RIP v1/v2	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3
OSPF	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3
BGP	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3
VRRP	8.6R1	8.5R4	8.7R1	Y	8.7R1	8.7R2	8.7R2	8.7R3
IS-IS	Y	Y	Y	Y	Y	Y	8.7R2	8.7R3
PIM-SM/DM	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3
DHCP Relay	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.7R1	8.7R2	8.7R3
UDP Relay	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.7R1	8.7R2	8.7R3
DVMRP	N	N	N	N	N	N	N	N
BFD	Y	Y	Y	Y	Y	Y	8.7R2	8.7R3
IGMP Snooping	8.5R4	Y	8.7R1	Y	8.6R1	8.7R1	8.7R2	8.7R3
IP Multicast Headend Mode	8.5R4	Y	8.7R1	Y	8.6R1	8.7R1	8.7R2	8.7R3
IP Multicast Tandem Mode	8.5R4	Y	8.7R1	Y	8.6R1	Y	Y	Y
IPv6 Protocols								
Static Routing	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3
RIPng	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3
OSPFv3	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3
BGP	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3
VRRPv3	8.5R4	8.5R4	8.7R1	Y	8.7R1	8.7R2	8.7R2	8.7R3
IS-IS	Y	Y	Y	Y	Y	Y	8.7R2	8.7R3
PIM-SM/DM	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.7R1	8.7R2	8.7R3
DHCP Relay	8.6R1	8.6R1	8.7R1	8.6R1	8.6R1	8.7R1	8.7R2	8.7R3
UDP Relay	8.6R1	8.6R1	8.7R1	8.6R1	8.6R1	8.7R1	8.7R2	8.7R3
BFD	Y	Y	Y	Y	Y	Y	8.7R2	8.7R3
IPv6 MLD Snooping	8.5R4	Y	8.7R1	Y	Y	8.7R2	8.7R2	8.7R3
IPv6 Multicast Headend Mode	8.5R4	Y	8.7R1	Y	Y	8.7R2	8.7R2	8.7R3
IPv6 Multicast Tandem Mode	8.5R4	Y	8.7R1	Y	Y	Y	Y	Y

SPB BVLAN Scalability and Convergence Guidelines

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

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

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

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

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

Root Bridge						Services	Num	Tandem
BVLAN	ECT-algorithm	In Use	mapped	ISIDS	Multicast	(Name : MAC Address)		
4000	00-80-c2-01	YES	YES	5	SGMODE			
4001	00-80-c2-02	NO	NO	0	SGMODE			

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

Appendix D: General Upgrade Requirements and Best Practices

This section is to assist with upgrading an OmniSwitch. The goal is to provide a clear understanding of the steps required and to answer any questions about the upgrade process prior to upgrading. Depending upon the AOS version, model, and configuration of the OmniSwitch various upgrade procedures are supported.

Standard Upgrade - The standard upgrade of a standalone chassis or virtual chassis (VC) is nearly identical. All that's required is to upload the new image files to the *Running* directory and reload the switch. In the case of a VC, prior to rebooting the Master will copy the new image files to the Slave(s) and once the VC is back up the entire VC will be synchronized and running with the upgraded code.

ISSU - The In Service Software Upgrade (ISSU) is used to upgrade the software on a VC or modular chassis with minimal network disruption. Each element of the VC is upgraded individually allowing hosts and switches which are dual-homed to the VC to maintain connectivity to the network. The actual downtime experienced by a host on the network should be minimal but can vary depending upon the overall network design and VC configuration. Having a redundant configuration is suggested and will help to minimize recovery times resulting in sub-second convergence times.

Virtual Chassis - The VC will first verify that it is in a state that will allow a successful ISSU upgrade. It will then copy the image and configuration files of the ISSU specified directory to all of the Slave chassis and reload each Slave chassis from the ISSU directory in order from lowest to highest chassis-id. For example, assuming chassis-id 1 is the Master, the Slave with chassis-id 2 will reload with the new image files. When Slave chassis-id 2 has rebooted and rejoined the VC, the Slave with chassis -id 3 will reboot and rejoin the VC. Once the Slaves are complete they are now using the new image files. The Master chassis is now rebooted which causes the Slave chassis to become the new Master chassis. When the original Master chassis reloads it comes back as a Slave chassis. To restore the role of Master to the original Master chassis the current Master can be rebooted and the original Master will takeover, re-assuming the Master role.

