

Release Notes - Rev. A

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

Release 8.8R2

These release notes accompany release 8.8R2. These release notes provide important information on individual software features and hardware modules. Since much of the information in these release notes is not included in the hardware and software user manuals, it is important that you read all sections of this document before installing new hardware or loading new software.

Contents

Contents 2

Related Documentation 3

System Requirements 4

[IMPORTANT] *MUST READ*: AOS Release 8.8R2 Prerequisites and Deployment Information 10

Licensed Features 13

ALE Secure Diversified Code..... 13

New / Updated Hardware Support and Guidelines 14

New Software Features and Enhancements 15

Open Problem Reports and Feature Exceptions 17

Hot-Swap/Redundancy Feature Guidelines 20

Technical Support 23

Appendix A: Feature Matrix 25

Appendix B: MACsec Platform Support 34

Appendix C: SPB L3 VPN-Lite Service-based (Inline Routing) / External Loopback Support / BVLAN Guidelines..... 35

Appendix D: General Upgrade Requirements and Best Practices..... 38

Appendix E: Standard Upgrade - OmniSwitch Standalone or Virtual Chassis 42

Appendix F: ISSU - OmniSwitch Chassis or Virtual Chassis 44

Appendix G: FPGA / U-boot Upgrade Procedure 47

Appendix H: CPLD Upgrade Procedure for ONIE-Based Devices 50

Appendix I: Fixed Problem Reports 51

Appendix J: Installing/Removing Packages 56

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 8.8.56.R02 (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
OS6360-PH48	8.8.114.R01	8.8.114.R01	0.12	0.12

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

OmniSwitch 6465 - AOS Release 8.8.56.R02 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6465-P6	8.5.83.R01	8.7.2.R02 ² 8.7.30.R03 ³ 8.8.33.R01 ⁴	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 8.8.56.R02 (GA)

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

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6560-24Z8	8.5.22.R01	8.7.2.R02 ³ 8.7.30.R03 ⁷	0.7	0.8 ⁵
OS6560-P24Z8	8.4.1.23.R02	8.7.2.R02 ³ 8.7.30.R03 ⁷	0.6	0.7 ¹ 0.8 ⁵
OS6560-24X4	8.5.89.R02	8.7.2.R02 ⁴ 8.7.30.R03 ⁷	0.4	0.4
OS6560-P24X4	8.5.89.R02	8.7.2.R02 ⁴ 8.7.30.R03 ⁷	0.4	0.4
OS6560-P48Z16 (903954-90)	8.4.1.23.R02	8.7.2.R02 ³ 8.7.30.R03 ⁷	0.6	0.7 ¹ 0.8 ⁵
OS6560-P48Z16 (all other PNs)	8.5.97.R04	8.7.2.R02 ³ 8.7.30.R03 ⁷	0.3	0.6 ² 0.7 ⁶
OS6560-48X4	8.5.97.R04	8.7.2.R02 ⁴ 8.7.30.R03 ⁷	0.4	0.7 ² 0.8 ⁶
OS6560-P48X4	8.5.97.R04	8.7.2.R02 ⁴ 8.7.30.R03 ⁷	0.4	0.7 ² 0.8 ⁶
OS6560-X10	8.5.97.R04	8.7.2.R02 ⁴ 8.7.30.R03 ⁷	0.5	0.8 ²
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 8.8.56.R02 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6860/OS6860E (except U28/P24Z8)	8.1.1.70.R01	8.7.30.R03 ²	0.9	0.10 ¹
OS6860E-U28	8.1.1.70.R01	8.7.30.R03 ²	0.2	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 8.8.56.R02 (GA)

Hardware	Minimum ONIE	Current ONIE	Minimum CPLD	Current CPLD
OS6860N-U28	2019.05.00.10	2019.05.00.11	12	12

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

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

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

OmniSwitch 6865 - AOS Release 8.8.56.R02 (GA)

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

1. FPGA versions 0.25 and 0.14 are optional for the fast and perpetual PoE feature support.
2. U-boot 8.7.2.R02 is optional to address eUSB issue CRAOS8X-13819.
3. Optional uboot update for CRAOS8X-24464, ability to disable/authenticate uboot access.
4. Optional uboot update to support boot from USB feature.

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

OmniSwitch 6900-X20/X40 - AOS Release 8.8.56.R02 (GA)

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

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

OmniSwitch 6900-T20/T40 - AOS Release 8.8.56.R02 (GA)

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

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
1. Optional uboot update for CRAOS8X-24464, ability to disable/authenticate uboot access.				

OmniSwitch 6900-Q32 - AOS Release 8.8.56.R02 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
CMM	7.3.4.277.R01	8.7.30.R03 ¹	0.1.8	0.1.8
1. Optional uboot update for CRAOS8X-24464, ability to disable/authenticate uboot access.				

OmniSwitch 6900-X72 - AOS Release 8.8.56.R02 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
CMM	7.3.4.31.R02	8.6.189.R02 ¹ 8.7.30.R03 ²	0.1.10	0.1.11 ¹
1. FPGA version 0.1.11 and U-boot version 8.6.189.R02 are optional to address CRAOS8X-11118. 2. Optional uboot update for CRAOS8X-24464, ability to disable/authenticate uboot access.				

