

Release Notes - Rev. B

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

Release 8.7R3

These release notes accompany release 8.7R3. 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 8.7R3 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 18

Hot-Swap/Redundancy Feature Guidelines 22

Technical Support 25

Appendix A: Feature Matrix 26

Appendix B: SPB L3 VPN-Lite Service-based (Inline Routing) / External Loopback Support / BVLAN Guidelines 34

Appendix C: General Upgrade Requirements and Best Practices 37

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

Appendix E: ISSU - OmniSwitch Chassis or Virtual Chassis 44

Appendix F: FPGA / U-boot Upgrade Procedure 47

Appendix G: OS6900-V72/C32 Flash Cleanup Procedure / FEC Disable 49

Appendix H: Fixed Problem Reports 50

Appendix I: Installing/Removing Packages 54

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-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 8.7.98.R03 (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
OS6360-P24X	8.7.149.R02	8.7.30.R03 ²	0.12	0.12

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

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

OmniSwitch 6465 - AOS Release 8.7.98.R03 (GA)

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

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.

OmniSwitch 6560 - AOS Release 8.7.98.R03 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6560-24Z24	8.5.22.R01	8.7.2.R02 ³ 8.7.30.R03 ⁷	0.7	0.8 ⁵
OS6560-P24Z24	8.4.1.23.R02	8.7.2.R02 ³ 8.7.30.R03 ⁷	0.6	0.7 ¹ 0.8 ⁵
OS6560-24Z8	8.5.22.R01	8.7.2.R02 ³ 8.7.30.R03 ⁷	0.7	0.8 ⁵
OS6560-P24Z8	8.4.1.23.R02	8.7.2.R02 ³ 8.7.30.R03 ⁷	0.6	0.7 ¹ 0.8 ⁵
OS6560-24X4	8.5.89.R02	8.7.2.R02 ⁴ 8.7.30.R03 ⁷	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

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6560-P48Z16 (904044-90)	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 8.7.98.R03 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6860/OS6860E (except U28/P24Z8)	8.1.1.70.R01	8.7.30.R03 ²	0.9	0.10 ¹
OS6860E-U28	8.1.1.70.R01	8.7.30.R03 ²	0.2	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 8.7.98.R03 (GA)

Hardware	Minimum ONIE	Current ONIE	Minimum FPGA	Current FPGA
OS6860N-U28	2019.05.00.10	2019.05.00.10	12	12
OS6860N-P48Z			12	12
OS6860N-P48M			11	11

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

OmniSwitch 6865 - AOS Release 8.7.98.R03 (GA)

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

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6865-U28X	8.4.1.17.R01	8.7.2.R02 ² 8.7.30.R03 ³	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. Note: CRAOS8X-4150 for the OS6865-U28X was fixed with FPGA version 0.12 and higher.				

OmniSwitch 6900-X20/X40 - AOS Release 8.7.98.R03 (GA)

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

OmniSwitch 6900-T20/T40 - AOS Release 8.7.98.R03 (GA)

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

OmniSwitch 6900-Q32 - AOS Release 8.7.98.R03 (GA)

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

OmniSwitch 6900-X72 - AOS Release 8.7.98.R03 (GA)

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

OmniSwitch 6900-V72/C32 - AOS Release 8.7.98.R03 (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

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

OmniSwitch 6900-X48C6/T48C6/X48C4E/V48C8- AOS Release 8.7.98.R03 (GA)

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

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

OmniSwitch 9900 - AOS Release 8.7.98.R03 (GA)

Hardware	Minimum Coreboot-uboot	Current Coreboot-uboot	Minimum Control FPGA	Current Control FPGA	Minimum/Current Power FPGA
OS99-CMM	8.3.1.103.R01	8.3.1.103.R01 8.7.30.R03 ¹	2.3.0	2.3.0	0.8
OS9907-CFM	8.3.1.103.R01	8.3.1.103.R01	-	-	-
OS99-GNI-48	8.3.1.103.R01	8.3.1.103.R01	1.2.4	1.2.4	0.9
OS99-GNI-P48	8.3.1.103.R01	8.3.1.103.R01	1.2.4	1.2.4	0.9
OS99-XNI-48 (903753-90)	8.3.1.103.R01	8.3.1.103.R01	1.3.0	1.3.0	0.6
OS99-XNI-48 (904049-90)	8.6.261.R01	8.6.261.R01	1.4.0	1.4.0	0.7
OS99-XNI-U48 (903723-90)	8.3.1.103.R01	8.3.1.103.R01	2.9.0	2.9.0	0.8

Hardware	Minimum Coreboot-u-boot	Current Coreboot-u-boot	Mimimun Control FPGA	Current Control FPGA	Minimum/ Current Power FPGA
OS99-XNI-U48 (904047-90)	8.6.261.R01	8.6.261.R01	2.10.0	2.10.0	0.8
OS99-GNI-U48	8.4.1.166.R01	8.4.1.166.R01	0.3.0	0.3.0	0.2
OS99-CNI-U8	8.4.1.20.R03	8.4.1.20.R03	1.7	1.7	N/A
OS99-XNI-P48Z16	8.4.1.20.R03	8.4.1.20.R03	1.4	1.4	0.6
OS99-XNI-U24	8.5.76.R04	8.6.261.R01	1.0	2.9.0	0.8
OS99-XNI-P24Z8	8.5.76.R04	8.6.261.R01	1.1	1.4.0	0.7
OS99-XNI-U12Q	8.6.117.R01	8.6.117.R01	1.5.0	1.5.0	N/A
OS99-XNI-UP24Q2	8.6.117.R01	8.6.117.R01	1.5.0	1.5.0	N/A
1. Optional u-boot update for CRAOS8X-24464, ability to disable/authenticate u-boot access.					

[IMPORTANT] *MUST READ*: AOS Release 8.7R3 Prerequisites and Deployment Information

General Information

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

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

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

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

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

Note: OS6560-P48Z16 (904044-90) - 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 B for additional information.
AOS Release 8.7R2
There are new default user password polices being implemented in 8.7R2. This change does not affect existing users. <ul style="list-style-type: none"> - cannot-contain-username: enable - min-uppercase: 1 - min-lowercase: 1 - min-digit: 1 - min-nonalpha: 1
The OmniSwitch 6360 does not contain a real-time clock. <ul style="list-style-type: none"> - It is recommended to use NTP to ensure time synchronization on OS6360s. - When the switch is reset, the switch will boot up from an approximation of the last known good time. - When the switch is powered off it cannot detect the time left in the powered off state. When it boots up it will have the same time as when the switch was last powered off.
AOS Release 8.7R3
The Kerberos Snooping is not supported in bridge mode in this release. <ul style="list-style-type: none"> - A new interfaces port break-out enable command has been introduced for splitter transceiver support on the OS6900-X48C6/T48C6 models. Other models continue to use interfaces primary-port split-mode.

Licensed Features

The table below lists the 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: All other platforms, including the OS6900-V72/C32, do not support these Data Center features.	

	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
<p>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.</p> <p>2. Performance software license is optional allowing the 2 RJ45/SFP+ combo ports (25/26) of the OS6360-PH24 model to operate at 10G speed. Ports support 1G by default.</p> <p>3. MACsec is supported on the OS6900-X48C4E.</p>							

ALE Secure Diversified Code

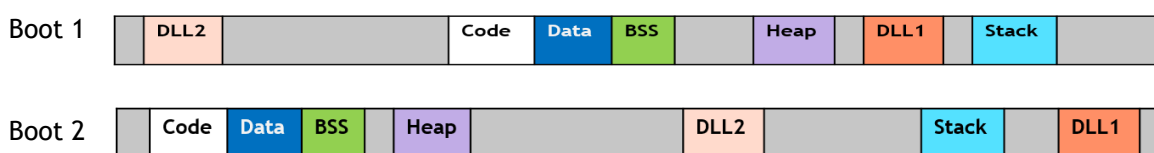
Alcatel-Lucent Enterprise provides network equipment that is hardened in conjunction with an independent 3rd party organization. ALE secure diversified code promotes security and assurance at the network device level using independent verification and validation of source code and software diversification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

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

Software Diversification

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

ASLR



Please contact customer support for additional information.