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

Supported Upgrade Paths and Procedures

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

Platform	AOS Releases Supporting ISSU to 8.8R1 (GA)
OS6360	8.7.252.R02 (GA) 8.7.98.R03 (GA)
OS6465	8.7.277.R01 (GA) 8.7.280.R01 (MR) 8.7.354.R01 (GA) 8.7.252.R02 (GA) 8.7.98.R03 (GA)
OS6560	8.7.354.R01 (GA) 8.7.252.R02 (GA) 8.7.98.R03 (GA)
OS6860(E)	8.7.277.R01 (GA) 8.7.280.R01 (MR) 8.7.354.R01 (GA) 8.7.252.R02 (GA) 8.7.98.R03 (GA)
OS6860N	8.8.152.R01 (GA)*
OS6865	8.7.277.R01 (GA) 8.7.280.R01 (MR) 8.7.354.R01 (GA) 8.7.252.R02 (GA) 8.7.98.R03 (GA)
OS6900	8.7.277.R01 (GA) 8.7.280.R01 (MR) 8.7.354.R01 (GA) 8.7.252.R02 (GA) 8.7.98.R03 (GA)
OS6900-V72/C32/ X48C6/T48C6/X48C4E/V48C8	8.8.152.R01 (GA)*
OS9900	8.7.354.R01 (GA) 8.7.252.R02 (GA) 8.7.98.R03 (GA)
*ISSU will not be supported to 8.8.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.	

8.8R1 ISSU Supported Releases

Prerequisites

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

- Be the responsible party for maintaining the switch's configuration.

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

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

Switch Maintenance

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

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

```
6900-> show system
System:
Description: Alcatel-Lucent OS6900-X20 8.6.289.R01 GA, July 14, 2019.,
Object ID: 1.3.6.1.4.1.6486.801.1.1.2.1.10.1.1,
Up Time: 0 days 0 hours 1 minutes and 44 seconds,
Contact: Alcatel-Lucent, http://alcatel-lucent.com/wps/portal/enterprise,
```



```

Name:          6900,
Location:      Unknown,
Services:      78,
Date & Time:   MON AUG 12 2019 06:55:43 (UTC)
Flash Space:
Primary CMM:
Available (bytes): 1111470080,
Comments      : None

```

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

```

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

```

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

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

```

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

```

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

```

6900-> write memory flash-synchro

```

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

```

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

```

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

```

6900-> show tech-support eng complete

```

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

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

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

2. FTP the Upgrade Files to the Switch

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

3. Upgrade the image file

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

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

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

4. Verify the Software Upgrade

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

```
OS6900-> show microcode
/flash/working
Package           Release           Size      Description
-----+-----+-----+-----
Tos.img           8.8.152.R01      239607692 Alcatel-Lucent OS
```

```
6900-> show running-directory
```

CONFIGURATION STATUS

```
Running CMM       : MASTER-PRIMARY,
CMM Mode          : VIRTUAL-CHASSIS MONO CMM,
Current CMM Slot  : CHASSIS-1 A,
Running configuration : WORKING,
Certify/Restore Status : CERTIFY NEEDED
```

SYNCHRONIZATION STATUS

```
Running Configuration : SYNCHRONIZED
```

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

5. Certify the Software Upgrade

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

```
OS6900-> copy running certified
-> show running-directory
CONFIGURATION STATUS
Running CMM       : MASTER-PRIMARY,
CMM Mode          : VIRTUAL-CHASSIS MONO CMM,
Current CMM Slot  : CHASSIS-1 A,
Running configuration : WORKING,
```

Certify/Restore Status : CERTIFIED

SYNCHRONIZATION STATUS

Running Configuration : SYNCHRONIZED

Appendix F: ISSU - OmniSwitch Chassis or Virtual Chassis

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

1. Download the Upgrade Files

Go to the Service and Support Website and download and unzip the ISSU upgrade files for the appropriate platform and release. The archive contains the following:

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

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

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

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

3. Clean up existing ISSU directories

It is important to connect to the Slave chassis and verify that there is no existing directory with the path `/flash/issu_dir` on the Slave chassis. ISSU relies upon the switch to handle all of the file copying and directory

creation on the Slave chassis. For this reason, having a pre-existing directory with the same name on the Slave chassis can have an adverse effect on the process. To verify that the Slave chassis does not have an existing directory of the same name as the ISSU directory on your Master chassis, use the internal VF-link IP address to connect to the Slave. In a multi-chassis VC, the internal IP addresses on the Virtual Fabric Link (VFL) always use the same IP addresses: 127.10.1.65 for Chassis 1, 127.10.2.65 for Chassis 2, etc. These addresses can be found by issuing the debug command **'debug show virtual-chassis connection'** as shown below:

```
OS6900-> debug show virtual-chassis connection
```