OmniSwitch 6900-V72/C32/C32E - AOS Release 8.8.56.R02 (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 8.8.56.R02 (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 - 0x3 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 - 0x3 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

Hardware	Minimum ONIE	Current ONIE	Minimum CPLD	Current CPLD
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 8.8.56.R02 (GA)

Hardware	Minimum Coreboot-u-boot	Current Coreboot-u-boot	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 8.8.152.R01 ²	1.2.4	1.2.4 1.2.5 ²	0.9
OS99-GNI-P48	8.3.1.103.R01	8.3.1.103.R01 8.8.152.R01 ²	1.2.4	1.2.4 1.2.5 ²	0.9
OS99-XNI-48 (903753-90)	8.3.1.103.R01	8.3.1.103.R01 8.8.152.R01 ²	1.3.0	1.3.0 1.5.0 ²	0.6
OS99-XNI-48 (904049-90)	8.6.261.R01	8.6.261.R01 8.8.152.R01 ²	1.4.0	1.4.0 1.5.0 ²	0.7
OS99-XNI-U48 (903723-90)	8.3.1.103.R01	8.3.1.103.R01 8.8.152.R01 ²	2.9.0	2.9.0 2.11.0 ²	0.8
OS99-XNI-U48 (904047-90)	8.6.261.R01	8.6.261.R01 8.8.152.R01 ²	2.10.0	2.10.0 2.11.0 ²	0.8
OS99-GNI-U48	8.4.1.166.R01	8.4.1.166.R01 8.8.152.R01 ²	1.6.0	1.6.0 1.7.0 ²	0.2
OS99-CNI-U8	8.4.1.20.R03	8.4.1.20.R03 8.8.152.R01 ²	1.7	1.7 1.9 ²	N/A
OS99-XNI-P48Z16	8.4.1.20.R03	8.4.1.20.R03 8.8.152.R01 ²	1.4	1.4 1.6 ²	0.6
OS99-XNI-U24	8.5.76.R04	8.6.261.R01 8.8.152.R01 ²	1.0	2.9.0 2.11.0 ²	0.8
OS99-XNI-P24Z8	8.5.76.R04	8.6.261.R01 8.8.152.R01 ²	1.1	1.4.0 1.6.0 ²	0.7
OS99-XNI-U12Q	8.6.117.R01	8.6.117.R01 8.8.152.R01 ²	1.5.0	1.5.0 1.6.0 ²	N/A
OS99-XNI-UP24Q2	8.6.117.R01	8.6.117.R01 8.8.152.R01 ²	1.5.0	1.5.0 1.6.0 ²	N/A
1. Optional u-boot update for CRAOS8X-24464, ability to disable/authenticate u-boot access.					
2. Optional Uboot/FPGA update for future CMM2 and OS9912 compatibility.					

[IMPORTANT] *MUST READ*: AOS Release 8.8R2 Prerequisites and Deployment Information

General Information

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

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

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

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

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

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

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

Exceptions:

- Copper ports or ports with copper transceivers do not support faster convergence.
- OS6865-P16X and OS6865-U12X ports 3 and 4 do not support faster convergence.
- VFL ports do not support faster convergence.
- Splitter ports (i.e. 4X10G or 4X25G) do not support faster convergence.

- **MACsec Licensing Requirement**
Beginning in 8.6R1 the MACsec feature requires a site license, this license can be generated free of cost. After upgrading, the feature will be disabled until a license is installed. There is no reboot required after applying the license.
- **SHA-1 Algorithm - Chosen-prefix attacks against the SHA-1 algorithm are becoming easier for an attacker¹.** For this reason, we 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" Leurent, G and Peyrin, T (2020) <https://eprint.iacr.org/2020/014.pdf>

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

Deprecated Features / Functionality Changes

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

AOS Release 8.5R4
EVB - Beginning in 8.5R4, support for EVB is being removed. Any switches with an EVB configuration cannot be upgraded to 8.5R4 or above.
NTP - Beginning with AOS Release 8.5R4, OmniSwitches will not synchronize with an unsynchronized NTP server (stratum 16), as per the RFC standard. Existing installations where OmniSwitches are synchronizing from another OmniSwitch, or any other NTP server which is not synchronized with a valid NTP server, will not be able to synchronize their clocks. The following NTP commands have been deprecated: - ntp server synchronized - ntp server unsynchronized
AOS Release 8.6R1
DHCPv6 Guard - Configuration via an IPv6 interface name is deprecated in 8.6R1. Commands entered using the CLI must use the new 'ipv6 dhcp guard vlan vlan-id' format of the command. The old format will still be accepted if present in a vcboot.cfg to preserve backwards compatibility.
IP Helper - The 'ip helper' commands have been deprecated in 8.6R1 and replaced with 'ip dhcp relay'. The old format will still be accepted if present in a vcboot.cfg to preserve backwards compatibility.
SAA - The vlan-priority and drop-eligible parameters have been deprecated from all SAA commands beginning in 8.6R1.
MACsec is now supported on ports 33-48 of the 6560-(P)48X4. CRAOS8X-7910 was resolved in 8.6R1.

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

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 or 49/50) of the OS6360-PH24 or OS6360-PH48 models to operate at 10G speed. Ports support 1G by default.							
3. MACsec is supported on the OS6900-X48C4E.							

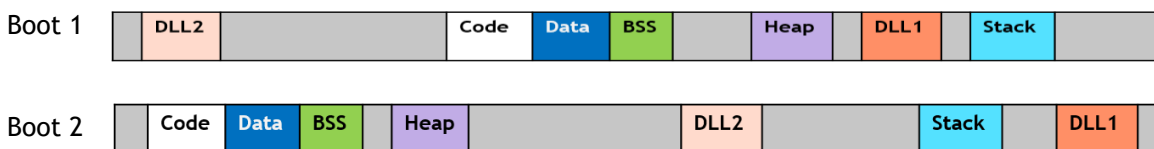
ALE Secure Diversified Code

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

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

Software Diversification

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



Please contact customer support for additional information.