New / Updated Hardware Support and Guidelines

The following new hardware is being introduced in this release.

OS6900-V48C8

Fixed configuration chassis in a 1U form factor with:

- 48 x SFP28 ports
- 8 x QSFP28 ports
- 2 x SFP+ ports (Currently not functional)
- USB port
- RJ-45 console port
- EMP port
- Front-to-rear or rear-to-front cooling
- AC or DC power supply
- **Note:** The OS6900-V48C8 doesn't support a mix of 1G/10G and 25G speeds on the 4-port groups of ports 1-48 listed below. Mixing 1G and 10G speeds is supported.

the same color-coded ports must operate at the same speed				the same color-coded ports must operate at the same speed				the same color-coded ports must operate at the same speed				the same color-coded ports must operate at the same speed			
1	4	7	10	13	16	19	22	25	28	31	34	37	40	43	46
2	5	8	11	14	17	20	23	26	29	32	35	38	41	44	47
3	6	9	12	15	18	21	24	27	30	33	36	39	42	45	48

Front Panel Ports 1-48 Representation

Transceivers and Guidelines

The following transceiver support and guidelines have been added in the release. Please refer to the Transceivers and Hardware Guides for additional information.

- Splitter transceiver support is added to the 6900-X/T48C6 for the following transceivers:
 - QSFP-4X10G-SR, QSFP-4X10G-C, QSFP-4X25G-C
 - Uses the new **interfaces port break-out enable** command.

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.

8.7R3 New Feature/Enhancements Summary

Feature	Platform
Package Manager Changes	All
Enable/Disable Uboot Access	6360, 6465, 6560, 6860(E), 6865, 6900 (except 6900-V72/C32/X48C6/T48C6/X48C4E/V48C8), 9900
NTP Over IPv6	All
TACACS+ Over IPv6	All
Increase auth-server down timer	All
SPB Inline Routing	OS6900-X48C4E

Management / NMS Related Features

Package Manager Changes

In 8.7R3 the package manager version name is changed to version number. For example: *uos-ams-v1.deb*. Here v1 is version 1. The version number is increased every time there is a change in functionality or a new feature is included in the package. For example: *uos-ams-v1.deb*, *uos-ams-v2.deb* etc. The package manager verify command is enhanced to verify and provide the version compatibility information for the release.

- The package manager CLI commands are now part of the system partition manager family.
- The OmniSwitch allows running of cron configuration files. The cron configuration file stores time-based jobs that need to be run. The file is located at `/flash/<working_dir>/pkg/ams` folder in the switch. All scheduled jobs are stored in crontab format which is used to timely run the job. The jobs can be prepared and saved as `cron.cfg` and the config file can be replaced with default config file in AMS pkg directory.

The following CLI commands are associated with this feature:

- **pkgmgr verify**

Enable/Disable Uboot Access

The AOS bootloader (uboot) provides access to system parameters, with which boot images and system variables can be manipulated by any user having physical/console access to the switch, which can cause security related issues.

With this feature, an option is provided to disable access to uboot shell. When the option is disabled, any key-press at AOS boot does not allow access to the uboot shell. AOS images are booted with the pre-set parameters.

When the Uboot access is enabled, Uboot shell can be accessed with any key-press at AOS boot.

The following CLI commands are associated with this feature:

- **uboot access {enable | disable}**
- **show uboot config**

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

Allow Uboot Shell Access after Authenticating with Password

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

The following CLI commands are associated with this feature:

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

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

Note: U-boot Access/Authentication feature is supported from release 8.7R03 onwards. To enable U-boot Access/Authentication, U-boot needs to be upgraded to the latest version. Refer to the [Upgrade Instructions](#) for version information. In case of AOS image downgrade, U-boot Access/Authentication configurations needs to be restored to the default values before downgrade.

NTP Over IPv6

In 8.7R3 NTP is enabled to support IPv6. Both IPv4 and IPv6 addresses could be used at the same time to configure the NTP service on the switches. NTP broadcast is limited to IPv4 since IPv6 does not support broadcast addresses and NTP module currently does not support multicast addresses.

The NTP service source IP CLI is also currently limited to IPv4. When an IPv6 NTP server is configured as an NTP time source for the switch, all the outgoing NTP packets sent to that server will have the source IP address selected by the NTP algorithm based on the kernel routing table.

The following CLI commands are associated with this feature:

- **ntp server** {ip_address | server_name} [key key_id | | minpoll poll | maxpoll poll | version version | prefer | burst | iburst | preempt]
- **no ntp server** ip_address
- **ntp peer** {ip_address | server_name} [key key_id | | minpoll poll | maxpoll poll | version version]
- **no ntp peer** {ip_address }
- **ntp interface** {interface_ip} {enable | disable}
- **show ntp server status** [ip_address]

TACACS+ Over IPv6

In 8.7R3 TACACS+ is enabled to support IPv6 TACACS servers. This will allow authentication of IPv6 enabled TACACS+ clients.

- TACAS authentication is not allowed on slave console on a VC. Only local admin user on slave or secondary console can authenticate through TELNET access.
- System command supports only partition manager family based authorization.
- WebView supports only partition manager family based authorization.

The following CLI commands are associated with this feature:

- **aaa tacacs+-server** server_name host {hostname | ip_address | ipv6_address1} [hostname2 | ip_address2 | ipv6_address2] {key secret | prompt-key} [salt salt | hash-salt hash_salt] [timeout seconds] [port port] [vrf-name name]

Increase Auth-server Down Timer

In 8.7R3 the authentication server down timer range is increased to 43200 seconds from 1000 seconds.

The following CLI commands are associated with this feature:

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

SPB Inline Routing

The OS6900-X48C4E supports inline routing beginning in 8.7R3. This was an EA feature in 8.7R2.

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-28229	A memory leak may occur in the dpcmm task if the number of UNP users on a VC is more than 1000 and device profiling is enabled.	Disable device profiling is not required.
CRAOS8X-24299	After upgrading the switch the OSPF Area Border router (ABR) stopped generating the default route for NSSA area.	Remove and re-apply the default metric for the nssa area.
CRAOS8X-27368	On an OS9900 when linkagg port is admin disabled, fdb flush is issued for that particular port which is resulting in flushing MAC on other fixed port which is unrelated to the linkagg.	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-28077	The Kerberos Snooping is not supported in bridge mode in this release.	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-23545	A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance and even could impact management connectivity to the device. The traffic storm control feature supported in AOS, prevents LAN ports from being disrupted by a broadcast, multicast or unicast traffic storm on physical interfaces.	Use the interfaces flood-limit command to configure the flood rate settings on a single port, a range of ports, or an entire Network Interface (NI). Use the interfaces flood-limit action command to configure the action on a single port, a range of ports, when the port reaches the storm violated state.

Hardware / Transceivers

CR	Description	Workaround
CRAOS8X-26489	On an 9900-XNI-U48, when an SFP-10G-SR is hot-swapped with an SFP-GIG-T transceiver, traffic continues to flow but LED remains off.	There is no known workaround at this time.
CRAOS8X-26236	On OS6900-X48C6/T48C6/X48C4E and OS6860N models fast hot-swaps of some transceivers can cause the switch not to detect the transceiver.	It's recommended to wait approximately 10 seconds between removal and installation of transceiver.
CRAOS8X-24676	On an OS6900-X48C6/X48C4E "bcmcmd esm ERR" error messages are seen when inserting or removing an SFP-10G-T transceiver.	There is no known workaround at this time. This is a display issue only.
CRAOS8X-26560	When both 1G and 25G are inserted in the same port group and the 25G has link, removal of the 25G transceiver should link up the 1G. However, the 1G stays down. The 1G will link up upon a hot-swap.	There is no known workaround at this time.