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

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

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

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

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

6. Log out of the Slave chassis:

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

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

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

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

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

9. Upgrade the image files using ISSU:

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

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

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

This indicates that the ISSU is completed

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

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

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

10. Verify the Software Upgrade

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

```
OS6900-> show microcode
/flash/working

Package      Release      Size      Description
-----+-----+-----+-----
Tos.img      8.8.152.R01  239607692 Alcatel-Lucent OS
```

11. Certify the Software Upgrade

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

```
OS6900-> 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 pmnds
	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	8.7.33.R01
	Platforms	OS6465, OS6865

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_7594
- U-boot.8.8.R01.33.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_7594
Parse /flash/fpga_kit_7594
fpga file: OS6900-X72_CPLD_V01B_20191204.vme
Please wait...
fpga file: OS6900-X72_CPLD_V01B_20191204.vme
update chassis 1
Starting CMM ALL FPGA Upgrade
CMM 1/1
Successfully updated
Reload required to activate new firmware.
```

4. If required, a u-boot upgrade can then be performed, for example:

-> update uboot cmm all file /flash/u-boot.8.8.R01.33.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: Fixed Problem Reports






The following problem reports were closed in this release.






CR/PR NUMBER	Description
Case: 00570180 CRAOS8X-29500 CRAOS8X-27737	<p>Summary: GRE tunnel status showing down with tunnel-dst-unreachable message when OSPF link are disturbed.</p> <p>Explanation: When a route entry with same prefix as that of tunnel destination is getting deleted, the operational state of tunnel is going down with the reason "tunnel-dst-unreachable".</p> <p>Fix is given to avoid GRE operational status from going DOWN though a route entry with same prefix as that of tunnel destination is getting deleted.</p> <p> Click for Additional Information</p>
Case: 00557643 CRAOS8X-28072	<p>Summary: NI in OS9900 reset due to unexpected IPC handshake.</p> <p>Explanation: The trigger for the reset was due to LagNi has received an unexpected IPC handshake message while it was trying to read from a Socket. NI will not reset normally on a socket read. This issue will not happen frequently.</p> <p>Fix is given to handle the IPC handshake exceptions in LagNI module.</p> <p> Click for Additional Information</p>
Case: 00550234 CRAOS8X-27628	<p>Summary: Powered devices are not coming up on PoE ports seen when downgrading the switch from any builds of 8.7R02 to 8.4.1.141.R03.</p> <p>Explanation: The PoE controller state is enabled in 8.7R02 but not programmed to the PoE controller and once the switch is downgraded to 8.4 R01, the switch assumes the PoE controller is programmed as the PoE controller state is enabled and this leads to a port mapping issue.</p> <p>Fix is given will ensure the PoE controller will be re-initialized during an upgrade from fix build or downgrade from fix build to get the Powered devices coming up successfully.</p> <p> Click for Additional Information</p>
Case: 00556835 CRAOS8X-28143	<p>Summary: User lockout for Admin account in 8.7.R02.</p> <p>Explanation: Expected behavior is Admin account must not lockout in any scenario for console access and should be locked for other type of sessions.</p> <p>However, when password expiration date is set and when it expires for admin account, the admin user cannot log in as it locks the account. Fix is given to have admin account user to log in through console without getting locked after the password expiration.</p> <p> Click for Additional Information</p>
Case: 00581409 CRAOS8X-30586	<p>Summary: OS6900-X48C6: "show interfaces status" doesn't display complete output with an - ERROR: Invalid Chassis/Slot/Port, chassis 1 slot 1 port range <1 to 69>.</p> <p>Explanation: Due to the break-out mode enabled on one of the 100G port and after reload to take effect of</p>







