# Release Notes - Rev. B

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

## Release 8.9R4

These release notes accompany release 8.9R4. These release notes provide important information on individual software features and hardware modules. Since much of the information in these release notes is not included in the hardware and software user manuals, it is important that you read all sections of this document before installing new hardware or loading new software.

**Note - The OS9912 and OS99-CNI-U20 are currently not supported in AOS Release 8.9R4.**
(They are referenced in the 8.9R4 user guides and release notes. The release notes will be updated with additional information once the products are supported at a future date.

## Contents

## Related Documentation

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

- OmniSwitch 6360 Hardware User Guide
- OmniSwitch 6465 Hardware User Guide
- OmniSwitch 6900 Hardware User Guide
- OmniSwitch 6560 Hardware User Guide
- OmniSwitch 6570M Hardware User Guide
- OmniSwitch 6860 Hardware User Guide
- OmniSwitch 6865 Hardware User Guide
- OmniSwitch 9900 Hardware User Guide
- OmniSwitch AOS Release 8 CLI Reference Guide
- OmniSwitch AOS Release 8 Network Configuration Guide
- OmniSwitch AOS Release 8 Switch Management Guide
- OmniSwitch AOS Release 8 Advanced Routing Configuration Guide
- OmniSwitch AOS Release 8 Data Center Switching Guide
- OmniSwitch AOS Release 8 Specifications Guide
- OmniSwitch AOS Release 8 Transceivers Guide

## System Requirements

### Memory Requirements

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

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

### U-Boot and FPGA Requirements

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

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

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

### OmniSwitch 6360 - AOS Release 8.9.94.R04 (GA)

| Hardware | Minimum U-Boot | Current U-Boot | Minimum FPGA | Current FPGA |
|---|---|---|---|---|
| OS6360-10 | 8.7.149.R02 | 8.7.30.R03[2]<br>8.9.85.R02[4] | 0.11 | 0.11<br>0.12[5] |

| Hardware | Minimum U-Boot | Current U-Boot | Minimum FPGA | Current FPGA |
|---|---|---|---|---|
| OS6360-P10 | 8.7.149.R02 | 8.7.30.R03[2]<br>8.9.85.R02[4] | 0.11 | 0.11<br>0.12[5] |
| OS6360-P10A (904324-90) | 8.8.2.R03 | 8.8.2.R03<br>8.9.85.R02[4] | 0.1 | 0.1<br>0.2[5] |
| OS6360-24 | 8.7.149.R02 | 8.7.30.R03[2]<br>8.9.85.R02[4] | 0.15 | 0.17[1]<br>0.20[3] |
| OS6360-P24 | 8.7.149.R02 | 8.7.30.R03[2]<br>8.9.85.R02[4] | 0.15 | 0.17[1]<br>0.20[3] |
| OS6360-P24X | 8.7.149.R02 | 8.7.30.R03[2]<br>8.9.85.R02[4] | 0.12 | 0.12<br>0.13[5] |
| OS6360-PH24 | 8.7.149.R02 | 8.7.30.R03[2]<br>8.9.85.R02[4] | 0.12 | 0.12<br>0.13[5] |
| OS6360-48 | 8.7.149.R02 | 8.7.30.R03[2]<br>8.9.85.R02[4] | 0.15 | 0.17[1]<br>0.20[3] |
| OS6360-P48 | 8.7.149.R02 | 8.7.30.R03[2]<br>8.9.85.R02[4] | 0.15 | 0.17[1]<br>0.20[3] |
| OS6360-P48X | 8.7.149.R02 | 8.7.30.R03[2]<br>8.9.85.R02[4] | 0.12 | 0.12<br>0.13[5] |
| OS6360-PH48 | 8.8.114.R01 | 8.8.114.R01<br>8.9.85.R02[4] | 0.12 | 0.12<br>0.13[5] |

1. FPGA version 0.17 is REQUIRED to address issues CRAOS8X-26370 and CRAOS8X-25033.
2. Optional uboot update for CRAOS8X-24464, ability to disable/authenticate uboot access.
3. Optional FPGA update for reduced fan speed at boot up.
4. Highly recommended to address NAND flash corruption issue (CRAOS8X_35470). Also adds support for Gowin CPLD.
5. For switches currently shipping from the factory. No upgrade required for existing switches.

## OmniSwitch 6465 - AOS Release 8.9.94.R04 (GA)

| Hardware | Minimum U-Boot | Current U-Boot | Minimum FPGA | Current FPGA |
|---|---|---|---|---|
| OS6465-P6 | 8.5.83.R01 | 8.7.2.R02[2]<br>8.7.30.R03[3]<br>8.8.33.R01[4]<br>8.9.85.R02[5] | 0.10 | 0.10 |
| OS6465-P12 | 8.5.83.R01 | 8.7.2.R02[2]<br>8.7.30.R03[3]<br>8.8.33.R01[4]<br>8.9.85.R02[5] | 0.10 | 0.10 |
| OS6465-P28 | 8.5.89.R02 | 8.7.2.R02[2]<br>8.7.30.R03[3]<br>8.8.33.R01[4]<br>8.9.85.R02[5] | 0.5 | 0.7[1] |
| OS6465T-12 | 8.6.117.R01 | 8.7.2.R02[2]<br>8.7.30.R03[3] | 0.4 | 0.4 |

| Hardware | Minimum U-Boot | Current U-Boot | Minimum FPGA | Current FPGA |
|---|---|---|---|---|
| | | 8.8.33.R01[4]<br>8.9.85.R02[5] | | |
| OS6465T-P12 | 8.6.117.R01 | 8.7.2.R02[2]<br>8.7.30.R03[3]<br>8.8.33.R01[4]<br>8.9.85.R02[5] | 0.4 | 0.4 |
| OS6465-P12 (ENH-240) | 8.8.33.R01 | 8.8.33.R01<br>8.9.85.R02[5] | 0.5 | 0.5 |