Layer 2 / Multicast

PR	Description	Workaround
CRAOS8X-20826	On an OS6900, multicast packets are received on nack port after changing the active RP to different interface.	There is no known workaround at this time.
CRAOS8X-11084	Packet drop seen in BFD config when VRRP VLAN interface is toggled.	There is no known workaround at this time.
CRAOS8X-26502	While converging due to a link/node failure in a MRP ring network, sometimes the very few multicast IGMP clients are not relearned with lot of multicast streams(>200). Clients will be relearned after the next query interval.	There is no known workaround at this time.

QoS

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

CRAOS8X-4424	With color-only policy action configuration, Egress queue are not honour the colour marking and packets drop is observed and expected traffic rate is not achieved.	There is no known workaround at this time.
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>".

Service Related

PR	Description	Workaround
CRAOS8X-12513	When 2048 IGMP groups were sent over SPB service, only 1025 IGMP groups were received with 1024 SAPs per service configured on the edge switch. Seen with large amount of SAPs (>1K) configured on same port.	Distribute SAPs across different ports.
CRAOS8X-27773	CPE test head process can restart/crash if test is started and stopped within few seconds	It is advised not to stop the test for atleast 5 seconds after test start command is executed.
CRAOS8X-26113	After configuring the MVRP on port for learning 2.5k vlans, when the port is added as NNI port and transparent bridging is being enabled, without any time gap. Because of this an internal conflict is observed between NNI configuration and MVRP learning and port is going to blocking state at hardware level.	In case of using more number MVRP vlans (i.e 2.5K), verify the VPAS for MVRP learned vlans,before configuring ethernet transparent bridging.

Virtual Chassis

PR	Description	Workaround
CRAOS8X-914	Sometimes after a VC-takeover, one of the users that was learned in blocking on UNP access linkagg is getting flushed though the mac-aging timer has not expired.	There is no known workaround at this time
CRAOS8X-3877	On 6900 and 6900V72, untagged packets are mirrored as tagged	Use port mirroring.

	traffic when when monitored port is across VC chassis. On standalone box, monitored egress traffic is tagged.	
--	---	--

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

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

Region	Phone Number
North America	800-995-2696
Latin America	877-919-9526
European Union	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484

Email: ebg_global_supportcenter@al-enterprise.com

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

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

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

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

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

Third Party Licenses and Notices

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

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

```
FOSS Name : FOSS Version : Name of Applicable License : Pointer to file containing License Text
libatomic      : 1.0.0      : GPLv3+ & GPLv3+      : /flash/foss/gpl-3.0.txt +
                with exceptions &      /flash/foss/gpl-2.0.txt +
                GPLv2+ with exceptions /flash/foss/lgpl-2.1.txt +
                & LGPLv2+ & BSD      /flash/foss/bsd1.txt
openvswitch    : 2.12.0     : Apache License 2.0    : /flash/foss/apache-license-2.0.txt
```

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 8.7R3.

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	6900-X48C4E	OS6900-V48C8	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	8.7R2	8.7R3	8.6R1
Automatic Remote Configuration Download (RCL)	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.6R2	8.7R1	8.7R2	8.7R3	Y
Automatic/Intelligent Fabric	8.7R2	8.5R1	Y	Y	8.7R2	Y	Y	Y	Y	Y	8.7R3	Y
Automatic VC	8.7R2	N	Y	Y	8.7R1	Y	Y	8.6R2	8.7R1	8.7R2	8.7R3	N
Bluetooth - USB Adapter with Bluetooth Technology	8.7R2	8.6R2	8.6R2	Y	8.7R1	8.6R2	8.7R1	8.6R2	N	N		N
Console Disable	8.7R2	8.6R2	8.6R2	8.6R2	8.7R1	8.6R2	8.6R2	8.6R2	8.7R1	8.7R2	8.7R3	8.6R2
Dying Gasp	N	Y	Y	Y	8.7R1	Y	N	N	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	N	N
EEE support	Y	N	N	Y	8.7R1	Y	Y	N	N	N	N	N
Embedded Python Scripting / Event Manager	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.7R2	8.7R2	8.7R2	8.7R3	N
IP Managed Services	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
Hitless Security Patch Upgrade	8.7R2	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R2	8.7R3	8.7R1
In-Band Management over SPB	N	N	N	8.5R4	8.7R1	8.5R4	8.5R4	8.5R4	8.7R1	8.7R2	8.7R3	8.5R4
ISSU	8.7R2	Y	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
NAPALM Support	8.7R2	8.5R1	8.5R1	8.5R1	8.7R1	8.5R1	8.5R1	8.7R2	8.7R2	8.7R2	8.7R3	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	8.7R2	8.7R3	8.5R4
NTP - IPv6	8.7R3	8.7R3	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	N	N
OV Cirrus - Zero touch provisioning	8.7R2	Y	Y	Y	8.7R1	Y	Y	8.7R2	8.7R2	8.7R2	8.7R3	N
OV Cirrus - Configurable NAS Address	8.7R2	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.5R4	8.7R1	8.7R2	8.7R3	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	8.7R2	8.7R3	8.5R4
OV Cirrus - Managed	8.7R2	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.5R4	8.7R1	8.7R2	8.7R3	8.5R4

Feature	6360	6465	6560	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6	6900-X48C4E	OS6900-V48C8	9900
OVSDB	N	N	N	N	N	N	8.7R1 (X72/Q32)	8.7R1	N	N	N	N
Package Manager	8.7R2	8.6R2	8.6R2	8.6R2	8.7R1	8.6R2	8.6R2	8.6R2	8.7R1	8.7R2	8.7R3	8.6R2
Readable Event Log	8.7R2	8.6R1	8.6R1	8.6R1	8.7R1	8.6R1	8.6R1	8.6R1	8.7R1	8.7R2	8.7R3	8.6R1
Remote Chassis Detection (RCD)	N	N	N	8.6R2	8.7R1	N	Y	N	8.7R1	8.7R2	8.7R3	Y
SAA	8.7R2	8.5R1	8.7R2	Y	8.7R2	Y	Y	8.7R1	8.7R1	8.7R2	8.7R3	Y
SAA SPB	N	N	N	Y	8.7R2	Y	Y	8.7R1	8.7R1	8.7R2	8.7R3	8.6R2
SAA UNP	N	Y	N	Y	N	Y	Y	N	N	N	N	N
SNMP v1/v2/v3	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
Uboot Enable/Disable/Authenticate	8.7R3	8.7R3	8.7R3	8.7R3	N	8.7R3	8.7R3	N	N	N	N	8.7R3
UDLD	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	N	N	N	N	EA
USB Disaster Recovery	8.7R2	8.5R1	Y	Y	8.7R1 (onie)	Y	Y	8.7R1 (onie)	8.7R1 (onie)	8.7R2 (onie)	8.7R3 (onie)	Y
USB Flash (AOS)	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	N	N	N	N	N
Virtual Chassis (VC)	8.7R2	8.5R2	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
Virtual Chassis Split Protection (VCSP)	8.7R2	Y	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
VRF	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
VRF - IPv6	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
VRF - DHCP Client	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
Web Services & CLI Scripting	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.7R1	8.7R1	8.7R2	8.7R3	Y
Layer 3 Feature Support												
ARP	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
BFD	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
BGP	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
DHCP Client / Server	8.7R2	8.6R1	Y	Y	8.7R1	Y	Y	8.5R4	8.7R1	8.7R2	8.7R3	Y
DHCP Relay	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R4	8.7R1	8.7R2	8.7R3	Y
DHCPv6 Server	N	N	N	Y	8.7R1	Y	Y	8.7R1	8.7R1	8.7R2	8.7R3	Y