	<p>this configuration, switch displayed incomplete ports with an error. There was no production impact. Fix is given to display all the 54 ports in “show interfaces status” output.</p> <p> Click for Additional Information</p>
<p>Case: 00573589 <i>CRAOS8X-29818</i></p>	<p>Summary: Console log printed for 25G connection as 10G connection when bringing up 4X25G splitter cable on OS6900.</p> <p>Explanation: Unable to use splitter cable on port 1/1/9A and 1/1/9D. Other than 2 ports all the other prts are working fine.</p> <p>The fix is given to avoid displaying the incorrect port speed detection log.</p> <p> Click for Additional Information</p>
<p>Case: 00569481 <i>CRAOS8X-29151</i></p>	<p>Summary: OpenSSL vulnerability analysis of CVE-2021-3712 with AOS 8X switches.</p> <p>Explanation: An ASN1 string might not be NUL terminated when an application directly creates it or when it uses ASN1_STRING_set0() function to do the same. Issue happens when this non NUL terminated ASN1 string is processed by any of the affected OpenSSL functions. Since these functions assume the string to be NUL terminated, buffer overrun can occur when they try to print the string.</p> <p>The issue is fixed in OpenSSL by adding conditions in the affected functions to check and use the buffer length field in ASN1_STRING data structure while printing ASN1 strings, so that the memory beyond that length is not accessed.</p> <p> Click for Additional Information</p>
<p>Case: 00562383 <i>CRAOS8X-28419</i></p>	<p>Summary: EMP warning message on OS6560 and OS6860E -"swlogd ipv6 itf WARN: ip6cmmEmp_islftUsblnserted".</p> <p>Explanation: The IP interface name starting with word “emp” (such as employee) are considered as EMP (Ethernet Management Port) and gets converted to “EMP” automatically instead of “employee”.</p> <p>Fix is given to retain the same string name as configured in IP interface commands.</p> <p> Click for Additional Information</p>
<p>Case: 00574423 <i>CRAOS8X-29999</i></p>	<p>Summary: Incomplete error message "Password is not allowed to be modified until" has been thrown while logging into the switch using expired users following the upgrade to any code post 8.6.R02.</p> <p>Explanation: This issue is noticed when "user password-min-age" is configured for expired users and then upgrade to 8.6.R02 and above codes. This is identified to be a bug in lack of migrating "passwordAllowModifyDate" filed from userTable7 to userTable8. Having min-age as 0 resolves this.</p> <p>NOTE: Issue seen while upgrading with min-age set from any code prior to 8.6.R02 to above AOS images. Example: (8.4.R03 to 8.6.R02 and 8.5R1 to 8.7.R02)</p> <p> Click for Additional Information</p>
<p>Case: 00543032 <i>CRAOS8X-27085</i></p>	<p>Summary: SNMP Poll to collect mac-address failed.</p> <p>Explanation: SNMP polling to gather info about devices connected to the network through dot1dTpFdbEntry</p>







	<p>(1.3.6.1.2.1.17.4.3) and dot1qTpFdbEntry (1.3.6.1.2.1.17.7.1.2.2) and 1.3.6.1.4.1.6486.801.1.2.1.8.1.1.8.1.13 did not work.</p> <p>The fix is available in 8.8.R01.</p> <p> Click for Additional Information</p>
<p>Case: 00564230 CRAOS8X-28818</p>	<p>Summary: OS6560: HTTP and FTP packets are dropped on macsec enabled ports.</p> <p>Explanation: After enabling macsec, some of the HTTP, HTTPS, FTP and also SSH data packets are dropped on the ports.</p> <p> Click for Additional Information</p>
<p>Case: 00536107 CRAOS8X-26697</p>	<p>Summary: OS6860E-24: After link flap, the OSPF adjacency gets stuck in EXSTART/EXCH state.</p> <p>Explanation: After OSPF adjacency flap, OSPF routes are properly updated in the software but not in hardware. This results in loss of connectivity.</p> <p> Click for Additional Information</p>
<p>Case: 00532519 CRAOS8X-26884</p>	<p>Summary: 6860N-P48Z: multicast PTP flows fail when passing through multiple hops.</p> <p>Explanation: 6860N-P48Z-sends-out-tagged-multicast-packets-on-untagged-ports-As-the-end-devices-receive-tagged-frames-the-packets-are-discarded-resulting-in-communication-issue</p> <p> Click for Additional Information</p>
<p>Case: 00541920 CRAOS8X-26978</p>	<p>Summary: OS6560-P24X4: LEDs OFF on ports 1/1/25-26. No functional impact.</p> <p>Explanation: After reloading an OS6560-P24X4, the LEDs on the ports 1/1/25-26 are OFF. There is no functional impact.</p> <p> Click for Additional Information</p>
<p>Case: 00560486 CRAOS8X-28106</p>	<p>Summary: Missing log entries in AOS switches.</p> <p>Explanation: In AOS sometimes the logging stops and few entries are missed. A mechanism is introduced to periodically verify if the swlog module is running and logging properly.</p> <p> Click for Additional Information</p>
<p>Case: 00565098 CRAOS8X-29982</p>	<p>Summary: Improper Capacitor Detection results are seen for the ports in which the end-device compatible with IEEE specifications are connected. Hence, the port detect "FAULT State change 1b to 25" and the lanpower in the port is turned OFF.</p> <p>Explanation: To provide lanpower via PoE to the legacy devices, capacitor-detection is enabled. If switch has mixed end device environment with PoE and non-PoE devices, it would create an issue since</p>