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

## OmniSwitch 6560 - AOS Release 8.9.94.R04 (GA)

| Hardware | Minimum U-Boot | Current U-Boot | Minimum FPGA | Current FPGA |
|---|---|---|---|---|
| OS6560-24Z24 | 8.5.22.R01 | 8.7.2.R02[3]<br>8.7.30.R03[7]<br>8.9.85.R02[9] | 0.7 | 0.8[5] |
| OS6560-P24Z24 | 8.4.1.23.R02 | 8.7.2.R02[3]<br>8.7.30.R03[7]<br>8.9.85.R02[9] | 0.6 | 0.7[1]<br>0.8[5] |
| OS6560-24Z8 | 8.5.22.R01 | 8.7.2.R02[3]<br>8.7.30.R03[7]<br>8.9.85.R02[9] | 0.7 | 0.8[5] |
| OS6560-P24Z8 | 8.4.1.23.R02 | 8.7.2.R02[3]<br>8.7.30.R03[7]<br>8.9.85.R02[9] | 0.6 | 0.7[1]<br>0.8[5] |
| OS6560-24X4 | 8.5.89.R02 | 8.7.2.R02[4]<br>8.7.30.R03[7]<br>8.9.85.R02[8] | 0.4 | 0.4 |
| OS6560-P24X4 | 8.5.89.R02 | 8.7.2.R02[4]<br>8.7.30.R03[7]<br>8.9.85.R02[8] | 0.4 | 0.4 |
| OS6560-P48Z16 (903954-90) | 8.4.1.23.R02 | 8.7.2.R02[3]<br>8.7.30.R03[7]<br>8.9.85.R02[9] | 0.6 | 0.7[1]<br>0.8[5] |
| OS6560-P48Z16 (all other PNs) | 8.5.97.R04 | 8.7.2.R02[3]<br>8.7.30.R03[7]<br>8.9.85.R02[9] | 0.3 | 0.6[2]<br>0.7[6] |
| OS6560-48X4 | 8.5.97.R04 | 8.7.2.R02[4]<br>8.7.30.R03[7]<br>8.9.85.R02[8] | 0.4 | 0.7[2]<br>0.8[6] |

| Hardware | Minimum<br>U-Boot | Current<br>U-Boot | Minimum<br>FPGA | Current<br>FPGA |
|---|---|---|---|---|
| OS6560-P48X4 | 8.5.97.R04 | 8.7.2.R02[4]<br>8.7.30.R03[7]<br>8.9.85.R02[8] | 0.4 | 0.7[2]<br>0.8[6] |
| OS6560-X10 | 8.5.97.R04 | 8.7.2.R02[4]<br>8.7.30.R03[7]<br>8.9.85.R02[8] | 0.5 | 0.8[2] |
| 1. FPGA version 0.7 is optional to address issue CRAOS8X-7207.<br>2. FPGA versions are optional to address issue CRAOS8X-16452.<br>3. U-boot 8.7.2.R02 is optional to address eUSB issue CRAOS8X-13819.<br>4. U-boot 8.7.2.R02 is optional to address UBIFS error issues CRAOS8X-4813/13440.<br>5. FPGA version 0.8 is optional to address issue CRAOS8X-22857.<br>6. FPGA versions 0.7 and 0.8 are optional to support 1588v2.<br>7. Optional uboot update for CRAOS8X-24464, ability to disable/authenticate uboot access.<br>8. Highly recommended to address the NAND flash corruption issue (CRAOS8X_35470).<br>9. Ships from factory. No upgrade required, there are no functional changes in this uboot version for these models. | | | | |

## OmniSwitch 6570M - AOS Release 8.9.94.R04 (GA)

| Hardware | Minimum<br>U-Boot | Current<br>U-Boot | Minimum<br>FPGA | Current<br>FPGA |
|---|---|---|---|---|
| OS6570M-12 | 8.9.25.R02 | 8.9.25.R02<br>8.9.92.R02[1]<br>8.9.139.R03[3]<br>8.9.92.R04[4] | 0.11 | 0.11 |
| OS6570M-12D | 8.9.25.R02 | 8.9.25.R02<br>8.9.92.R02[1]<br>8.9.139.R03[3]<br>8.9.92.R04[4] | 0.11 | 0.11 |
| OS6570M-U28 | 8.9.25.R02 | 8.9.25.R02<br>8.9.92.R02[1]<br>8.9.139.R03[3]<br>8.9.70.R04[4] | 0.11 | 0.11<br>0.12[2] |
| 1. Adds support for Gowin CPLD.<br>2. Addresses power supply interrupt issue.<br>3. Addresses CRAOS8X-40924 for disabling uboot access.<br>4. Adds support for signed AOS images. | | | | |

## OmniSwitch 6860(E) - AOS Release 8.9.92.R04 (GA)

| Hardware | Minimum<br>U-Boot | Current<br>U-Boot | Minimum<br>FPGA | Current<br>FPGA |
|---|---|---|---|---|
| OS6860/OS6860E (except U28/P24Z8) | 8.1.1.70.R01 | 8.7.30.R03[2] | 0.9 | 0.10[1] |
| OS6860E-U28 | 8.1.1.70.R01 | 8.7.30.R03[2] | 0.20 | 0.20 |
| OS6860E-P24Z8 | 8.4.1.17.R01 | 8.7.30.R03[2] | 0.5 | 0.7[1] |

| Hardware | Minimum<br>U-Boot | Current<br>U-Boot | Minimum<br>FPGA | Current<br>FPGA |
|---|---|---|---|---|
| 1. FPGA versions .7 and .10 are optional on the PoE models for the fast and perpetual PoE feature support.<br>2. Optional uboot update for CRAOS8X-24464, ability to disable/authenticate uboot access. | | | | |

## OmniSwitch 6860N – AOS Release 8.9.94.R04 (GA)

| Hardware | Minimum<br>ONIE | Current<br>ONIE | Minimum<br>CPLD | Current<br>CPLD |
|---|---|---|---|---|
| OS6860N-U28 | 2019.05.00.10 | 2019.05.00.11 | 12 | 12 |
| OS6860N-P48Z | 2019.05.00.10 | 2019.05.00.11 | 12 | 13[1] |
| OS6860N-P48M | 2019.05.00.10 | 2019.05.00.11 | 11 | 12[1] |
| O6860N-P24M | 2019.05.00.11 | 2019.05.00.11 | 2 | 3[1] |
| OS6860N-P24Z | 2019.05.00.11 | 2019.05.00.11 | 2 | 3[1] |
| 1. Addresses CRAOS8X-29731/30471 – OS6860N power supply issue.<br>**Note**: These models use the **Uosn.img** image file. | | | | |