Feature	6360	6465	6560	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6	6900-X48C4E	OS6900-V48C8	9900
DHCPv6 Relay	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.7R1	8.7R1	8.7R2	8.7R3	Y
DHCP Snooping / IP Source Filtering	8.7R2	8.5R4	Y	Y	8.7R1	Y	Y	8.6R2	8.7R1	8.7R2	8.7R3	Y
ECMP	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
IGMP v1/v2/v3	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
GRE	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	8.5R2
IP-IP tunneling	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	8.5R2
IPv6	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
IPv6 - DHCPv6 Snooping	8.7R2	8.6R1	8.6R1	8.5R3	8.7R1	8.5R4	N	8.6R2	8.7R1	8.7R2	8.7R3	8.7R1
IPv6 - Source filtering	8.7R2	N	8.6R1	8.5R3	8.7R1	8.5R4	N	8.6R2	8.7R1	8.7R2	8.7R3	8.7R1
IPv6 - DHCP Guard	EA	EA	EA	EA	N	EA	N	N	N	N	N	N
IPv6 - DHCP Client Guard	EA	EA	EA	EA	N	EA	N	N	N	N	N	N
IPv6 - RA Guard (RA filter)	N	N	8.5R2	Y	8.7R1	Y	Y	N	N	N	N	N
IPv6 - DHCP relay and Neighbor discovery proxy	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	N	N	N	N	Y
IP Multinetting	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
IPSec (IPv6)	N	N	N	Y	8.7R1	Y	Y	N	N	N	N	EA
ISIS IPv4/IPv6	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	8.5R2
M-ISIS	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	8.5R2
OSPFv2	N	N	8.5R2 ¹	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
OSPFv3	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
RIP v1/v2	N	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
RIPng	N	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
UDP Relay (IPv4)	8.7R2	8.5R4	8.5R4	Y	8.7R1	Y	Y	8.5R4	8.7R1	8.7R2	8.7R3	8.5R4
UDP Relay (IPv6)	8.7R2	8.6R1	8.6R1	8.6R1	8.7R1	8.6R	8.6R1	8.6R1	8.7R1	8.7R2	8.7R3	8.6R1
VRRP v2	8.7R2	8.5R2	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
VRRP v3	8.7R2	8.5R2	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y

Feature	6360	6465	6560	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6	6900-X48C4E	OS6900-V48C8	9900
Server Load Balancing (SLB)	N	N	N	Y	N	Y	Y	N	N	N	N	N
Static routing	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
Multicast Features												
DVMRP	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	N
IPv4 Multicast Switching	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
Multicast *,G	8.7R2	Y	8.5R2	8.5R2	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
IPv6 Multicast Switching	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
PIM-DM	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
PIM-SM	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
PIM-SSM	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R1	8.7R3	Y
PIM-SSM Static Map	N	N	N	N	N	N	N	N	N	N	N	N
PIM-BiDir	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
PIM Message Packing	N	N	N	8.6R1	8.7R1	N	8.6R1	8.6R1	8.7R1	8.7R2	8.7R3	N
PIM - Anycast RP	N	N	N	8.6R2	8.7R1	8.6R2	8.6R2	8.6R2	8.7R1	8.7R2	8.7R3	8.6R2
Monitoring/Troubleshooting Features												
Ping and traceroute	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
Policy based mirroring	N	N	N	Y	8.7R1	Y	Y	8.7R1	8.7R1	8.7R2	8.7R3	8.5R4
Port mirroring	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
Port monitoring	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
Port mirroring - remote	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.7R2	8.7R2	8.7R2	8.7R3	8.6R1
Port mirroring - remote over linkagg	N	N	N	Y	8.7R1	Y	Y	8.7R2	8.7R2	8.7R2	8.7R3	8.6R1
RMON	8.7R2	8.5R1	Y	Y	N	Y	Y	N	N	N		N
SFlow	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.7R1	8.7R1	8.7R2	8.7R3	Y
Switch logging / Syslog	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
TDR	N	N	N	Y	8.7R2	N	N	N	N	N	N	N

Feature	6360	6465	6560	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6	6900-X48C4E	OS6900-V48C8	9900
Layer 2 Feature Support												
802.1q	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
DHL	8.7R2	8.5R1	Y	Y	8.7R1	Y	N	N	N	N	N	N
ERP v2	N	8.5R1	8.5R2	Y	8.7R1	Y	Y	8.7R1	8.7R1	8.7R2	8.7R3	8.5R3
HAVLAN	N	EA	N	Y	N	Y	Y	8.6R2	8.7R1	8.7R2	8.7R3	EA
Link Aggregation (static and LACP)	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
LLDP (802.1ab)	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
Loopback detection - Edge (Bridge)	8.7R2	8.5R1	Y	Y	8.7R1	Y	N	8.6R2	8.7R1	8.7R2	8.7R3	Y
Loopback detection - SAP (Access)	N	N	N	Y	8.7R1	Y	Y	8.6R2	8.7R1	8.7R2	8.7R3	Y
MAC Forced Forwarding / Dynamic Proxy ARP	8.7R2	8.7R1	N	8.6R1	N	8.6R1	N	N	N	N	N	N
MRP	N	8.7R2	N	N	N	8.7R2	N	N	N	N	N	N
Port mapping	8.7R2	Y	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	N
Private VLANs (PVLAN)	N	N	N	Y	8.7R2	Y	Y	N	8.7R2	8.7R2	8.7R3	N
SIP Snooping	N	N	N	Y	N	N	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	8.7R2	8.7R3	Y
Spanning Tree (PVST+, Loop Guard)	8.7R2	N	Y	Y	8.7R1	Y	Y	N	N	N	N	EA
MVRP	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R4	8.7R1	8.7R2	8.7R3	Y
SPB ²	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
SPB - Over Shared Ethernet	N	N	N	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R1	8.7R2	8.7R3	8.7R1
SPB - HW-based LSP flooding	N	N	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	8.7R2	8.7R3	Y
IPv4	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
IPv6	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
Auto-Qos prioritization of NMS/IP Phone Traffic	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
Auto-Qos - New MAC range	8.7R2	8.5R2	8.5R2	8.5R2	8.7R1	8.5R2	8.5R2	8.5R2	8.7R1	8.7R2	8.7R3	8.5R2

Feature	6360	6465	6560	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6	6900-X48C4E	OS6900-V48C8	9900
Groups - Port	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
Groups - MAC	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
Groups - Network	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
Groups - Service	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
Groups - Map	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
Groups - Switch	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
Ingress/Egress bandwidth limit	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
Per port rate limiting	N	N	N	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	N
Policy Lists	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.7R1	8.7R1	8.7R2	8.7R3	Y
Policy Lists - Egress	N	N	N	Y	8.7R1	Y	Y	8.7R1	8.7R1	8.7R2	8.7R3	N
Policy based routing	N	N	N	Y	8.7R1	Y	Y	8.6R2	8.7R1	8.7R2	8.7R3	EA
Tri-color marking	N	N	N	Y	8.7R1	Y	Y	N	N	N	N	N
QSP Profiles 1	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
QSP Profiles 2/3/4	N	N	N	Y	QSP-2 only	Y	Y	QSP-2 only	QSP-2 only	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	N	N	Y
Custom QSP Profiles	8.7R2	Y	Y	Y	Y	Y	X72 only (EA)	Y	Y	Y	8.7R3	Y
GOOSE Messaging Prioritization	N	8.7R1	N	N	N	8.7R1	N	N	N	N	N	N
Metro Ethernet Features												
CPE Test Head	N	8.6R1	N	N	N	N	N	N	N	N	N	N
Ethernet Loopback Test	N	N	N	8.6R1	8.7R1	8.6R1	N	N	N	N	N	N
Ethernet Services (VLAN Stacking)	N	8.5R1	N	Y	8.7R2	Y	Y	8.5R4	8.7R1	8.7R2	8.7R3	N
Ethernet OAM (ITU Y1731 and 802.1ag)	N	8.5R1	N	Y	8.7R1	Y	Y	8.7R1	8.7R1	8.7R2	8.7R3	EA
EFM OAM / Link OAM (802.3ah)	N	8.6R1	8.6R1	8.5R4	8.7R2	8.5R4	N	N	N	8.7R2	8.7R3	N
PPPoE Intermediate Agent	N	8.6R1	N	N	N	8.6R1	N	N	N	N	N	N
1588v2 End-to-End Transparent Clock	N	8.5R1	8.7R2	Y	N	Y	Y (X72/Q32)	N	N	N	N	N