New / Updated Hardware Support and Guidelines

The following new hardware is being introduced in this release.

OS6360-PH48

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

- Forty-six (46) - 10/100/1000Base-T PoE (802.3at) ports.
- Two (2) - 10/100/1000/2.5G PoE (802.3bt) ports.
- Two (2) - RJ45/SFP+ combo ports. (Default 1G, upgradeable to 10G)
- Two (2) - SFP+ software configurable ports:
 - Two (2) - SFP uplinks
 - Two (2) - SFP+ uplink or VFL ports
- Internal 950W AC power supply

Transceivers

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

- **3FE49327AA - XS-010S-Q,XGS PON ONT,1x10GE**
 - This transceiver is supported on the OS6360 and OS6560 SFP+ ports.

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.

8.8R2 New Feature/Enhancements Summary

Feature	Platform
Management Features	
AOS Support to Upgrade CPLD for ONIE-based Platforms	6860N, 6900-V72/C32/C32E/X48C6/T48C6/X48C4E/V48C8,
RMON Support	6860N, 6900-V72/C32/C32E/X48C6/T48C6/X48C4E/V48C8
QoS Features	
QoS - SP and WRR on Same Profile	6360, 6465
LPS - Prevent First Packet Loss	All
Service Features	
SPB - Increase the Adjacencies from 70 to 128	6860N, OS6900- V72/C32/C32E/X48C6/T48C6/X48C4E/V48C8, OS9900
Transparent Bridging Support	6860N

Management Features

AOS Support to Upgrade CPLD for ONIE-based Platforms

The CPLD for ONIE-based platforms can be upgraded using AOS commands.

The following CLI commands are associated with this feature:

- **update cpld-fpga cmm *chassis/cmm file filename***

RMON Support

RMON support has been added on the OS6860N and OS6900-V72/C32/C32E/X48C6/T48C6/X48C4E/V48C8 models in 8.8R2.

Qos Features

QoS - SP and WRR on Same Profile

AOS release 8.8R2 allows configuration of strict priority (SP) and WRR schedulers as part of same QoS QSP profile.

LPS - Reinject the First Packet of LPS to Forwarding Path

This feature is developed to avoid the packet loss due to LPS port learning. The feature will reinject the packets received from client back to the forwarding path. By default all the packets trapped on LPS port will be reinjected back to the switch once the MAC is successfully learned.

The feature can also be customized to filter and inject packets matching specific protocol types or UDP source and destination ports..

The following CLI commands are associated with this feature:

- **[no] port-security [port <c/s/p1[-p2]>] pkt-relay:** Enables packet relay feature on a single or range of LPS ports.
- **port-security pkt-relay protocol {udp} {icmp} {igmp}:** Configures the protocol filter criteria for packet relay feature.
- **port-security pkt-relay protocol {udp [src-port <port1[-port2]>}]:** Configures the UDP source ports as the criteria for packet relay.
- **port-security pkt-relay protocol {udp [dst-port <port1[-port2]>}]:** Configures the UDP destination ports as the criteria for packet relay.
- **show port-security port:** Displays the packet relay configuration on the port.
- **show port-security pkt-relay filter:** Displays the protocol filter configuration for LPS packet relay feature.

Service Related Features

SPB - Increase Number of Support Adjacencies

The number of supported adjacencies has been increased from 70 to 128 in 8.8R2.

Ethernet Service Transparent Bridging Support

Ethernet service transparent bridging is supported on the OS6860N beginning in 8.8R2.

The following CLI commands are associated with this feature:

- **ethernet-service transparent-bridging {enable | disable}**

Open Problem Reports and Feature Exceptions

The problems listed here include problems known at the time of the product's release.

System / General / Display

CR	Description	Workaround
CRAOS8X-28757	Telnet traffic when going through SPB network does not match DPI signatures.	There is no known workaround at this time.
CRAOS8X-32460	Host Agent messages not found in syslog even after retrying for 15 seconds after NI reset.	There is no known workaround at this time.
CRAOS8X-3877	Untagged packets are mirrored as tagged traffic when monitored port is across VC chassis. On standalone configuration monitored egress traffic is tagged.	Use port mirroring.

Hardware / Transceivers

CR	Description	Workaround
CRAOS8X-32089	Traffic Loss seen above 8 Gbps speed on the XS-010S-Q,XGS PON ONT,1x10GE transceiver (3FE49327AA).	There is no known workaround at this time.

QoS

PR	Description	Workaround
CRAOS8X-10498	"qos port 1/1/3 maximum ingress-bandwidth 80M" doesn't work after vc-takeover and reload. It gets overwritten by default ingress-bandwidth of a port.	Configure ingress-bandwidth through "interfaces port c/s/p ingress-bandwidth mbps <num> burst <num>" instead of "qos port c/s/p maximum ingress-bandwidth <num>".
CRAOS8X-4424	With color-only policy action configuration, egress queue is not honoring the color marking, packet drop is observed and expected traffic rate is not achieved.	There is no known workaround at this time.

Service Related

PR	Description	Workaround
CRAOS8X-30334	When configuring the 4K services an error message such as "service 27 bind-sdp 11 description dut2_sap27 => SDP Bind creation failure (11)" may be seen and configuration is not applied.	Issue is only seen when configuring 4K services. Rebooting and reconfiguring the services fixes the issue.
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.	Distribute SAPs across different ports.