	<p>capacitor-detection is not compatible with IEEE specifications. Whenever a FAULT is detected in the port, the switch will send the “pethPsePortOnOffNotification” trap.</p> <p> Click for Additional Information</p>
<p>Case: 00543841 CRAOS8X-27155</p>	<p>Summary: Traffic from client with Static IP address is not blocked by IP source filtering, if the port is part of the port group “UserPorts”.</p> <p>Explanation: DHCP-snooping binding entry will only be created, if the end device gets an IP address via DHCP. “UserPorts” config will create an “ACCEPT” rule to allow valid non-spoofed traffic. In 6860N, the “anti-spoof” rules gets more precedence over “IP source filtering” and hence the traffic was allowed.</p> <p> Click for Additional Information</p>
<p>Case: 00571923 CRAOS8X-29478</p>	<p>Summary: Since upgrade to AOS 8.7R03 Management station is not able to poll several objects by SNMP.</p> <p>Explanation: SNMP Bulk Request fails when polling IF-MIB therefore following logs are printed and Management station cannot monitor devices.</p> <p><i>2021 Sep 20 17:37:00.678 OS6860E-Core2 swlogd SNMP aluSubagent_main ERR: snmp_check_user_permission NEXT functional privileges failed for DISTROW table type</i> <i>2021 Sep 20 17:37:00.678 OS6860E-Core2 swlogd SNMP aluSubagent_main ERR: snmp_check_user_permission table name ifXTable user name snmpuser3</i></p> <p> Click for Additional Information</p>
<p>Case: 00562543 CRAOS8X-28315</p>	<p>Summary: On OmniVista the UNP status is not True for every UNP Port enabled.</p> <p>Explanation: The SNMPWalk request does not return all entries when polling alaDaUNPPortTable if non-UNP ports are set between UNP Ports enabled.</p> <p> Click for Additional Information</p>
<p>Case: 00561817 00563083 CRAOS8X-28286</p>	<p>Summary: OS9900 No MAC Addresses learnt in newly created SPB services</p> <p>Explanation: On SPB Service used for IPMS traffic the mclIdx Index reached the maximum counters 20480 resulting of no enough counters available for new SPB Services.</p> <p> Click for Additional Information</p>
<p>Case: 00556450 CRAOS8X-27884</p>	<p>Summary: AOS 8.7R02 Build 252 - Core dump observed on AGCMM when connecting IPTouch to UNP Ports and sending Network Policy through LLDP.</p> <p>Explanation: When IPTouch is sending untagged frames followed by tagged frames, AGCMM module crash with incident:</p> <p>swlogd AGCMM AG-General INFO: agCmmSentAllocationReqToSvcMgr():633: Msg (requestId = 9) sent to Service Manager failed</p> <p> Click for Additional Information</p>


<p>Case: 00551424 CRAOS8X-27653</p>	<p>Summary: OS6860N - service spb "vlan-xlation" modified from No to Yes (Auto) on the SPB Service bound to IP Interface (In-line routing)</p> <p>Explanation: Current behavior is: when an IP Interface is created/bound on a SPB Service, we automatically enable the VLAN-Translation. We added an ERROR message when user tries to modify the vlan-xlation on the service:</p> <p>OS6860N -> service 5 spb isid 6000 bvlan 600 vlan-xlation enable</p> <p>ERROR: Modify vlan translation currently not allowed for service (5)</p> <p> Click for Additional Information</p>
<p>Case: 00553301 CRAOS8X-27737</p>	<p>Summary: When connecting a PC and an IPTouch to same UNP Port of type access with tagged VLAN, switch sends EAP Failure</p> <p>Explanation: Each time the 2nd device is authenticated, MAC is flushed and EAP Failure is generated</p> <p> Click for Additional Information</p>
<p>Case: 00553308 CRAOS8X-27739</p>	<p>Summary: OS6860N - Core dump on AGCMM module - Error: unable to connect to access guardian.</p> <p>Explanation: After pushed config from OV 2500 with modifications on UNP config like removed the auth-server-down, we noticed Core Dump on AGCMM module.</p> <p>Tue Jun 15 10:23:11 : ChassisSupervisor appMgr ALRT message: +++ appMgrClientTerminated: restarting task +++ Failed App /bin/agCmm</p> <p>Tue Jun 15 10:23:11 : AGCMM AG-Cp-Web ERR message:+++ Lighttpd error: (network.c.320) can't bind to socket: 127.2.255.1:265 Address already in use</p> <p>Tue Jun 15 10:23:12 : ipmscmm info ALRT message:+++ unable to connect to access guardian: 0</p> <p> Click for Additional Information</p>
<p>Case: 00552794 CRAOS8X-27760</p>	<p>Summary: OS6860N - LLDP malformed frames for LLDP-Med/Network Policy.</p> <p>Explanation: Phones connected to UNP Ports do not receive their VLAN ID via LLDP Network Policy. LLDP Frames generated by switch are malformed or contain wrong contents.</p> <p> Click for Additional Information</p>
<p>Case: 00494583 CRAOS8X-22176</p>	<p>Summary: OS6560 "Notify failed on some devices" error when notifying Unified policy with OV-L3-AcceptAllPolicy-IPv6</p> <p>Explanation: If Unified Policy contains a policy with a name up to 16 characters, the policy is not applied on Switch's QOS</p> <p> Click for Additional Information</p>