## OmniSwitch 6865 – AOS Release 8.9.94.R04 (GA)

| Hardware | Minimum<br>U-Boot | Current<br>U-Boot | Minimum<br>FPGA | Current<br>FPGA |
|---|---|---|---|---|
| OS6865-P16X | 8.3.1.125.R01 | 8.7.2.R02[2]<br>8.7.30.R03[3]<br>8.8.33.R01[4] | 0.20 | 0.25[1] |
| OS6865-U12X | 8.4.1.17.R01 | 8.7.2.R02[2]<br>8.7.30.R03[3]<br>8.8.33.R01[4] | 0.23 | 0.25[1] |
| OS6865-U28X | 8.4.1.17.R01 | 8.7.2.R02[2]<br>8.7.30.R03[3]<br>8.8.33.R01[4] | 0.11 | 0.14[1] |
| 1. FPGA versions 0.25 and 0.14 are optional for the fast and perpetual PoE feature support.<br>2. U-boot 8.7.2.R02 is optional to address eUSB issue CRAOS8X-13819.<br>3. Optional uboot update for CRAOS8X-24464, ability to disable/authenticate uboot access.<br>4. Optional uboot update to support boot from USB feature.<br>**Note**: CRAOS8X-4150 for the OS6865-U28X was fixed with FPGA version 0.12 and higher. | | | | |

## OmniSwitch 6900-X20/X40 – AOS Release 8.9.94.R04 (GA)

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

## OmniSwitch 6900-T20/T40 – AOS Release 8.9.94.R04 (GA)

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

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

## OmniSwitch 6900-Q32 – AOS Release 8.9.94.R04 (GA)

| Hardware | Minimum<br>U-Boot | Current<br>U-Boot | Minimum<br>FPGA | Current<br>FPGA |
|---|---|---|---|---|
| CMM | 7.3.4.277.R01 | 8.7.30.R03[1] | 0.1.8 | 0.1.8 |

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

## OmniSwitch 6900-X72 – AOS Release 8.9.94.R04 (GA)

| Hardware | Minimum<br>U-Boot | Current<br>U-Boot | Minimum<br>FPGA | Current<br>FPGA |
|---|---|---|---|---|
| CMM | 7.3.4.31.R02 | 8.6.189.R02[1]<br>8.7.30.R03[2] | 0.1.10 | 0.1.11[1] |

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

## OmniSwitch 6900-V72/C32/C32E/X48C6/T48C6/X48C4E/V48C8/T24C2/X24C2- AOS Release 8.9.94.R04 (GA)

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

| Hardware | Minimum ONIE | Current ONIE | Minimum CPLD | Current CPLD |
|---|---|---|---|---|
| OS6900-X48C4E | 2019.05.00.10 | 2019.05.00.10 | CPLD 1 - 3<br>CPLD 2 - 2<br>CPLD 3 – 3<br>CPU CPLD – N/A | CPLD 1 – 3<br>CPLD 2 - 2<br>CPLD 3 – 3<br>CPU CPLD - 2.14[1]<br>CPU CPLD – 2.15[2] |
| OS6900-V48C8 | 2020.02.00.01 | 2020.02.00.01 | CPLD 1 - 2<br>CPLD 2 - 3<br>CPLD 3 - 2 | CPLD 1 – 2<br>CPLD 2 - 3<br>CPLD 3 – 2 |
| OS6900-T24C2 | 2019.08.00.03 | 2019.08.00.03 | CPLD 1 - 2.0<br>CPLD 2 - 2.0<br>CPLD CPU - 6.0 | CPLD 1 - 2.0<br>CPLD 2 - 2.0<br>CPLD CPU - 6.0 |
| OS6900-X24C2 | 2019.08.00.03 | 2019.08.00.03 | CPLD 1 - 6.0<br>CPLD 2 - 6.0<br>CPLD CPU - 6.0 | CPLD 1 - 6.0<br>CPLD 2 - 6.0<br>CPLD CPU - 6.0 |
| 1. Optional CPU CPLD update to address CRAOS8X-30098.<br>2. Required CPLD update to address CRAOS8X-43968 (Hardware revision 6 only).<br>**Note**: These models use the **Yos.img** image file. | | | | |

## OmniSwitch 9900 – AOS Release 8.9.94.R04 (GA)

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

| Hardware | Minimum Coreboot-uboot | Current Coreboot-uboot | Minimun Control FPGA | Current Control FPGA | Minimum/ Current Power FPGA |
|---|---|---|---|---|---|
| OS99-CNI-U8 | 8.4.1.20.R03 | 8.4.1.20.R03<br>8.8.152.R01[2] | 1.7 | 1.7<br>1.9[2] | N/A |
| OS99-XNI-P48Z16 | 8.4.1.20.R03 | 8.4.1.20.R03<br>8.8.152.R01 | 1.4 | 1.4<br>1.6 | 0.7 |
| OS99-XNI-U24 | 8.5.76.R04 | 8.6.261.R01<br>8.8.152.R01[2] | 1.0 | 2.9.0<br>2.11.0[2] | 0.8 |
| OS99-XNI-P24Z8 | 8.5.76.R04 | 8.6.261.R01<br>8.8.152.R01 | 1.1 | 1.4.0<br>1.6.0 | 0.7 |
| OS99-XNI-U12Q | 8.6.117.R01 | 8.6.117.R01<br>8.8.152.R01 | 1.6.0 | 1.5.0<br>1.6.0 | N/A |
| OS99-XNI-UP24Q2 | 8.6.117.R01 | 8.6.117.R01<br>8.8.152.R01 | 1.5.0 | 1.5.0<br>1.6.0 | N/A |
| OS99-CNI-U20 | 8.9.183.R03 | 8.9.183.R03 | 1.2.0 | 1.2.0 | 0.4 |

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

## [IMPORTANT] *MUST READ*: AOS Release 8.9R4 Prerequisites and Deployment Information

### General Information

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

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

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

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

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

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

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

  Exceptions:
  - Copper ports or ports with copper transceivers do not support faster convergence.
  - OS6865-P16X and OS6865-U12X ports 3 and 4 do not support faster convergence.
  - VFL ports do not support faster convergence.
  - Splitter ports (i.e. 4X10G or 4X25G) do not support faster convergence.
  - OS6570M-12/12D ports 9 and 10 do not support fast convergence.