Feature	6360	6465	6560	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6	6900-X48C4E	OS6900-V48C8	9900
1588v2 Peer-to-Peer Transparent Clock	N	N	8.7R2	N	N	N	N	N	N	N	N	N
1588v2 Across VC	N	N	N	N	N	N	8.5R2 (X72)	N	N	N	N	N
Access Guardian / Security Features												
802.1x Authentication	8.7R2	8.5R2	Y	Y	8.7R1	Y	Y	8.7R1	8.7R1	8.7R2	8.7R3	Y
Access Guardian - Bridge	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.6R1	8.7R1	8.7R2	8.7R3	Y
Access Guardian - Access	N	N	N	Y	8.7R1	Y	Y	8.5R4	8.7R1	8.7R2	8.7R3	Y
Application Fingerprinting	N	N	N	N	N	N	Y	N	N	N	N	N
Application Monitoring and Enforcement (Appmon)	N	N	N	Y	8.7R2	N	N	N	N	N	N	N
ARP Poisoning Protection	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R2	8.7R1	8.7R2	8.7R3	Y
BYOD - COA Extension support for RADIUS	8.7R2	Y	Y	Y	8.7R1	Y	8.62	8.6R2	8.7R1	8.7R2	8.7R3	Y
BYOD - mDNS Snooping/Relay	8.7R2	Y	Y	Y	8.7R1	Y	8.62	8.6R2	8.7R1	8.7R2	8.7R3	Y
BYOD - UPNP/DLNA Relay	8.7R2	Y	Y	Y	8.7R1	Y	8.62	8.6R2	8.7R1	8.7R2	8.7R3	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	8.7R2	8.7R3	Y
Captive Portal	8.7R2	8.5R4	Y	Y	8.7R1	Y	8.62	8.6R2	8.7R1	8.7R2	8.7R3	Y
IoT Device Profiling	8.7R2	8.5R2	8.5R2	8.5R2	8.7R1	8.5R2	8.5R2	8.6R1	8.7R1	8.7R2	8.7R3	8.5R2
IoT Device Profiling (IPv6)	8.7R2	8.7R1	8.7R1	8.7R1	N	8.7R1	8.7R1	N	N	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	8.7R2	8.7R3	Y
Interface Violation Recovery	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.7R1	8.7R1	8.7R2	8.7R3	Y
Kerberos Snooping (services)	8.7R2	N	8.6R2	8.6R2	N	8.6R2	8.6R2	8.6R2	N	N	N	8.6R2
L2 GRE Tunnel Access (Edge) (bridge ports)	N	N	Y	Y	8.7R2	Y	8.6R1 ³	8.7R1	8.7R2	8.7R2	8.7R3	Y
L2 GRE Tunnel Access (Edge) (access ports)	N	N	N	8.6R1	8.7R2	8.6R1	8.6R1	8.7R1	8.7R2	8.7R2	8.7R3	8.6R1
L2 GRE Tunnel Aggregation	N	N	N	Y	8.7R2	Y	Y ³	8.7R1	8.7R2	8.7R2	8.7R3	Y
Learned Port Security (LPS)	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.5R4	8.7R1	8.7R2	8.7R3	Y
MACsec ⁴	N	8.5R1	8.5R4	Y	8.7R1	N	N	N	N	X48C4E	N	8.5R2
MACsec MKA Support ⁴	N	8.5R2	8.5R4	8.5R2	8.7R1	N	N	N	N	X48C4E	N	8.5R2
Quarantine Manager	N	8.7R2	8.7R2	Y	8.7R2	Y	8.7R2	8.7R2	8.7R2	8.7R2	8.7R3	8.7R2

Feature	6360	6465	6560	6860(E)	6860N	6865	6900	6900-V72/C32	6900-X48C6/T48C6	6900-X48C4E	OS6900-V48C8	9900
RADIUS - RFC-2868 Support	8.7R2	8.5R4	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.5R4	8.7R1	8.7R2	8.7R3	8.5R4
Role-based Authentication for Routed Domains	N	N	N	8.5R4	8.7R1	8.5R4	8.5R4	8.6R1	8.7R1	8.7R2	8.7R3	8.5R4
Storm Control (flood-limit)	8.7R2	Y	Y	Y	8.7R1	Y	Y	Y	8.7R1	8.7R2	8.7R3	Y
Storm Control (Unknown unicast with action trap/shutdown)	N	N	N	Y	N	Y	Y	N	N	N	N	N
TACACS+ Client	8.7R2	8.5R1	Y	Y	8.7R1	Y	Y	8.6R1	8.7R1	8.7R2	8.7R3	Y
TACACS+ command based authorization	8.7R2	N	N	Y	8.7R1	Y	Y	8.7R2	8.7R2	8.7R2	8.7R3	N
TACACS+ - IPv6	8.7R3	8.7R3	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	N	N	Y
802.3bt	8.7R2	Y	8.6R2	N	8.7R1	N	N	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	N	N	Y
Display of detected power class	8.7R2	8.5R1	Y	Y	8.7R1	Y	N	N	N	N	N	Y
LLDP/802.3at power management TLV	8.7R2	8.5R1	Y	Y	8.7R1	Y	N	N	N	N	N	Y
HPOE support	8.7R2 (95W)	8.5R1 (60W)	Y (95W)	Y (60W)	8.7R1 (95W)	Y (75W)	N	N	N	N	N	Y (75W)
Time Of Day Support	8.7R2	8.5R1	Y	Y		Y	N	N	N	N	N	Y
Perpetual PoE	8.7R2	N	N	Y	Y	Y	N	N	N	N	N	N
Fast PoE	8.7R2	N	N	Y	Y	Y	N	N	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	N	N
Data Center Bridging (DCBX/ETS/PFC)	N	N	N	N	N	N	Y	N	N	N	N	N
EVB	N	N	N	N	N	N	N	N	N	N	N	N
FCoE / FC Gateway	N	N	N	N	N	N	Y	N	N	N	N	N
VXLAN ⁵	N	N	N	N	N	N	Q32/X72	8.5R3	N	N	N	N
VM/VXLAN Snooping	N	N	N	N	N	N	Y	N	N	N	N	N
FIP Snooping	N	N	N	N	N	N	Y	N	N	N	N	N
Notes:												
1. OS6560 supports stub area only.												
2. See protocol support table in Appendix B.												
3. Not supported on 6900-T20/T40/X20/X40.												
4. Site license required beginning in 8.6R1.												
5. L2 head-end only on OS6900-V72/C32.												