<p>Case: 00566540 CRAOS8X-28826</p>	<p>Summary: OS9900_ Connection drops during OS9900 CMM failover when 1G SFP is replaced with 10G SFP Resulting Ping loss.</p> <p>Explanation: During the takeover the line parameters will be set for the ports. If there is a difference in parameters, the port is admin disabled to apply the line parameters and then admin enabled.</p> <p>This issue will be resolved in 8.8.R1.</p> <p> Click for Additional Information</p>
<p>Case: 00547183 CRAOS8X-27765</p>	<p>Summary : User cannot perform lanpower related operations even with 'lanpower' read-write privilege.</p> <p>Explanation : This issue is due to 'lanpower' not having its own family; it is using the same family as 'module'. Issue is fixed from AOS 8.8R01, where user configured with 'lanpower' privilege will be able to perform lanpower related operations.</p> <p> Click for Additional Information</p>
<p>Case: 00562696 CRAOS8X-28814</p>	<p>Summary : "Write Memory failed! Unable to retrieve QOS configuration." error is seen when issuing <write memory flash-synchro> command.</p> <p>Explanation : The issue is observed when we try to modify an existing policy rule multiple times. A fix to this issue is provided from AOS 8.8R01.</p> <p> Click for Additional Information</p>
<p>Case: 00553686 CRAOS8X-28449</p>	<p>Summary: Alcatel switches do not always include the switch device name in the logs, which was displayed as conslog and kernel. The observed problem has been fixed and would be available from AOS 8.8R01 GA release.</p> <p>Explanation: While viewing the logs using the Log concentrator application, some of the logs were associated with the different keywords "ConsLog" or "kernel". However, some of the logs were included with the Hostname. While capturing the logs using the wirehshark tool, we could see logs are not having the switch hostname. While viewing the logs directly in the switch, it could be noticed the switch is always displaying the device name with timestamp in the logs. In the current microcode AOS 8.8R01 GA the switch replaces its device name with "ConsLog" or "kernel" when generating and sending logs.</p> <p> Click for Additional Information</p>
<p>Case: 00556633 CRAOS8X-28162</p>	<p>Summary: Display of Incomplete linkagg configuration in the output of "show configuration snapshot linkagg" CLI command.</p> <p>Explanation: The "show configuration snapshot linkagg" CLI command does not display the line of linkagg lacp agg 23 due to MIP overflow was not handled and hence the issue occurred.</p> <p> Click for Additional Information</p>
<p>Case: 00576735 CRAOS8X-30151</p>	<p>Summary: To create a read-only user on AOS8x with the ability to read and list files in /flash/python/ directory</p>

	<p>Explanation: A read-only user in AOS8x is not able to read and list files in /flash/python/ directory</p> <p> Click for Additional Information</p>
<p>Case: 00578924 CRAOS8X-30434</p>	<p>Summary: Unable to split more than 2 QSFP28 Ports on OS6900-T48C6.</p> <p>Explanation: The 6900X48C6 and 6900T48C6 support the break-out mode only in port 51 and 54, documentation is updated with this info.</p> <p> Click for Additional Information</p>
<p>Case: 00579609 CRAOS8X-30656</p>	<p>Summary: Break-out B C and D ^ports can be recognized only after switch reboot.</p> <p>Explanation: After changing the splitter cable from port 51 to 54 in slave unit the ports B C and D are in down state till reloading the switch.</p> <p> Click for Additional Information</p>
<p>Case: 00580606 CRAOS8X-30624</p>	<p>Summary: loosing vlan configuration on port 51 and 54 after reboot.</p> <p>Explanation: After rebooting a switch with configuration of break-out mode enable on ports 49-54 having vlan tagged to this ports the switch once UP consider the port A B C D of port 49 as 50,51, 52 53 and A,B,C,D of 50 as 54,55,56,57 which make an error in config. Fix is available in 8.8R01.</p> <p> Click for Additional Information</p>
<p>Case: 00576322 CRAOS8X-30149</p>	<p>Summary: Swlog stops logging locally after enabling output socket.</p> <p>Explanation: Swlogd is no more logging in swlog_chassis2 file as the switch was keeping the path of ISSU directory when the issue happens, the deletion of the issu directory in addition of enabling output socket created this behavior.</p> <p> Click for Additional Information</p>
<p>Case: 00561886 CRAOS8X-28229</p>	<p>Summary: OS6860: high memory seen while getting IP addresses for thousands of DHCP clients, connected on UNP ports, caused by dpcmm process.</p> <p>Explanation: dpcmm , if device-profile enabled, will work and collect data from UNP ports and share it with OV2500. Also, there is a limit of 1000 users, if there are more users than the limit, dpcmm will leak memory.</p> <p> Click for Additional Information</p>
<p>Case: 00557416 CRAOS8X-27961</p>	<p>Summary: OS6900/OS6860: temporary loss of traffic happening on router, when system time reaches 497 days. Swlog consoles display ipni arp and arptimer alarm messages at issue time.</p> <p>Explanation: the internal ARP timer (restarted when ARP entries are about to age out) gets ineffective when the switch systemUptime reaches the 497 days 2:27mn52s. During this time, ARP resolved can't get learnt and the ARP resolution keeps happening at a high rate, hitting the switch CPU; overall, the switch experiences traffic latency.</p>