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

- SHA-1 Algorithm - Chosen-prefix attacks against the SHA-1 algorithm are becoming easier for an attacker[1]. For this reason, we have disabled the "ssh-rsa" public key signature algorithm by default. The better alternatives include:

  - The RFC8332 RSA SHA-2 signature algorithms rsa-sha2-256/512. These algorithms have the advantage of using the same key type as "ssh-rsa" but use the safer SHA-2 hash algorithms. RSA SHA-2 is enabled in AOS.
  - The RFC5656 ECDSA algorithms: ecdsa-sha2-nistp256/384/521. These algorithms are supported in AOS by default.

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

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

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

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

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

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

## Deprecated Features / Functionality Changes

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

| **AOS Release 8.5R4** |
|---|
| EVB - Beginning in 8.5R4, support for EVB is being removed. Any switches with an EVB configuration cannot be upgraded to 8.5R4 or above. |
| NTP - Beginning with AOS Release 8.5R4, OmniSwitches will not synchronize with an unsynchronized NTP server (stratum 16), as per the RFC standard. Existing installations where OmniSwitches are synchronizing from another OmniSwitch, or any other NTP server which is not synchronized with a valid NTP server, will not be able to synchronize their clocks. The following NTP commands have been deprecated:<br>- ntp server synchronized<br>- ntp server unsynchronized |
| |
| **AOS Release 8.6R1** |
| DHCPv6 Guard - Configuration via an IPv6 interface name is deprecated in 8.6.R1. Commands entered using the CLI must use the new 'ipv6 dhcp guard vlan vlan-id' format of the command. The old format will still be accepted if present in a vcboot.cfg to preserve backwards compatibility. |
| IP Helper - The 'ip helper' commands have been deprecated in 8.6R1 and replaced with 'ip dhcp relay'. The old format will still be accepted if present in a vcboot.cfg to preserve backwards compatibility. |
| SAA - The vlan-priority and drop-eligible parameters have been deprecated from all SAA commands beginning in 8.6R1. |
| MACsec is now supported on ports 33-48 of the 6560-(P)48X4. CRAOS8X-7910 was resolved in 8.6R1. |
| |
| **AOS Release 8.6R2** |
| Distributed ARP - Beginning 8.6R2 distributed ARP is no longer supported. |
| WRED - Beginning in 8.6R2 WRED is no longer supported. |
| QoS - Beginning in 8.6R2 the 'qos dscp-table' command is no longer supported. |
| NTP - The ntp parameter for the 'ip service source-ip' command was deprecated in 8.5R4. Support has been added back in 8.6R2. |
| |
| **AOS Release 8.7R1** |
| MACsec - Static mode is not supported on OS6860N. |
| Transceivers - Beginning in AOS release 8.7R1 an error message will be displayed when the unsupported QSFP-4X25G-C transceiver is inserted on an OS99-CNI-U8 module. |
| SPB - Beginning in 8.7.R01 the default number of BVLANs created via Auto Fabric is reduced from 16 to 4. This new default value is only applicable to factory default switches running 8.7R1 with no vcboot.cfg file. Upgrading to 8.7.R1 will not change the number of configured BVLANs in an existing configuration. See Appendix C for additional information. |
| **AOS Release 8.7R2** |
| There are new default user password polices being implemented in 8.7R2. This change does not affect existing users.<br>- cannot-contain-username: enable<br>- min-uppercase: 1<br>- min-lowercase: 1<br>- min-digit: 1 |

| |
|---|
| - min-nonalpha: 1 |
| The OmniSwitch 6360 does not contain a real-time clock.<br>- It is recommended to use NTP to ensure time synchronization on OS6360s.<br>- When the switch is reset, the switch will boot up from an approximation of the last known good time.<br>- When the switch is powered off it cannot detect the time left in the powered off state. When it boots up it will have the same time as when the switch was last powered off. |
| **AOS Release 8.7R3** |
| The Kerberos Snooping is not supported in bridge mode in this release. |
| **AOS Release 8.8R1** |
| Unsupported commands (Part of AOS 88R1 but not supported)<br>- mrp interconnect<br>- show mrp interconnect<br>- clear mrp interconnect |
| A software check was added in AOS releases 8.7R1, 8.7R2, and 8.7R3 restricting the use of the affected power supplies below while awaiting certification on the OS6560. This check was removed in 8.8R1 after the power supplies were certified resulting in the minimum AOS version 8.8R1 requirement.<br>**OS6560-BP-PH** - This OS6560 600W power supply, OS6560-BP-PH (904072-90), requires a minimum AOS version of 8.8R1.<br>**OS6560-BP-PX** - This OS6560 920W power supply, OS6560-BP-BX (904073-90), requires a minimum AOS version of 8.8R1.<br>Refer to the OmniSwitch 6560 Hardware Guide for additional power supply information. |
| **AOS Release 8.8R2** |
| The French language support is being removed from WebView to help reduce package size. If the default language is French it will default to English after upgrade. |
| **AOS Release 8.9R1** |
| Metro License Features – Some Metro features are now licensed on the OS6560 beginning in 8.9R1. See Metro License for information on re-enabling them after upgrading to 8.9R1. |
| **AOS Release 8.9R4** |
| The initial GA build of 8.9.92.R04 was replaced with 8.9.94.R04 to address CRAOS8X-44637. |
| OmniSwitch 6570 signed AOS image support. See Signed AOS Image for details. |
| The OS9912 and OS99-CNI-U20 are currently not supported in AOS Release 8.9R4.<br>(They are referenced in the 8.9R4 user guides and release notes. The release notes will be updated with additional information once the products are supported at a future date.) |

## Licensed Features

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

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

| | **Feature/Performance License Required** | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | OS6360 | OS6465 | OS6560 | OS6570M | OS6860 | OS6860N | OS6900 | OS9900 |
| Licensed Features | | | | | | | | |
| MACsec (OS-SW-MACSEC) | N/A | Yes | Yes | N/A | Yes | Yes | Yes[3] | Yes |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 10G support (OS6560-SW-PERF) | N/A | N/A | Yes[1] | N/A | N/A | N/A | N/A | N/A |
| 10G support (OS6360-SW-PERF) | Yes[2] | N/A | N/A | N/A | N/A | N/A | N/A | N/A |
| 10G support (OS6570-SW-PERF4) | N/A | N/A | N/A | Yes[4] | N/A | N/A | N/A | N/A |
| MPLS | N/A | N/A | N/A | N/A | N/A | Yes | N/A | N/A |