	Seen with large amount of SAPs (>1K) configured on same port.	
--	---	--

Virtual Chassis

PR	Description	Workaround
CRAOS8X-32465	After switch does 2nd VC-takeover, it can't learn the DHCP binding entries immediately.	Switch has a delay of 20s before being able to learn the DHCP binding entries of DHCP packet with option 82.

Layer 2 / Multicast

PR	Description	Workaround
CRAOS8X-11084	Packet drop seen in BFD config when VRRP VLAN interface is toggled.	There is no known workaround at this time.
CRAOS8X-32090	Untagged traffic is not forwarded on a tagged port configured on ISAM side.	There is no known workaround at this time.
CRAOS8X-29130	Multicast traffic drop seen on an OS9900 when hash-control load-balance non-unicast is enabled.	There is no known workaround at this time.
CRAOS8X-27368	On an OS9900 when linkagg port is admin disabled, fdb flush is issued for that particular port which is resulting in flushing MACs on other fixed port which is unrelated to the linkagg.	There is no known workaround at this time.
CRAOS8X-7428	IPMS Proxy is not supported on a service.	There is no known workaround at this time.
CRAOS8X-23137	When high number of VLANs are mapped to DHL links then during failover we can see 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 few seconds in between toggling admin state (disable/enable) of bulk of VLANs.
CRAOS8X-26502	While converging due to a link/node failure in a MRP ring network, sometimes a very few multicast IGMP clients are not relearned with a lot of multicast streams (>200).	Clients will be relearned after the next query interval.

Layer 3

PR	Description	Workaround
----	-------------	------------

CRAOS8X-30910	OSPF packets are not transmitted when configured with 16 SPB services and 8 VRFs, OSPF neighborship is not formed.	Reloading the switch fixes the issue.
CRAOS8X-28291	There is no provision for the redundant broker to takeover master role once the AMS process on the current broker crashes and does not recover.	There is no work around at this time.

Hot-Swap/Redundancy Feature Guidelines

Hot-Swap Feature Guidelines

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

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

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

OS6860N-P48M Hot-Swap/Insertion Compatibility

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

OS6900 Hot-Swap/Insertion Compatibility

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

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

OS9900 Hot-Swap/Insertion Compatibility

Hot-Swap Procedure

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

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

VC Hot-Swap / Removal Guidelines

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

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

Fast/Perpetual PoE Unlike Power Supply Swapping

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

1. Disable fpoe and ppoe (Only needs to be executed if lanpower is started).
2. Save and synchronize the configuration.

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

Technical Support

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

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

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

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

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

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

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

Third Party Licenses and Notices

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

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

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

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

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

Appendix A: Feature Matrix

The following is a feature matrix for AOS Release 8.8R2.

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
BFD	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
BGP	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
DHCP Client / Server	8.7R2	8.6R1	Y	Y	8.7R1	Y	Y	8.5R4	8.7R1	Y

Feature	6360	6465	6560	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E	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	8.8R2	Y	Y	8.8R2	8.8R2	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
RoCEv2	N	N	N	N	N	N	N	8.7R2	N	N
Custom QSP Profiles	8.7R2	Y	Y	Y	Y	Y	X72 only (EA)	Y	Y	Y
GOOSE Messaging Prioritization	N	8.7R1	N	N	N	8.7R1	N	N	N	N
Metro Ethernet Features										
CPE Test Head	N	8.6R1	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	N	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

Feature	6360	6465	6560	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E	9900
EFM OAM / Link OAM (802.3ah)	N	8.6R1	8.6R1	8.5R4	8.7R2	8.5R4	N	N	N	N
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	8.8R2	8.7R2	N	N	N	N	N	N	N
1588v2 Across VC	N	N	N	N	N	N	8.5R2 (X72)	N	N	N
Access Guardian / Security Features										
802.1x Authentication	8.7R2	8.5R2	Y	Y	8.7R1	Y	Y	8.7R1	8.7R1	Y
Access Guardian - Bridge	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.6R1	8.7R1	Y
Access Guardian - Access	N	N	N	Y	8.7R1	Y	Y	8.5R4	8.7R1	Y
Application Fingerprinting	N	N	N	N	N	N	Y	N	N	N
Application Monitoring and Enforcement (Appmon)	N	N	N	Y	8.7R2	N	N	N	N	N
ARP Poisoning Protection	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	Y
BYOD - COA Extension support for RADIUS	8.7R2	Y	Y	Y	8.7R1	Y	8.62	8.6R2	8.7R1	Y
BYOD - mDNS Snooping/Relay	8.7R2	Y	Y	Y	8.7R1	Y	8.62	8.6R2	8.7R1	Y
BYOD - UPNP/DLNA Relay	8.7R2	Y	Y	Y	8.7R1	Y	8.62	8.6R2	8.7R1	Y
BYOD - Switch Port location information pass-through in RADIUS requests	8.7R2	Y	Y	Y	8.7R1	Y	8.62	8.6R2	8.7R1	Y
Captive Portal	8.7R2	8.5R4	Y	Y	8.7R1	Y	8.62	8.6R2	8.7R1	Y
IoT Device Profiling	8.7R2	8.5R2	8.5R2	8.5R2	8.7R1	8.5R2	8.5R2	8.6R1	8.7R1	8.5R2
IoT Device Profiling (IPv6)	8.7R2	8.7R1	8.7R1	8.7R1	N	8.7R1	8.7R1	N	N	8.7R1
Directed Broadcasts - Control	8.7R2	8.5R2	8.5R2	8.5R2	8.7R1	8.5R2	8.5R2	8.7R1	8.7R1	Y
Interface Violation Recovery	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.7R1	8.7R1	Y
Kerberos Snooping (services)	8.7R2	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

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

Feature	6360	6465	6560	6860(E)	6860N	6865	6900	6900- V72/ C32	6900- X48C6/ T48C6/X48C4E/V48C8/C32E	9900
FIP Snooping	N	N	N	N	N	N	Y	N	N	N
Notes: 1. OS6560 supports stub area only. 2. See protocol support table in Appendix C. 3. Not supported on 6900-T20/T40/X20/X40. 4. Site license required beginning in 8.6R1. 5. L2 head-end only on OS6900-V72/C32.										