	<p> Click for Additional Information</p>
<p>Case: 00554311 CRAOS8X-27784</p>	<p>Summary: OS6860N: Storm Threshold violation could be seen, on links flapping, even if no incoming broadcast traffic is seen on these interfaces.</p> <p>Explanation: Calculation for Storm Threshold violation depends on a HW counter that gets reset to 0 (during link flappings). This explains why Storm Threshold violation are seen even if no broadcast incoming packets are seen.</p> <p> Click for Additional Information</p>
<p>Case: 00578934 CRAOS8X-30261</p>	<p>Summary: OS6900 : once the IP interface is overwritten (from VLAN domain to SPB control BVLAN, then back to VLAN domain, connectivity is lost between SPB switches.</p> <p>Explanation: When the control-bvlan is mapped to the IP interface, the broadcast/multicast flag is removed to avoid flooding in SPBM interface. So when vlan is changed back to normal vlan, this flag is not added back. Hence ARP-Requests are not sent out and ping fails.</p> <p>Removing the VLAN ip interface and re adding it, will solve the connectivity problem.</p> <p> Click for Additional Information</p>
<p>Case: 00576977 CRAOS8X-30080</p>	<p>Summary: For 6900X48/T48-C6 model, the breakout mode is supported only in ports 51 and 54, the VFL is not supported on break-out ports using the 4x10G mode.</p> <p>Explanation: Cli and specification documentation are having the info that VFL is not supported on break-out port when using the 4x10G break-out mode.</p> <p> Click for Additional Information</p>
<p>Case: 00577086 CRAOS8X-30127</p>	<p>Summary: For 6900X48/T48-C6 model the VFL is supported on 10G ports.</p> <p>Explanation: Adding the information that 10G port are supporting the VFL to user guides documentation.</p> <p> Click for Additional Information</p>
<p>Case: 00538383 CRAOS8X-28240</p>	<p>Summary: 6465-P28 LED on port 1/1/25 and 1/1/26 are amber however for ports 27 and 28 LED are green, same speed on this 4 ports that supports 10G documentation don't have info regarding amber color.</p> <p>Explanation: All last 4 ports will have same color which is green and documentation will be updated with this info.</p> <p> Click for Additional Information</p>
<p>Case: 00568683 00580183 CRAOS8X-29567</p>	<p>Summary: PVST+ BPDUs are not being recognized even when pvst+compatibility is enabled. Tunneling over SPB is also not working when STP is configured for tunnel in the L2profile.</p> <p>Explanation: When pvst+compatibility is enabled not all switches in the broadcast domain were recognizing the root bridge which was sending PVST+ BPDUs.</p>