1. Performance software license is optional allowing ports 25/26 (OS6560-24X4/P24X4) and ports 49/50 (OS6560-48X4/P48X4) to operate at 10G speed. Ports support 1G by default.
2. Performance software license is optional allowing the 2 RJ45/SFP+ combo ports (25/26 or 49/50) of the OS6360-PH24 or OS6360-PH48 models to operate at 10G speed. Ports support 1G by default.
3. MACsec is supported on the OS6900-X48C4E.
4. Performance software license is optional allowing the OS6570M-U28 ports 25-28 to operate at 10G speed. Ports support 1G by default.

| | **Metro License Required** |
|---|---|
| | OmniSwitch 6560 |
| Licensed Features | |
| | |
| CPE Test Head | Yes |
| PPPoE-IA | Yes |
| Ethernet OAM | Yes |
| SAA | Yes |
| Link OAM | Yes |
| VLAN Stacking | Yes |
| DPA | Yes |
| Hardware Loopback | Yes |
| IPMVLAN | Yes |
| **Note**: Starting in 8.9R1 the features above require a Metro license. | |

| | **Advanced Routing License Required** | |
|---|---|---|
| | OmniSwitch 6570M | OmniSwitch 6560 |
| Licensed Features | | |
| | | |
| OSPFv2 and OSPFv3 | Yes | Yes (Up to 2 Areas) |
| Multicast Routing PIM (IPv4 & IPv6) | Yes | Not Supported |
| Multiple VRFs | Yes | Not Supported |
| ISIS (IPv4 and IPv6) | Yes | Not Supported |
| GRE Tunneling | Yes | Not Supported |
| IP-IP Tunneling | Yes | Not Supported |
| Route Redistribution | Yes | Yes |
| VRF Route Leaking | Yes | Not Supported |
| **Note**: Starting in 8.9R4 the table above lists the features supported with the Advanced Routing license. | | |

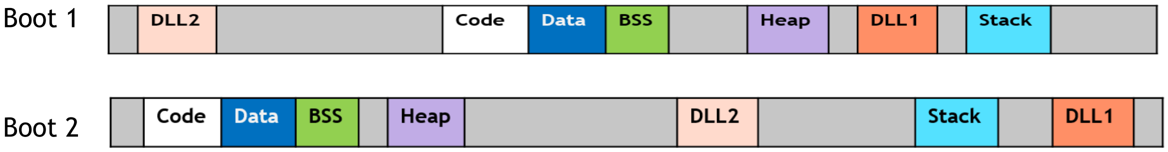
## ALE Secure Diversified Code

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

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

### Software Diversification

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



Please contact customer support for additional information.

## New / Updated Hardware Support and Guidelines

**There is no new hardware in this release.**

## 8.9R4 New Feature and Enhancements

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

### Summary Table

| Feature | OmniSwitch Platform |
|---|---|
| | |
| Management Features | |
| Signed AOS Image | 6570M |
| OmniVista Cirrus 10 LAN Management | All |
| Authorize Special Character in Admin Password | All |
| VC-of-8 Support | 6570M |
| VC-of-6 Support | 6900-X48C4E |
| Lightning Configuration Mode | 6360 |
| System Name Maximum Length | All |
| | |
| Layer 3 Features | |
| OSPFv2+OSPFv3 Multi-area Support | 6560 |
| 64 IPv6 Interfaces Support | 6560 |
| QinQ IP Interface | 6465, 6570M |
| BGP Route-filter Route-map | |
| VRF-aware Policy-based Routing | 6860N, 6900-V72/C32/X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2 |
| Advanced Routing License | 6560, 6570M |
| | |
| Service Features | |
| UNP Learned Port Security (LPS) support for MPLS/VPLS services | 6860N |
| IGMP Snooping Support over MPLS/VPLS Services | 6860N |
| DHCP v4 Snooping support over SPB/VxLAN/L2GRE/VPLS Services | 6860N, 6900-V72/C32/X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2, 9900 |
| | |
| MPLS | |
| BGP-RR support for MPLS | OS6860N |
| LDP session security & VPLS Statistics Support | OS6860N |
| | |
| Other Features | |
| BYOD web-redirection performance Improvement | 6860, 6865 |
| NISv3 Enhancements | All |
| AAA Authentication Enhancement | All |
| Support MACSec on OS99-CNI-U20 | 9900 |
| | |
| Parity Features | |

| Feature | OmniSwitch Platform |
|---|---|
| Server Load Balancing Support and Enhancements | 6860N, 6900-V72/C32/X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2 |
| RPMIR with Loopback Support | 6860, 6860N, 6865 |
| Transparent Bridging Support | 6900-V72/C32/X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2 |
| Policy Based Routing Support | 6570M, 9900 |

## Management Features

### Signed AOS Image

This feature enhancement provides the ability for an OmniSwitch 6570M to determine if the AOS software comes from a trusted source and to detect if it has been tampered with after signing. Using RSA-2048 and SHA-256, 8.9R4 AOS images are signed with a private key allowing uboot to verify the signature with a corresponding public key during boot up.

- Currently supported on OmniSwitch 6570M-12/12D/U28 models only.
- This feature requires both the uboot and AOS to be upgraded to the 8.9R4 versions.
- Once the uboot has been upgraded to 8.9R4 only signed AOS images can be loaded on the switch.
- If an unsigned AOS image (pre 8.9R4) is required to be loaded, the uboot must be downgraded to a version prior to 8.9R4.
- Uboot versions prior to 8.9R4 will work with both signed and unsigned AOS images.
- OmniSwitch 6570M switches will continue to ship from the factory with the 8.9R3 uboot version.

To recover a switch that has failed signature verification:

- If the ‘certified’ directory has a signed image, issue the ‘reset’ command at the uboot prompt to reboot the switch from the ‘certified’ directory.
- If the ‘certified’ directory does not contain a signed image, the uboot disaster recovery process must be used with 8.9R4 images.

### OVNG LAN Management

The OmniSwitch now supports remote management and monitoring through the cloud based OmniVista Cirrus 10 NMS. Leveraging the AMS application framework, the OmniSwitch enables the installation of the OmniVista Cirrus 10 Monitoring and Configuration agents, enabling a seamless push mechanism from the switch to the OmniVista NMS. The agents provides a flexible configuration framework in line with Model-based Telemetry standards like openconfig-telemetry. The solution is delivered as a Debian package that is automatically installed by OmniVista Cirrus and that integrates both Monitoring and Configuration Agents.