Appendix B: MACsec Platform Support

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

MACsec Support (MACsec site license required)	
OmniSwitch 9900	
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
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 8.8R2 (GA)
OS6360	8.8.152.R01 (GA) 8.7.98.R03 (GA) 8.7.252.R02 (GA)
OS6465	8.8.152.R01 (GA) 8.7.98.R03 (GA) 8.7.252.R02 (GA) 8.7.354.R01 (GA) 8.7.280.R01 (MR) 8.7.277.R01 (GA)
OS6560	8.8.152.R01 (GA) 8.7.98.R03 (GA) 8.7.252.R02 (GA) 8.7.354.R01 (GA)
OS6860(E)	8.8.152.R01 (GA) 8.7.98.R03 (GA) 8.7.252.R02 (GA) 8.7.354.R01 (GA) 8.7.280.R01 (MR) 8.7.277.R01 (GA)
OS6860N*	8.8.153.R01 (GA)
OS6865	8.8.152.R01 (GA) 8.7.98.R03 (GA) 8.7.252.R02 (GA) 8.7.354.R01 (GA) 8.7.280.R01 (MR) 8.7.277.R01 (GA)
OS6900	8.8.152.R01 (GA) 8.7.98.R03 (GA) 8.7.252.R02 (GA) 8.7.354.R01 (GA) 8.7.280.R01 (MR) 8.7.277.R01 (GA)
OS6900-V72/C32/ X48C6/T48C6/X48C4E/V48C8*	8.8.153.R01 (GA) 8.8.152.R01 (GA)
OS9900	8.8.152.R01 (GA) 8.7.98.R03 (GA) 8.7.252.R02 (GA) 8.7.354.R01 (GA)
*ISSU is not supported to 8.8.R02 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.	

8.8R2 ISSU Supported Releases

Prerequisites

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

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

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

Switch Maintenance

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Appendix E: Standard Upgrade - OmniSwitch Standalone or Virtual Chassis

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

1. Download the Upgrade Files

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

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

2. FTP the Upgrade Files to the Switch

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

3. Upgrade the image file

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

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

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

4. Verify the Software Upgrade

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

```
OS6900-> show microcode
/flash/working
Package           Release           Size           Description
-----+-----+-----+-----
Tos.img           8.8.56.R02      239607692    Alcatel-Lucent OS
```

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

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

5. Certify the Software Upgrade

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

```
OS6900-> copy running certified

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

Appendix F: ISSU - OmniSwitch Chassis or Virtual Chassis

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

1. Download the Upgrade Files

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

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

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

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

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

3. Clean up existing ISSU directories

It is important to connect to the Slave chassis and verify that there is no existing directory with the path `/flash/issu_dir` on the Slave chassis. ISSU relies upon the switch to handle all of the file copying and directory creation on the Slave chassis. For this reason, having a pre-existing directory with the same name on the Slave chassis can have an adverse effect on the process. To verify that the Slave chassis does not have an existing directory of the same name as the ISSU directory on your Master chassis, use the internal VF-link IP address to connect to the Slave. In a multi-chassis VC, the internal IP addresses on the Virtual Fabric Link (VFL) always use the same IP addresses: 127.10.1.65 for Chassis 1, 127.10.2.65 for Chassis 2, etc. These addresses can be found by issuing the debug command `'debug show virtual-chassis connection'` as shown below:

```
OS6900-> debug show virtual-chassis connection
                Address                Address
Chas  MAC-Address      Local IP      Remote IP      Status
-----+-----+-----+-----+-----
1     e8:e7:32:b9:19:0b  127.10.2.65  127.10.1.65   Connected
```

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

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

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

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

6. Log out of the Slave chassis:

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

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

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

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

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

9. Upgrade the image files using ISSU:

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

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

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

This indicates that the ISSU is completed

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

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

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

10. Verify the Software Upgrade

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

```
OS6900-> show microcode
/flash/working
Package      Release      Size      Description
-----+-----+-----+-----
Tos.img      8.8.56.R02  239607692 Alcatel-Lucent OS
```

11. Certify the Software Upgrade

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