	<p> Click for Additional Information</p>
<p>Case: 00537931 CRAOS8X-26776</p>	<p>Summary: Enabling MVRP flushes and relearns VLANs frequently on 6350 access layer switch</p> <p>Explanation: MVRP is sending flush event messages to the same port it is receiving MVRP learn events.</p> <p> Click for Additional Information</p>
<p>Case: 00562309 CRAOS8X-28439</p>	<p>Summary: OS9900_Ports that have speed and auto-negotiation enabled drop connection when the Primary CMM fails over to the Secondary CMM.</p> <p>Explanation: During the takeover the line parameters will be set for the ports. If there is a difference in parameters, the port is admin disabled to apply the line parameters and then admin enabled.</p> <p>This issue will be resolved in 8.8.R1.</p> <p> Click for Additional Information</p>
<p>Case: 00554047 CRAOS8X-27769</p>	<p>Summary: Getting intermittent failures when trying to load QoS policies to 6465 from OV. Failure is successful sometimes and fails with Error Handling - Flush the LDAP Policies in QoS log.</p> <p>Explanation: With fix under AOS 8.8 R01 GA, now successfully load policies from both CLI and OV.</p> <p> Click for Additional Information</p>
<p>Case: 00544352 CRAOS8X-27279</p>	<p>Summary: OS6860N: Storm Threshold Violation issue caused by duplicated DHCP broadcast issue.</p> <p>Explanation: The handling of broadcast between the ASIC and CPU was incorrectly programmed. Issue has been fixed under 8.8 R01 GA.</p> <p> Click for Additional Information</p>
<p>Case: 00560873 CRAOS8X-28297</p>	<p>Summary: Mac-address count is not getting flushed on UNP ports with LPS enabled. Port is down, but keep with 3 macs learned.</p> <p>Explanation: when lldp re-authentication is triggered and even if client is still under byod in-progress state, lps check for max bridge count is performed and failing at that point. Hence violation is being raised.</p> <p>This issue is resolved in 8.7.257.R02 or 8.8.R01.</p> <p> Click for Additional Information</p>
<p>Case: 00589809 CRAOS8X-31414</p>	<p>Summary: With service inline routing, packets received on a SAP port are discarded if they have to be routed via the same SAP port.</p> <p>Explanation: The packets from any client received on OS6900-V48C8 are not routed if the routed packets have to egress from the same link. It is noticed that the packets are getting discarded on the router which in this case is OS6900-V48C8. Issue is fixed in AOS 8.8 R01.</p> <p> Click for Additional Information</p>
<p>Case: 00584841 CRAOS8X-31439</p>	<p>Summary: On OS6900-C32, upon upgrading to 8.7 R03, the 4X25G links are not coming up.</p>

	<p>Explanation: Observed issue is identified as bug due to interface FEC mode changing as it should be in FC mode for OS6900-C32 switch model. The issue has been fixed and available from AOS 8.8 R01 GA.</p> <p> Click for Additional Information</p>
--	---

Appendix I: Installing/Removing Packages

The package manager provides a generic infrastructure to install AOS or non-AOS third party Debian packages and patches. The following packages are supported. The package files are kept in the **flash/working/pkg** directory or can be downloaded from the Service & Support website.

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

Installing Packages

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

```
-> pkgmgr verify nos-mrp-v1.deb
    Verifying MD5 checksum.. OK
-> pkgmgr install nos-mrp-v1.deb
-> write memory
-> show pkgmgr
```

Legend: (+) indicates package is not saved across reboot

(*) indicates packages will be installed or removed after reload

Name	Version	Status	Install Script
-----+-----+-----+-----			
ams	default	installed	default
ams-apps	default	installed	default
mrp	8.7.R03-xxx	installed	/flash/working/pkg/mrp/install.sh

Removing Packages

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

```
-> pkgmgr remove mrp
```

Purging mrp (8.7.R03-xxx)...

Removing package mrp.. OK

Write memory is required complete package mrp removal

```
-> write memory
```

Package(s) Committed

```
-> show pkgmgr
```

Legend: (+) indicates package is not saved across reboot

(*) indicates packages will be installed or removed after reload

Name	Version	Status	Install Script
-----+-----+-----+-----			
ams	default	installed	default
ams-apps	default	installed	default
mrp	8.7.R03-xxx	removed	/flash/working/pkg/mrp/install.sh

Remove the Debian package installation file. For example:

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

AOS Upgrade with Encrypted Passwords

AMS

The *ams-broker.cfg* configuration file for AMS contains plain text passwords. The passwords can be stored as encrypted beginning with the 8.7R1 release. Follow the steps below prior to upgrading to 8.7R1 or later release to store encrypted passwords.

1. Remove *ams-broker.cfg* file present under path */flash/<running-directory>/pkg/ams/* prior to upgrading AOS.
2. This will remove the broker configuration which must be re-configured after the upgrade.
3. Remove this file from each VC node.
4. Upgrade the switch.
5. Once the switch comes up after the upgrade, the password present under */flash/<running-directory>/pkg/ams/ams-broker.cfg* file will be encrypted.

IoT-Profiler

The *ovbroker.cfg* configuration file for AMS-APPS/IoT-Profiler contains plain text passwords. The passwords can be stored as encrypted beginning with the 8.7R1 release. Follow the steps below prior to upgrading to 8.7R1 or later release to store encrypted passwords.

1. Remove the *install.sh* file present under path */flash/<running-directory>/pkg/ams-apps/* for AMS-APPS prior to upgrading AOS.
2. Remove this file from each VC node.
3. Upgrade the switch.
4. Once the switch comes up after the upgrade, the password present under */flash/<running-directory>/pkg/ams-apps/ovbroker.cfg* file will be encrypted.