The following CLI commands are associated with this feature:

- **pkgmg install**
- **appmgr start ovng-agent monitoring-agent**
- **appmgr stop ovng-agent monitoring-agent**
- **appmgr start ovng-agent config-agent**
- **appmgr stop ovng-agent config-agent**
- **show appmgr**

### Authorize Special Character in Administrator Password

Prior to 8.9R4 the ‘!’ character was not allowed to be included in a user password. Starting in 8.9R04 the ‘!’ character can now be used in user passwords.

The following CLI commands are associated with this feature:

- **user** username **password** password

### VC-of-8 Support for OS6570M

The OS6570M models now support a VC of up to 8 switches. Previous releases supported a VC of up to 4 switches.

### VC-of-6 Support for OS6900-X48C4E

The OS6900-X48C4E now supports a VC of up to 6 switches. The VC can be either all OS6900-X48C4E models or it can be a mix of the OS6900-X48C4E and the OS6900-X48C6/T48C6/V48C8/C32E/T24C2/X24C2 models. In order to support a mixed VC a new vfl-type mode, either **standard** or **mixed**, is being introduced in 8.9R4.

> **Mixed Mode** - This is the only mode supported on the OS6900-X48C4E. It allows the OS6900-X48C4E to form a VC with other OS6900-X48C4E models or with OS6900-X48C6/T48C6/V48C8/C32E/T24C2/X24C2 models.
>
> **Standard Mode** - This is the default mode used on the OS6900-X48C6/T48C6/V48C8/C32E/T24C2/X24C2 models. In this mode the OS6900-X48C4E cannot be part of the VC.

- To have a mix of the OS6900-X48C4E and OS6900-X48C6/T48C6/V48C8/C32E/T24C2/X24C2 models the mode of the OS6900-X48C6/T48C6/V48C8/C32E/T24C2/X24C2 models must be changed to **mixed** and the VC must be rebooted.
- The OS6900-X48C4E supports forming a VC wth other OS6900-X48C4E models or with OS6900-X48C6/T48C6/V48C8/C32E/T24C2/X24C2 models, no other models are supported.

The following CLI commands are associated with this feature:

- **capability vfl-type {standard | mixed}**
- **show capability vfl-type**

### Lightning Configuration Mode

Lightning Configuration Mode allows an out-of-the-box, factory-default OmniSwitch 6360 to be quickly and easily deployed using a WebView quick configuration wizard. An out-of-the-box OmniSwitch 6360 will automatically be configured with a default IP address, HTTPS and DHCP functionality on port 1/1/1 and 1/1/2. This will allow an installer to connect a device to either port 1/1/1 or 1/1/2, obtain and IP address and begin a WebView session.

An administrator can create a base JSON template file with information such as switch Name, Location, IP address, DNS 1, DNS 2, DNS Domain name, Default Gateway, etc. This template can be shared with an installer, imported into WebView, modified based on a specific switch and then saved to the switch to complete the quick configuration in the field.

- Lightning Configure Mode is currently supported on as single, standalone OmniSwitch 6360.

### System Name Maximum Length

Starting in 8.9R4 the maximum length of the ‘system name’ of the switch has been increased from 32 to 64 characters.

- **system name**

## Layer 3 Features

### OSPFv2/OSPFv3 Multi-area Support on OS6560

Prior to this enhancement the OS6560 supported the configuration of an OSPF stub area only. Beginning in 8.9R4 a backbone area and any other type of OSPF area (stub, nssa or normal) can be configured on an OS6560 for both OSPFv2 and OSPFv3 with the Advanced Routing license. See table below for the supported specifications.

| | OSPFv2 | OSPFv3 |
|---|---|---|
| Maximum number of OSPF areas | 2 | 2 |
| Maximum number of interfaces | 8 | 8 |
| Maximum number of interfaces per area | 8 | 8 |
| Max number of neighbors | 8 | 8 |

The following CLI commands are associated with this feature:

- **ip ospf area**

.

### 64 IPv6 Interfaces Support

This enhancement adds support for up to 64 IPv6 interfaces on the OS6560.

### QinQ IP Interface

This feature allows SVLAN to CVLAN mapping on an IP interface. The mapping is applied for the packets flowing through the IP interface on NNI and UNI ports in SVLAN. The configuration is applied to all the ARP and IP packets on the subnet.

The following CLI is modified to allow the SVLAN to CVLAN mapping:

- **ip interface** name **address** address **mask** mask [**vlan** SVLAN] [**mapped-cvlan** CvlanId]
- **show ip interface**

### BGP Route-filter Route-map

This enhancement allows the setting of a route-tag for a BGP policy route map. This new "route-filter" route-map allows routes to get updated to the IPRM depending on the permit/deny action and matching/filtering policies defined in the route-filter route-map. This is different behavior than route-maps assigned to BGP peers, where a route is not accepted if it doesn't match on any of the policies in the associated route-map.

- **ip bgp policy route-map route-filter** *rmap_instance* **route-tag** *tag_value*

### Policy-based Routing VRF Aware

Policy Based Routing is now vrf-aware on the OS6860N, OS6900-V72/C32/X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2.

The The following CLI commands are associated with this feature:

- **policy condition**
- **policy action permanent gateway-ip**
- **show policy vrf-summary**

### Advanced Routing License

This enhancement adds support for Advanced Routing protocols on the OS6560 and OS6570M platforms with an installed license. The protocols are supported with the Advanced Routing license. The license must be installed on all elements of VC, mixing elements with and without the Advanced Routing license is not supported.

See Advanced Routing License Features for a list of licensed features.

## Service Features

### UNP Learned Port Security (LPS) support for MPLS/VPLS services

VPLS service is supported on a UNP Access port and LPS port.

- VPLS service on a UNP access port or as LPS port would be supported only on OmniSwitch 6860N.
- Both LDP and BGP signaling protocol types are supported.
- VPLS services does not support In-Line routing, hence captive-portal, BYOD and QMR (redirection) will not be supported.