```
OS6900-> copy running certified

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

Appendix G: FPGA / U-boot Upgrade Procedure

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

CR / Feature	Summary	
CRAOS8X-12042	Description	Switch does not shutdown after crossing danger threshold temperature.
	FPGA Version	0.7
	Platforms	OS6465-P28
CRAOS8X-7207	Description	Chassis reboots twice to join a VC.
	FPGA Version	0.7
	Platforms	OS6560-P24Z24,P24Z8,P48Z16 (903954-90)
CRAOS8X-4150	Description	VC LED status behavior.
	U-boot Version	0.12
	Platforms	OS6865-U28X
8.7R1 Release		
CRAOS8X-16452	Description	Port remains UP when only SFP is connected.
	FPGA Version	- 0.6 (OS6560-P48Z16 (904044-90)) - 0.7 (OS6560-48X4, OS6560-P48X4) - 0.8 (OS6560-X10)
	Platforms	OS6560-P48Z16 (904044-90), OS6560-48X4, OS6560-P48X4, OS6560-X10
CRAOS8X-11118	Description	1000BaseT SFP interface up before system ready
	U-boot/FPGA Version	- U-boot version 8.6.R02.189 - FPGA version 0.1.11
	Platforms	OS6900-X72
Fast/Perpetual PoE	Description	Fast and Perpetual PoE Support
	FPGA Version	0.7 (OS6860E-P24Z8) 0.10 0.14 (OS6865-U28X) 0.25 (OS6865-P16X/U12X)
	Platforms	OS6860/OS6865
8.7R2 Release		
CRAOS8X-4813/13440	Description	Uboot unable to mount NAND flash with UBIFS errors
	U-boot Version	8.7.2.R02
	Platforms	OS6465(T), 6560-24X4/P24X4/48X4/P48X4/X10
CRAOS8X-13819	Description	Uboot unable to mount eUSB flash
	U-boot Version	8.7.2.R02
	Platforms	OS6560-24Z24/P24Z24/24Z8/P24Z8/P48Z16 (all PNs), 6865
CRAOS8X-22857	Description	OS6560-P24Z24 reloads continuously with pmuds
	FPGA Version	0.8
	Platforms	OS6560-24Z24/P24Z24/24Z8/P24Z8/P48Z16 (903954-90)
1588v2 Support	Description	1588v2 Support
	FPGA Version	0.7 (OS6560-P48Z16 (904044-90)) 0.8 (OS6560-48X4/P48X4)
	Platforms	OS6560-48X4/P48X4/P48Z16(904044-90)

U-boot Password Authentication	Description	U-boot password support (Early Availability)
	U-boot Version	8.7.2.R02
	Platforms	OS6465
8.7R3 Release		
CRAOS8X-26370 CRAOS8X-25033	Description	Required upgrade to enable 12V Power Fail Interrupt (CRAOS8X-26370). Required upgrade to address fan speed issue. (CRAOS8X-25033)
	FPGA Version	0.17
	Platforms	OS6360-24/P24/48/P48
CRAOS8X-24464	Description	Uboot update for CRAOS8X-24464, ability to disable / authenticate uboot access.
	Uboot Version	8.7.30.R03
	Platforms	OS6360, 6465, 6560, 6860, 6865, 6900, 9900. (Not applicable for platforms that use ONIE)
8.8R1 Release		
Boot from USB	Description	Uboot update to allow switch to boot from USB.
	Uboot Version	8.7.33.R01
	Platforms	OS6465, OS6865
8.8R2 Release		
Future compatibility	Description	Uboot/FPGA update to allow future CMM2/OS9912 NI compatibility.
	Uboot/FPGA Versions	See OS9900 Table for versions.
	Platforms	9907

Note: AOS must be upgraded prior to performing an FPGA/CPLD or U-boot upgrade.

1. Download and extract the upgrade archive from the Service & Support website. In addition to the AOS images, the archive will also contain an FPGA upgrade kit and U-boot file, for example.

- CPLD File - fpga_kit_7715
- U-boot.8.8.R01.152.tar.gz

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

3. Enter the following to upgrade the FPGA. The ‘all’ parameter should be used when upgrading with an FPGA kit. Additionally, this will update all the elements of a VC, for example:

```
-> update fpga-cpld cmm all file fpga_kit_7715
Parse /flash/fpga_kit_7715
fpga file: OS6900-X72_CPLD_V01B_20191204.vme
Please wait...
fpga file: OS6900-X72_CPLD_V01B_20191204.vme
update chassis 1
Starting CMM ALL FPGA Upgrade
CMM 1/1
Successfully updated
Reload required to activate new firmware.
```

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

```
-> update uboot cmm all file /flash/u-boot.8.8.R02.15.tar.gz
Starting CMM ALL UBOOT Upgrade
Please wait...
```



```
CMM 1/1
u-boot-ppc_2040.bin: OK
U-boot successfully updated
Successfully updated
```

5. Once complete, a reboot is required.

Appendix H: CPLD Upgrade Procedure for ONIE-Based Devices

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

CR / Feature	Summary	
8.8R2 Release		
CRAOS8X-29731/30471	Description	OS6860N power supplies
	CPLD Version	os6860n_p48m_p48z_u28_maincpu_20220318.updater os6860n_p24m_p24z_cpu_mainboard_cpld_22020105.updater
	Platforms	OS6860N-P48M/P48Z/P24M/P24Z
Note: CPLD versions are compatible with previous AOS releases. Downgrading to a previous AOS release is supported.		

Note: AOS must be upgraded prior to performing an 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 a CPLD upgrade file, for example.

- CPLD File - *.updater

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





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







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






4. Once complete, a reboot is required.






Appendix I: Fixed Problem Reports



The following problem reports were closed in this release.