Appendix B: 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 6860N
IPv4 Protocols					
Static Routing	Y	8.6R2	8.7R2	8.7R3	8.7R2
RIP v1/v2	Y	8.6R2	8.7R2	8.7R3	8.7R2
OSPF	Y	8.6R2	8.7R2	8.7R3	8.7R2
BGP	Y	8.6R2	8.7R2	8.7R3	8.7R2
VRRP	Y	8.7R1	8.7R2	8.7R3	8.7R2
IS-IS	N	N	N	N	N
PIM-SM/DM	8.5R3	8.6R2	Y	Y	Y
DHCP Relay	8.5R3	8.6R2	8.7R2	8.7R3	8.7R2
UDP Relay	8.5R4	8.6R2	8.7R2	8.7R3	8.7R2
DVMRP	N	N	N	N	N
BFD	8.7R2	8.7R2	8.7R2	8.7R3	8.7R2
IGMP Snooping	Y	8.6R2	8.7R2	8.7R3	8.7R2
IP Multicast Headend Mode	Y	8.6R2	8.7R2	8.7R3	8.7R2
IP Multicast Tandem Mode	8.5R4	8.6R2	N	N	N
IPv6 Protocols					
Static Routing	8.5R4	8.6R2	8.7R2	8.7R3	8.7R2
RIPng	8.5R4	8.6R2	8.7R2	8.7R3	8.7R2
OSPFv3	8.5R4	8.6R2	8.7R2	8.7R3	8.7R2
BGP	8.5R4	8.6R2	8.7R2	8.7R3	8.7R2
VRRPv3	8.5R4	8.7R1	8.7R2	8.7R3	8.7R2
IS-IS	N	N	N	N	N
PIM-SM/DM	8.5R4	8.6R2	N	N	N
DHCP Relay	8.6R1	8.7R2	8.7R2	8.7R3	8.7R2
UDP Relay	8.6R1	8.7R2	8.7R2	8.7R3	8.7R2
BFD	8.7R2	8.7R2	8.7R2	8.7R3	8.7R2
IPv6 MLD Snooping	Y	8.7R2	8.7R2	8.7R3	8.7R2
IPv6 Multicast Headend Mode	Y	8.7R2	8.7R2	8.7R3	8.7R2
IPv6 Multicast Tandem Mode	8.5R4	8.7R2	N	N	N

External Loopback Support								
	OmniSwitch 9900	OmniSwitch 6860/6865	OmniSwitch 6860N	OmniSwitch 6900	OmniSwitch 6900-V72/ C32	OmniSwitch 6900-X48C6/ T48C6	OmniSwitch 6900-X48C4E	OmniSwitch 6900-V48C8
IPv4 Protocols								
Static Routing	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3
RIP v1/v2	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3
OSPF	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3
BGP	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3
VRRP	8.6R1	8.5R4	8.7R1	Y	8.7R1	8.7R2	8.7R2	8.7R3
IS-IS	Y	Y	Y	Y	Y	Y	8.7R2	8.7R3
PIM-SM/DM	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3
DHCP Relay	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.7R1	8.7R2	8.7R3
UDP Relay	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.7R1	8.7R2	8.7R3
DVMRP	N	N	N	N	N	N	N	N
BFD	Y	Y	Y	Y	Y	Y	8.7R2	8.7R3
IGMP Snooping	8.5R4	Y	8.7R1	Y	8.6R1	8.7R1	8.7R2	8.7R3
IP Multicast Headend Mode	8.5R4	Y	8.7R1	Y	8.6R1	8.7R1	8.7R2	8.7R3
IP Multicast Tandem Mode	8.5R4	Y	8.7R1	Y	8.6R1	Y	Y	Y
IPv6 Protocols								
Static Routing	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3
RIPng	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3
OSPFv3	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3
BGP	8.5R4	Y	8.7R1	Y	8.5R4	8.7R1	8.7R2	8.7R3
VRRPv3	8.5R4	8.5R4	8.7R1	Y	8.7R1	8.7R2	8.7R2	8.7R3
IS-IS	Y	Y	Y	Y	Y	Y	8.7R2	8.7R3
PIM-SM/DM	8.5R4	8.5R4	8.7R1	8.5R4	8.5R4	8.7R1	8.7R2	8.7R3
DHCP Relay	8.6R1	8.6R1	8.7R1	8.6R1	8.6R1	8.7R1	8.7R2	8.7R3
UDP Relay	8.6R1	8.6R1	8.7R1	8.6R1	8.6R1	8.7R1	8.7R2	8.7R3
BFD	Y	Y	Y	Y	Y	Y	8.7R2	8.7R3
IPv6 MLD Snooping	8.5R4	Y	8.7R1	Y	Y	8.7R2	8.7R2	8.7R3
IPv6 Multicast Headend Mode	8.5R4	Y	8.7R1	Y	Y	8.7R2	8.7R2	8.7R3
IPv6 Multicast Tandem Mode	8.5R4	Y	8.7R1	Y	Y	Y	Y	Y

SPB BVLAN Scalability and Convergence Guidelines

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

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

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

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

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

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

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

Appendix C: 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 8.7R3 (GA)
OS6360	8.7.252.R02
OS6465	8.6.289.R01 (GA) 8.6.299.R01 (MR) 8.6.189.R02 (GA) 8.6.196.R02 (MR) 8.6.203.R02 (reGA) 8.7.277.R01 (GA) 8.7.280.R01 (MR) 8.7.354.R01 (GA) 8.7.252.R02 (GA)
OS6560	8.6.289.R01 (GA) 8.6.299.R01 (MR) 8.6.189.R02 (GA) 8.6.196.R02 (MR) 8.6.203.R02 (reGA) 8.7.354.R01 (GA) 8.7.252.R02 (GA)
OS6860(E)	8.6.289.R01 (GA) 8.6.299.R01 (MR) 8.6.189.R02 (GA) 8.6.196.R02 (MR) 8.6.203.R02 (reGA) 8.7.277.R01 (GA) 8.7.280.R01 (MR) 8.7.354.R01 (GA) 8.7.252.R02 (GA)
OS6860N	8.7.277.R01 (GA) 8.7.280.R01 (MR) 8.7.354.R01 (GA) 8.7.252.R02 (GA)
OS6865	8.6.289.R01 (GA) 8.6.299.R01 (MR) 8.6.189.R02 (GA) 8.6.196.R02 (MR) 8.6.203.R02 (reGA) 8.7.277.R01 (GA) 8.7.280.R01 (MR) 8.7.354.R01 (GA) 8.7.252.R02 (GA)
OS6900	8.6.289.R01 (GA) 8.6.299.R01 (MR) 8.6.189.R02 (GA) 8.6.196.R02 (MR) 8.6.203.R02 (reGA) 8.7.277.R01 (GA)

	8.7.280.R01 (MR) 8.7.354.R01 (GA) 8.7.252.R02 (GA)
OS6900-V72/C32	8.6.289.R01 (GA) 8.6.299.R01 (MR) 8.6.189.R02 (GA) 8.6.196.R02 (MR) 8.6.203.R02 (reGA) 8.7.277.R01 (GA) 8.7.280.R01 (MR) 8.7.354.R01 (GA) 8.7.252.R02 (GA) See Appendix G when upgrading an OS6900-V72/C32.
OS6900-X48C6/T48C6	8.7.277.R01 (GA) 8.7.280.R01 (MR) 8.7.354.R01 (GA) 8.7.252.R02 (GA)
OS9900	8.6.289.R01 (GA) 8.6.299.R01 (MR) 8.6.197.R02 (GA) 8.6.203.R02 (reGA) 8.7.354.R01 (GA) 8.7.252.R02 (GA)

8.7R3 ISSU Supported Releases

Prerequisites

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

- Be the responsible party for maintaining the switch's configuration.
- Be aware of any issues that may arise from a network outage caused by improperly loading this code.
- Understand that the switch must be rebooted and network access may be affected by following this procedure.
- Have a working knowledge of the switch to configure it to accept an FTP connection through the EMP or Network Interface (NI) Ethernet port.
- Read the GA Release Notes prior to performing any upgrade for information specific to this release.
- Ensure there is a current certified configuration on the switch so that the upgrade can be rolled-back if required.
- Verify the current versions of U-Boot and FPGA. If they meet the minimum requirements, (i.e. they were already upgraded during a previous AOS upgrade) then only an upgrade of the AOS images is required.
- Depending on whether a standalone chassis or VC is being upgraded, upgrading can take from 5 to 20 minutes. Additional time will be needed for the network to re-converge.