The following UNP CLI commands are added and modified with this feature:

- **unp profile map service-type vpls**
- **unp vpls far-end-ip-list**
- **unp system-default vpls-signaling**
- **unp port dynamic-service vpls**
- **unp linkagg dynamic-service vpls**
- **unp port-template dynamic-service vpls**
- **show unp global configuration**
- **show unp profile map vpls**
- **show unp vpls far-end-ip-list**
- **show unp port config**

### IGMP Snooping Support over MPLS/VPLS Services

AOS supports the IGMP snooping feature on VPLS services so that each VPLS provider edge bridge performs multicast filtering on a per Service basis. When enabled on the VPLS service, the IGMP snooping logic will be applied to ensure that IP multicast traffic is not sent out of the SAP/SDP ports that have no devices requesting the specific streams.

Virtual Private LAN Service (VPLS) supports only IGMP Snooping (IPv4 Multicast Switching -IPMS)

The following CLI commands are associated with this feature:

- **ip multicast**

### DHCP v4 Snooping support over SPB/VxLAN/L2GRE/VPLS Services

DHCP Snooping is supported on a service domain. This allows the DHCP Snooping configuration on service and VLAN level. DHCP Snooping on the switch can be enabled either globally or on service and VLAN level. The following table displays the supported services on various platforms:

| Supported Platforms | Supported DHCP-Snooping on Service |
|---|---|
| 6860N | SPB, VxLAN, L2GRE, VPLS |
| 9900 | SPB, L2GRE |
| 9912 | SPB, L2GRE |
| 6900-V72/C32/X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2 | SPB, VxLAN, L2GRE |

The following CLI commands are introduced to configure the DHCP-Snooping on a service domain:

- **dhcp-snooping service** service-ID **admin-state** {enable|disable}
- **dhcp-snooping service** service-ID **mac-verification admin-state** {enable|disable}
- **dhcp-snooping service** service-ID **opt82-insertion admin-state** {enable|disable}
- **show dhcp-snooping service**

The following show commands are modified to display the DHCP-Snooping configuration on service domain:

- **dhcp-snooping binding** mac_address **port** chassis/slot/port:num **address** ip_address **service** service_ID
- **show dhcp-snooping**
- **show dhcp-snooping port**
- **show dhcp-snooping binding**

Note: DHCP Snooping is not supported in VxLAN Tandem Mode.

## MPLS Features

### BGP-RR support for MPLS

To reduce the number of BGP peering within an AS Route Reflection (RR) can be used. Rather than each BGP system having to peer with every other BGP system within the AS, each BGP speaker instead peers with a router reflector. Routing advertisements sent to the route reflector are then reflected (sent) out to all of the other BGP speakers. AOS supports BGP Route Reflection for IPv4 and IPv6 Unicast address families. For BGP VPLS route reflection, only IPv4 address family is supported.

### LDP Session Security & VPLS Statistics Support

To maintain integrity of LDP session messages and to prevent introduction of spoofed TCP segments in the LDP session connection stream, AOS provides MD5 key based authentication for LDP sessions.

MD5 key (password) for each potential LDP peer on a LDP enabled router can be configured. This key is used to compute and append a MD5 signature for each TCP segment carried by the corresponding LDP session to that peer. The peer computes the MD5 digest on the received TCP segment using locally configured shared key (password) and silently rejects the TCP segment if the computed MD5 signature does not match with received MD5 signature.

Authentication must be configured on both LDP peers using the same MD5 key (password), otherwise the peer session will not be established.

The following commands are added and modified with this feature:

- **mpls ldp neighbor <peer_address> md5 key {key | none}**
- **show mpls ldp neighbor**

AOS supports tunnel statistics for VPLS services.

The following commands are supported with this feature:

- **show service counters**
- **clear service counters**

## Other Features

### BYOD Web-redirection Performance Improvement

This feature enhances the performance of web redirection at the switch. It allows for configuring allowed servers (FQDN and IPV4) thereby processing the web redirection from a BYOD client only if the traffic is destined to one of the configured allowed servers which improves performance.

The following new CLIs are introduced to configure the web redirection:

- **unp redirect allowed-server** name **{**"fqdn string" | ipv4-address**}**
- **no unp redirect allowed-server** name
- **unp redirect allowed-server {polling-interval** min | refresh**}**
- **show unp redirect allowed-server** server-name
- **show unp fqdn resolved-ip** FQDN

### NISv3 Enhancements

As part of the NISv3 certification the following updates are made to the "secureadmin" user account:

- The minimum password length cannot be less than 9 characters and it cannot be disabled.
- The lowercase, uppercase, non-alphanumeric, and digit cannot be disabled for passwords.
- TELNET and FTP are disabled by default and cannot be enabled.
- Only HTTPS port 443 is supported.

The following CLIs are modified for "secureadmin" user:

- **user password-size** min
- **user password-policy min-lowercase**
- **user password-policy min-uppercase**
- **user password-policy min-nonalpha**
- **user password-policy min-digit**
- **user password-policy cannot-contain-consecutive-characters**
- **user password-policy cannot-contain-username**
- **ip service ftp admin-state**
- **ip service telnet admin-state**
- **show ip service**

### AAA Authentication Enhancement

In the previous behavior the switch used only the first available server configured with the ‘aaa authentication‘ command to check for user information. Starting in 8.9R4, if no user information is found on the first available server, the remaining available servers will be polled in order. If configured, the local database will be checked if no user information is found on the configured servers.

The following CLI commands are associated with this feature:

- **aaa authentication**

### Support MACSec on OS99-CNI-U20

This enhancement adds Static and Dynamic (128-bit) MACsec modes to the OS99-CNI-U20.

## Parity Features

### Server Load Balancing Support on OS6860N and OS6900 With Enhancements

Server Load Balancing is now supported on the OS6860N and the OS6900-V72/C32/X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2 models with the following enhancements.

**Multiple Policy Conditions in a Cluster -** Prior to this enhancement, a single hashing method could be configured per cluster which did not allow for two different hashing methods for the traffic bound to a cluster. This enhancement allows up to two hashing methods for a cluster to allow a value, such as the server IP address of the source and destination uni-directional flows, to be used to derive the hash value**.**

- **ip slb cluster condition *c1* condition *c2***

**Auto-Bypass -** Prior to this enhancement, when all servers of a cluster were down, traffic still matched the QoS policy rules and was dropped. With the auto-bypass enhancement, if all servers or the specified number of servers of a cluster are down the QoS policy rule will be disabled and traffic will be routed based on available routes.