CR/PR NUMBER	Description
Case: 00578886 CRAOS8X-30860	Summary: An issue with IP interface DHCP-Client Lease time in OS6360 and OS6560 switches. Explanation: The DHCP server (windows server) associated Lease time of 7 days, but the Lease time went up to max (49.710 days) in switch without any changes from the DHCP Server. This issue has been fixed under AOS 8.8 R02 GA.  Click for Additional Information
Case: 00594210 00604389 CRAOS8X-31709	Summary: 10G non-ALE DAC not working on OS6900-V48C6 model Explanation: 10G HP and ALU DAC does not come UP on OS6900-V48C6. The same DAC works on OS6900-X20/40 model and other ALE model switches.  Click for Additional Information
Case: 00591801 CRAOS8X-31471	Summary: OS6560: Empty ports [No SFP connected] are flapping. Explanation: In linkscan thread, link status will be done periodically. In the link status get, autotune does happen. Autotune takes place when the SFP is present, and the link is not up. Autotune should not happen, when there are no SFPs. This issue is generic to all OS6560 models and is applicable to all Phyless ports. Phyless ports in the following models: OS6560-P24X4/OS6560-24X4: Port 25-30 OS6560-P48X4/OS6560-48X4: Port 49-54 The solution is to exclude Auto-tune change for ports without SFP and link.  Click for Additional Information
Case: 00609479 00597667 CRAOS8X-31767	Summary: When doing SNMP Walk on every MIBs we observe lot of SNMP aluSubAgent Errors: Explanation: "swlogd SNMP aluSubagent_main ERR: mip_lib: mip_write_table: No sub-system registered this table..." error messages are continuously seen on a switch after upgrading to AOS 8.8.152.R01, such as: "swlogd SNMP aluSubagent_main ERR: mip_lib: mip_write_table: No sub-system registered this table(138254)pimInterfaceTable". This issue will be fixed as from AOS 8.8.R02.  Click for Additional Information
Case: 00598025 CRAOS8X-31822	Summary: lpCmm LanCmmMip INFO, ERR & WARN messages are filling up the switch logs. Explanation: These logs are seen when SNMP operation like snmpwalk is performed on the 'PETHPSEPORTTABLE'. Code changes have been made to limit the logging of these messages during snmpwalk and the fix will be available from AOS 8.8 R02 GA.

	<p> Click for Additional Information</p>
<p>Case: 00593976 00607107 CRAOS8X-31574</p>	<p>Summary: LED status of auto VFL Ports on OS6360 struck in orange/amber even if they are used as data ports (Uplink port).</p> <p>Explanation: According to the hardware specifications guide if the VFL port is used for auto virtual chassis formation it should be amber and if the port is used as a data port the LED status should be green but, the LED status is in amber for VFL ports even when it is used as a data port. Changes have been made to the mapping of LED registers, which requires updating the FPGA to fix the issue.</p> <p> Click for Additional Information</p>
<p>Case: 00581292 CRAOS8X-31070</p>	<p>Summary: Switch OS6900 is not taking the longest prefix route as the best path. Instead, the switch is selecting the old path as best.</p> <p>Explanation: When the static route is configured in the switch it gets added but it does not remove previously learned ARP. The fix is available in 8.8R2.</p> <p> Click for Additional Information</p>
<p>Case: 00603956 00609057 CRAOS8X-32121</p>	<p>Summary: Unable to upgrade OS6900 switches to 8.8.152.R01 if an empty expansion slot is present.</p> <p>Explanation: When the OS6900 switch is upgraded from the older version to 8.8.152 the expansion slot numbers are not correctly updated. Fix is available in 8.8.R02.</p> <p> Click for Additional Information</p>
<p>Case: 00600859 00602421 00600916 CRAOS8X-31931</p>	<p>Summary: Kernel crash logs are not logged in swlog in OS6865 switches.</p> <p>Explanation: When an OS6865 switch reboots or crashes due to kernel-level issues, the traces are not logged in swlog. The logs are missing for 5-6 minutes before reboot. Sometimes the NULL characters are seen before reboot. This affects the ability to find the exact cause of the kernel crash.</p> <p>An enhancement is done in 8.8.R02 to dump the kernel level issues in the swlog after reboot.</p> <p> Click for Additional Information</p>
<p>Case: 00597107 CRAOS8X-31796</p>	<p>Summary: Traffic is not forwarded on ports after the uucast flood-limit violation is cleared.</p> <p>Explanation: When the uucast flood-limit violation is cleared on the port, the port comes UP however the VLAN status on the port is inactive.</p> <p>This is the reason the port drops the traffic even though the port is UP, and mac is learned on the port. This is a bug as the portmgr does not update the vlanmgr after the port is recovered. This issue is seen only when the unknown unicast flood limit is crossed.</p> <p>The Broadcast and Multicast flood-limit violation works as expected.</p> <p> Click for Additional Information</p>
<p>Case: 0055522 CRAOS8X-27954</p>	<p>Summary: OS6560:SSH/Telnet not working if Unit 1 member of the linkagg change state to DOWN.</p> <p>Explanation:</p>

	<p>When the switch comes up with no ip interface having forwarding option enabled global router mac source address is not set which cause the failure of SSH and Telnet connections when the linkagg member from master unit is down.</p> <p> Click for Additional Information</p>
<p>Case: 00498279 CRAOS8X-22492</p>	<p>Summary: AOS 8.x default/enhanced modes, when configuring user SSH access read-write, telnet and http/https are also allowed to the user.</p> <p>Explanation: Conflict in the family was allowing to a user that have only SSH read-write rights to telnet as well as HTTP/HTTPS to the switch, 8.8R02 is fixing this conflict.</p> <p> Click for Additional Information</p>
<p>Case: 00587566 CRAOS8X-31307</p>	<p>Summary: PTP E2E is supported on all ports including SFP ports of the OS6465-P12 and OS6465T-P12.</p> <p>Explanation: PTP SFP ports are supported on switches OS6465-P12 and OS6465T-P12 however only E2E mode is supported for these platforms.</p> <p> Click for Additional Information</p>
<p>Case: 00541205 CRAOS8X-27074</p>	<p>Summary: EMP not reachable after remote connected to it is restarted. A note is printed in the release note explaining this limitation.</p> <p>Explanation: When the peer switch connected to EMP is restarted a negotiation mismatch is happening, this causing the EMP to receive/send traffic correctly, this is a limitation and the workaround is to disable then enable the remote end connected to EMP.</p> <p> Click for Additional Information</p>
<p>Case: 00585942 CRAOS8X-31225</p>	<p>Summary: 100MB full duplex Links, using SFP-GIG-T , on OS6860-U28 remain down after a reload.</p> <p>Explanation: The problem happening only for some specific devices is a timing issue with I2C communication trying to happen even if the Low level configuration of the Link is not complete yet.</p> <p>This behavior was observed in 87R01, 87R02 or 88R01 releases.</p> <p> Click for Additional Information</p>
<p>Case: 00599654 CRAOS8X-31887</p>	<p>Summary: 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 reenabled after approximately 20 seconds.</p> <p>Explanation: The issue can be seen on all AT only (non IEEE802.3bt) platforms which use 2.11 firmware: OS6360-P24/P48, OS6465, OS6560, OS6860/E, OS6865, and OS9900.</p> <p>OS6860N and OS6360-WNC platforms using 3.52 BT firmware, are not affected.</p> <p>This behavior was observed in 88R01 release.</p>