- The examples below use various models and directories to demonstrate the upgrade procedure. However, any user-defined directory can be used for the upgrade.
- If possible, have EMP or serial console access to all chassis during the upgrade. This will allow you to access and monitor the VC during the ISSU process and before the virtual chassis has been re-established.
- Knowledge of various aspects of AOS directory structure, operation and CLI commands can be found in the Alcatel-Lucent OmniSwitch User Guides. Recommended reading includes:
 - Release Notes - for the version of software you're planning to upgrade to.
 - The AOS Switch Management Guide
 - Chapter - Getting Started
 - Chapter - Logging Into the Switch
 - Chapter - Managing System Files
 - Chapter - Managing CMM Directory Content
 - Chapter - Using the CLI
 - Chapter - Working With Configuration Files
 - Chapter - Configuring Virtual Chassis

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

Switch Maintenance

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

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

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

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

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

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

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

```
6900-> show running-directory
CONFIGURATION STATUS
Running CMM : MASTER-PRIMARY,
```



```
CMM Mode : VIRTUAL-CHASSIS MONO CMM,  
Current CMM Slot : CHASSIS-1 A,  
Running configuration : vc_dir,  
Certify/Restore Status : CERTIFIED  
SYNCHRONIZATION STATUS  
Running Configuration : SYNCHRONIZED
```

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

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

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

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

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

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

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

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

Appendix D: Standard Upgrade - OmniSwitch Standalone or Virtual Chassis

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

1. Download the Upgrade Files

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

- OS6360 - Nosa.img
 - Refer to [Appendix F](#) for recommended/required FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6465 - Nos.img
 - Refer to [Appendix F](#) for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6560 - Nos.img
 - Refer to [Appendix F](#) for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6860 - Uos.img
 - Refer to [Appendix F](#) for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6860N - Uosn.img
- OS6865 - Uos.img
 - Refer to [Appendix F](#) for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6900 - Tos.img
 - Refer to [Appendix F](#) for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6900-V72/C32 - Yos.img. See [Appendix G](#).
- 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           8.7.98.R03       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 E: ISSU - OmniSwitch Chassis or Virtual Chassis

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

1. Download the Upgrade Files

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

- OS6360 - Nosa.img
 - Refer to [Appendix F](#) for recommended/required FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6465 - Nos.img
 - Refer to [Appendix F](#) for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6560 - Nos.img
 - Refer to [Appendix F](#) for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6860 - Uos.img
 - Refer to [Appendix F](#) for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6860N - Uosn.img
- OS6865 - Uos.img
 - Refer to [Appendix F](#) for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6900 - Tos.img
 - Refer to [Appendix F](#) for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6900-V72/C32 - Yos.img. See [Appendix G](#).
- OS6900-X48C6/T48C6 - 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
Chas  MAC-Address          Address          Address          Status
-----+-----+-----+-----+-----
1      e8:e7:32:b9:19:0b  127.10.2.65    127.10.1.65    Connected
```

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

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

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

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

6. Log out of the Slave chassis:

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

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

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

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

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

9. Upgrade the image files using ISSU:

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

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

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

This indicates that the ISSU is completed

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

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

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

10. Verify the Software Upgrade

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

```
OS6900-> show microcode
/flash/working
Package      Release      Size      Description
-----+-----+-----+-----
Tos.img      8.7.98.R03  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 F: 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	6465(T), 6560-24X4/P24X4/48X4/P48X4/X10
CRAOS8X-13819	Description	Uboot unable to mount eUSB flash
	U-boot Version	8.7.2.R02
	Platforms	6560-24Z24/P24Z24/24Z8/P24Z8/P48Z16(903954-90/904044-90), 6865
CRAOS8X-22857	Description	OS6560-P24Z24 reloads continuously with pmds
	FPGA Version	0.8
	Platforms	6560-24Z24/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	6360, 6465, 6560, 6860, 6865, 6900, 9900. (Not applicable for platforms that use ONIE)

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_7400 (Note: OS6360 uses fpga_kit_7517)
- U-boot.8.7.R03.#.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_7400
Parse /flash/fpga_kit_7400
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.8.7.R03.#.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 G: OS6900-V72/C32 Flash Cleanup Procedure / FEC Disable

Prior to performing a standard or ISSU upgrade on an OS6900-V72/C32 it's required to perform a cleanup of some files in the flash memory. This procedure must be performed when upgrading from the releases listed below. A script file has been created that will automatically perform the file cleanup on a VC or standalone chassis. It must be run from the maintenance shell prior to upgrading.

Additionally, the script will prompt the user to confirm if an ISSU upgrade is being performed. If an ISSU upgrade is being performed the script will create an additional file (*issu_no_fec_vfl_pre_86R2*) in the */flash* directory on both chassis in the VC. This file will prevent (Forward Error Correction) FEC from being automatically enabled after the upgrade on any 10G/40G VFLs, which is the default setting beginning in 8.6R2. This prevents a FEC mismatch between the Master and Slave chassis (enabled on Slave chassis / disabled on the Master chassis) during the ISSU upgrade.

- Standard Upgrade
 - If upgrading from AOS Release 8.5R02, 8.5R03, or 8.5R04 - Script file will perform flash cleanup.
 - If upgrading from AOS Release 8.6R01 or later - Script file not needed.
- ISSU Upgrade
 - If upgrading from AOS Release 8.6R01 - Script file will perform FEC disable.
- Script file name: *pre_update_script.sh* (Available from service & support website)
 - **Note:** An error, *"/mnt/chassis*: No such file or directory"*, may be displayed when running the script on a standalone chassis. This error has no affect on the upgrade.

1. FTP the script file to the */flash* directory on the Master chassis of the VC or standalone chassis.
2. OS6900-> su
3. YUKON #-> cd /flash
4. YUKON #-> sh pre_update_script.sh
5. YUKON #-> exit
6. OS6900->
7. You may now proceed to performing a standard or ISSU upgrade.
8. If performing an ISSU upgrade, perform the following after the upgrade is complete:

- Delete the *issu_no_fec_vfl_pre_86R2* file from the */flash* directory.
- Enable FEC on the VFL ports using the *'interfaces chassis/slot/port fec auto'* command. Enable FEC on a pair-by-pair basis.


Appendix H: Fixed Problem Reports

The following problem reports were closed in the 8.7.98.R03 release.