	<p>Work-around: The only workaround is to enable “lanpower capacitor-detection” on the port and then execute “lanpower admin-state disable” on the port.</p> <p> Click for Additional Information</p>
<p>Case: 00582050 CRAOS8X-31071</p>	<p>Summary: Uplink linkagg port down trap not seen by the NMS.</p> <p>Explanation: OS6860E-24 VC of 2 configured with linkagg size 2 with 1/1/27 and 2/1/27.</p> <p>While making the lacp port 1/1/27 toggle, the switch is sending SNMP traps for link down but not for lacp leave.</p> <p>Issue has been fixed under AOS 8.8 R02 GA.</p> <p> Click for Additional Information</p>
<p>Case: 00586334 00600458 00606875 CRAOS8X-31942</p>	<p>Summary: AOS 8.8R01 / AWOS 4.0.4 Stellar AP and OV 4.6R02 - no link displayed on topology map.</p> <p>Explanation: On OV running 4.6R02 or 4.6R01, link is not displayed between AOS 8.8R01 OmniSwitches and Stellar APs AWOS 4.0.4 or AWOS 4.0.3</p> <p>No issue if OmniSwitch is running AOS 6.x</p> <p>2 different behaviors:</p> <ul style="list-style-type: none"> - Link is not displayed at all - Link is displayed and after a discovery it disappears. <p> Click for Additional Information</p>
<p>Case: 00607190 CRAOS8X-32419</p>	<p>Summary: OS9900-OS99-CNI-U8: After reload FEC value changes from DISABLE to AUTO.</p> <p>Explanation: FEC value is disabled in the vcboot.cfg. However, after reload, the FEC status changes to AUTO. The issue is seen on OS99-CNI-U8.</p> <p> Click for Additional Information</p>
<p>Case: 00595257 CRAOS8X-31759</p>	<p>Summary: SPB In-Band Management Route cannot Redistribution more than 32 routes.</p> <p>Explanation: There are more than 32 routes present in the SPB In-Band, however only 32 routes are sent out on the ISIS-TLV to the ISIS neighbors. There is an issue on AOS implementation of SPB-MGMT routes redistribution that uses TLV 135. The old AOS only opens the first TLV 135 and does not check another TLV if exists.</p> <p> Click for Additional Information</p>
<p>Case: 00574365 CRAOS8X-29731</p>	<p>Summary: The AP is connected to the OS6860N-P48 switch and noticed the APs are rebooting randomly. Noticed "the power budget exceeded" from log messages in the switch but have enough power. "swlogd lpNi LanNi INFO: Port 33 FAULT State change 85 to 20 desc: Port is off: Power budget exceeded."</p> <p>Explanation: The issue is caused by the 6860N P48M Power supply CPLD firmware that set the wrongly power bank to 0 and cause all PDs to get unpowered. A new cpld upgrade will solve the problem.</p>

	 Click for Additional Information
Case: 00597885 CRAOS8X-31851	Summary: OS6860N: Devices over VXLAN using OS6860N can't ping to each other. Explanation: ARP was not populated due to an 802.1Q bug in the uplink port of a VXLAN when making 802.1Q configuration changes.  Click for Additional Information

Appendix J: Installing/Removing Packages

The package manager provides a generic infrastructure to install AOS or non-AOS third party Debian packages and patches. The following packages are supported in 8.7R3. The package files are kept in the `flash/working/pkg` directory or can be downloaded from the Service & Support website.

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

Installing Packages

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

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

Legend: (+) indicates package is not saved across reboot
 (*) indicates packages will be installed or removed after reload

Name	Version	Status	Install Script
ams	default	installed	default
ams-apps	default	installed	default
mrp	8.7.R03-xxx	installed	

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

Removing Packages

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

```
-> pkgmgr remove mrp
Purging mrp (8.7.R03-xxx)...
Removing package mrp.. OK
Write memory is required complete package mrp removal
```

```
-> write memory
Package(s) Committed
```

```
-> show pkgmgr
```

Legend: (+) indicates package is not saved across reboot
 (*) indicates packages will be installed or removed after reload

Name	Version	Status	Install Script
ams	default	installed	default
ams-apps	default	installed	default

mrp	8.7.R03-xxx	removed
-----	-------------	---------

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

Remove the Debian package installation file. For example:

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

AOS Upgrade with Encrypted Passwords

AMS

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

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

IoT-Profiler

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

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