CR/PR NUMBER	Description
Case: 00526825 CRAOS8X-26058	<p>Summary: After the ISSU upgrade of OS6900 switch from 8.5.196R04 to 8.6.R01/R02 and 8.7.R01/R02, the IP-helper configuration is not converted properly for the default-VRF. This issue is not seen with the standard upgrade procedure in the switch.</p> <p>Explanation: The "ip helper" command have been deprecated and replaced with "ip dhcp relay" command from 8.6R01. The old format will still be accepted if present in a vboot.cfg to preserve backwards compatibility. This issue is only seen in the default-VRF and not in the other VRF of the same switch. If the Relay Mode in the default-VRF of the switch is configured with "per-interface-mode", it would be changed to "Global" due to the issue. The switch continued to relay packets for most of VLANs; however, the relay packets are send frequently to all the relay IP address. Certain VLANs are still affected due to the configuration conversion issue.</p> <p>Click for Additional Information</p>
Case: 00542096 CRAOS8X-26996	<p>Summary: After the upgrade of OS6860E-U28 switch to the microcode 8.7.252.R02, the switch continuous to crash and reload.</p> <p>Explanation: The switch crashed due to the task 'radcli'. If a switch is configured with 2 radius server host, in which the primary server is 'unresponsive' and the backup server is 'active'. In this state, when the switch receives ftp/ssh access then the switch would continue to crash and reload.</p> <p>Click for Additional Information</p>
Case: 00533215 CRAOS8X-26612	<p>Summary: 802.1x authentication delayed after the MAC authentication is passed.</p> <p>Explanation: The PC used have a fast booting sequence as soon as MAC is passed then when 802.1x is triggered via user the EAPOL packets are not sent from switch to user.</p> <p>Click for Additional Information</p>
Case: 00541629 CRAOS8X-26965	<p>Summary: 802.1x is failing sometimes if machine authentication is enabled in user PC and the user authentication happened before the machine authentication is ended.</p> <p>Explanation: The ID of an existing authentication is reused instead of cancelling the ongoing machine authentication and triggering a 802.1x with a new ID.</p> <p>Click for Additional Information</p>
Case: 00540363 CRAOS8X-26904	<p>Summary: Linkagg in/out octets polled via SNMP using MIB2 are wrong.</p> <p>Explanation: When MIB2 is used in/out octets registers size of linkagg are very low (16bits) compared to the ports memembers register size(32bits), this bug is impacting the snmp polled stats as the linkagg is filled quicly which provid wrong info to the NMS tool.</p> <p>Click for Additional Information</p>
Case: 00528076 CRAOS8X-26233	<p>Summary: Health mon trap is sent from switch while performing to clear l2 stat for a port.</p> <p>Explanation:</p>

	<p>It is identified that while clearing the statistical data, from ESM layer the value is 0 is being passed to hmon. Modified the hmon calculation part, where it will cover all corner cases.</p> <p>Click for Additional Information</p>
<p>Case: 00538350 CRAOS8X-26841</p>	<p>Summary: OS6900-T40 with FIPS enable was only offering hmac-sha1, hmac-sha1-96.</p> <p>Explanation: In FIPS mode the switch only offers hmac-sha1, hmac-sha1-96 and not hmac-sha2-256, hmac-sha2-512. Issue is fixed in 8.7.R03.</p> <p>Click for Additional Information</p>
<p>Case: 00509671 CRAOS8X-24065</p>	<p>Summary: SSH strong Cipher is not overwriting the FIPS default list of Cipher.</p> <p>Explanation: SSH strong cipher command was not overwriting the default FIPS default cipher. This is fixed in 8.7.R03.</p> <p>Click for Additional Information</p>
<p>Case: 00532247 CRAOS8X-26530</p>	<p>Summary: OS6860 : Policy server flush command is removing policy port group UserPorts.</p> <p>Explanation: The “Policy Flush Server” command should flush all the qos related configuration except policy port group “UserPorts” command. In AOS 8.7R02 and the below, the policy server flush command has removed the policy port group UserPorts command. The fix is available in AOS 8.7R03</p> <p>Click for Additional Information</p>
<p>Case: 00473249 CRAOS8X-20195</p>	<p>Summary: SNMP walk returning all MIBs details instead of only particular protocol/service having user permission.</p> <p>Explanation: When performed an SNMP walk for Alcatel switches, output should list for particular protocol/service as per user permission.</p> <p>Click for Additional Information</p>
<p>Case: 00501846 CRAOS8X-23026</p>	<p>Summary: UNP clients are mapped to vlan 1 ,When restart the switch, the clients mapped to vlans could not communicate even its mapped to correct profile.</p> <p>Explanation: During the boot initialization stage, all the port are mapped to vlan 1(default), then the system will parse the configuration in the vcboot.cfg. However, the port bitmap was not programmed for vlan 1. Hence, problem in the vlan 1 client communication.</p> <p>Click for Additional Information</p>
<p>Case: 00502655 CRAOS8X-24652</p>	<p>Summary: OS6900 switch rebooted due to memory leak.</p> <p>Explanation: OS6900 switch rebooted due to memory leak ChassisSupervisor memMgr ALRT: WATERMARK_HIGH(2) The top 20 memory hogs in Zone High Memory(1).</p> <p>Click for Additional Information</p>
<p>Case: 00547239 CRAOS8X-27538</p>	<p>Summary: OS6860(E/N) is not sending RADIUS Access-Request via the uplink when the management IP Interface is terminating with .127</p>

	<p>Explanation: “radcli” component does not find the source IP address when generating the Radius Access-Request "Could not find server interface IP address". We notice that component is trying to generate the request by using the Loopback IP Interface 127.0.0.1 which is not authorized. The mismatch occurs when the management IP Interface is terminating by x.x.x.127.</p> <p>🔒 Click for Additional Information</p>
Case: 00553308 CRAOS8X-27739	<p>Summary: OS6860(E/N) / OS6465 AGCMM Core dump and switch crash.</p> <p>Explanation: Several core dumps are generated and a switch crash is noticed The faulty module is Access Guardian and issue started to be observed after enabled IoT Profiling/Enforcement with OmniVista.</p> <p>🔒 Click for Additional Information</p>
Case: 00532597 CRAOS8X-26621	<p>Summary: AOS 8.x - unnp port-template bridgeDefaultPortTemplate modifications are lost after switch reboot.</p> <p>Explanation: Modify the UNP default template bridgeDefaultPortTemplate to disable the mac-authentication After the reload all, the UNP template settings are back to default values.</p> <p>🔒 Click for Additional Information</p>
Case: 00524641 CRAOS8X-25994	<p>Summary: Ethernet port with autoneg enable does not work with 2 pair cable.</p> <p>Explanation: When a device is connected to any 8.X switch, using a 2 pair (only 4 wires), the port does not come UP. The issue is not seen if autoneg is disabled.</p> <p>🔒 Click for Additional Information</p>
Case: 00521734 CRAOS8X-25841	<p>Summary: Cannot get DHCP on VLAN 127 with Zero Touch Template Based Provisioning.</p> <p>Explanation: On 6465T-P12 switch, use of template based provisioning won't work if we want it to work in VLAN 127 (tagged). The switch will not send vlan 127 tagged frame for dhcp discover, however, in the console logs, we can see that the switch try both VLAN 1 and VLAN127</p> <p>🔒 Click for Additional Information</p>
Case: 00542906 CRAOS8X-27056	<p>Summary: OS6860(E/N) / OS6465 AGCMM Core dump and switch crash.</p> <p>Explanation: Several core dumps are generated, and a switch crash was noticed. The faulty module is Access Guardian and issue started to be observed after enabled IoT Profiling/Enforcement with OmniVista.</p> <p>🔒 Click for Additional Information</p>
Case: 00519501 CRAOS8X-25071	<p>Summary: Router ports could be added to other VLANs.</p> <p>Explanation: When assigning any VLAN to port first and try to make that port a router port then we see the following error: "ERROR: Trunk already tagged in vlan 4000".</p> <p>🔒 Click for Additional Information</p>
Case:	<p>Summary:</p>

00525342 CRAOS8X-25948	<p>EAP Supplicant timeout and TX timers does not work when changed from default.</p> <p>Explanation: The EAP timers i.e. Supplicant timeout and Tx Timeout are not taking effect after the default values are changed from CLI. This is a software issue which is fixed in 8.7.R03.</p> <p> Click for Additional Information</p>
---------------------------	--

Appendix I: Installing/Removing Packages

The package manager provides a generic infrastructure to install AOS or non-AOS third party Debian packages and patches. The following packages are supported 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.