- **ip slb cluster auto-bypass admin-state**
- **ip slb cluster auto-bypass inactive-servers**

**Wait-to-Restore -** This enhancement avoids immediate switchover of traffic when an inactive server becomes active again by configuring a delay before the switchover of traffic occurs.

- **ip slb cluster wait-to-restore**

### Remote Port Mirroring (RPMIR) with Loopback Support

With this enhancement RPMIR with Loopback support is added on the OS6860, OS6860N, and OS6865.

### Transparent Bridging - OS6900

This feature adds support fo transparent bridging on the 6900-V72/C32/X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2 models.

The following CLI commands are associated with this feature:

- **ethernet-services transparent-briding**
- **show ethernet-service**

### Policy Based Routing Support on OS6570M and OS9900

This enhancement adds policy based routing support on the OS6570M and OS9900.

The following CLI commands are associated with this feature:

- **policy action permanent gateway-ip**
- **policy action permanent gateway-ipv6**

## 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-3877 | On 6900 and 6900-V72, untagged packets are mirrored as tagged traffic when when monitored port is across VC chassis. On standalone box, monitored egress traffic is tagged. | Use port mirroring. |
| CRAOS8X-23137 | When a high number of VLANs are mapped to DHL links, during failover some traffic loss may be seen. | There is no known workaround at this time. |
| CRAOS8X-34219 | With a CFM2 and XNI-U48 board, port recovery after violation takes additional 2 mins with WTR of 15 seconds. | There is no known workaround at this time. |
| CRAOS8X-40728 | OS6900-V48C8 - Supports End-to-End Transparent Clock in a VC of 1 configuration at 1G/10G speeds. Not supported at 25G and 100G speeds.<br>OS6860N-P48Z - Supports End-to-End Transparent Clock in VC of 1 configuration at 1G/10G speeds. Not supported at 2.5G, 5G, and 25G. At 1G speeds with Fiber Transceivers the CF accuracy (2Way Mean) is in the range of 100ns to 200ns for traffic at packet sizes 512 and random.<br>OS6860N-U28 - Supports End-to-End Transparent Clock in VC of 1 configuration at 1G/10G speeds. Not supported at 25G speeds. At 1G speeds with Copper/Fiber Transceivers, the CF accuracy (2Way Mean) is in the range of 100ns to 350ns for traffic at packet sizes 512 and random. | There is no known workaround at this time. |
| CRAOS8X-41328 | On an OS9912 if a member port of a link aggregate with hashing/load-balancing enabled is disabled all the traffic may be sent on just one of the other ports instead of being load-balanced across the link aggregate. | There is no known workaround at this time. |
| CRAOS8X-41329 | On an OS9912 the maxpower (watts) displays incorrect values in webview when lanpower is turned off. | Use the CLI to show the accurate power consumption value when lanpower is stopped. |

| | | |
|---|---|---|
| CRAOS8X-41538 | On an OS9912 intermittent NI power-good failures may be seen after a reload for CNI-U20, CNI-U8, XNIU48 modules. | There is no known workaround at this time. |
| CRAOS8X-41742 | On an OS9912, fabric link down status may be seen during a CMM hot swap. The link will automatically recover but some packet loss may be seen. | There is no known workaround at this time. |
| CRAOS8X-41961 | On an OS9912 the 'lanpower maxpower' configuration may be missing after a reload or vctakeover. | There is no known workaround at this time. |
| CRAOS8X-44347 | The system name with a length greater than 32 characters will be truncated to the first 32 characters for inserting in the suboption of Option 82 which will be the circuit ID and remote ID. | There is no known workaround at this time. |
| CRAOS8X-44280 | The PPPoE Circuit-ID can be up to 63 characters. If the switch system name is configured with a 64 character string only first 63 characters of the system name is sent in the Circuit-ID and rest of the fields are skipped. | There is no known workaround at this time. |
| CRAOS8X-44679 | ISSU is not supported on OS6360, OS6465, OS6560, OS6570M and OS9900 from 8.9.92.R04 to 8.9.94.R04. | Use a standard upgrade. |
| Hardware / Transceivers | | |
| CRAOS8X-35256 | On 6860N 25G ports, 10G-GIG-SR/LR link up only at 10G and unable to config to 1G. | Workaround: If 1G speed is required, use single speed GIG transceivers. |
| CRAOS8X-38797 | In some situations on an OS9912, after multiple reloads and takeovers, the module in NI 2 does not come up and requires and extra reload. | AOS performs the reload automatically. |
| CRAOS8X-40689 | OS6570-U28/12 - With SFP-10G-CWDM the following issues can be seen:<br>1) 10G ports on the switch side stays up when peer side is admin-disabled.<br>2) Upon Cable removal, a switch side linkup or a LED up with link down can be seen. | Port can be recovered with a switch-side admin toggle or a transceiver hot-swap. |
| CRAOS8X-41609 | On 6860N 25G ports with a 4x10G transceiver, on intermittent admin disables one or more ports will continue to display up. | Admin enable the port when peer is disabled or disconnected or remove the transceiver. |
| CRAOS8X-41611 | OS99-CNI-U8 with 4x25G DAC cable link does not come up for certain lanes. | Use the QSFP-100G-SR4 fiber transceiver with 4X25G capability. |
| CRAOS8X-43304 | With DAC cable of any type and 100G speed, the total flap count increments one count more than expected on an OS6900-X48C4E model. | There is no known workaround at this time. |

| | | |
|---|---|---|
| CRAOS8X-43486 | On some platforms (OS6860N 25G ports, OS6900 10G and 25G ports, OS6560-P48X4 ports 53/54 and OS6360 uplink ports), the SFP-10G-GIG-LR/SR only links up at 10G and is unstable at 1G speed. | If 1G speed is required, use 1G transceivers. |
| Layer 3 | | |
| CRAOS8X-11084 | Packet drop seen in BFD config when VRRP VLAN interface is toggled. | There is no known workaround at this time. |
| CRAOS8X-33472 | When BGP peering sessions operate over an IPv6 TCP connection between two OS9900s it has been observed that there could be intermittent flapping of BGP session due to loss of TCP synchronization between the BGP routers. An error log may be observed as follows:<br>: bgp_0 tcp ERR message:<br>OS9900 vrfId 0: <,> Bad marker rcvd! Aborting peer session.<br>The BGP peering session will get re-established with no manual intervention necessary and the routing table will be restored. | There is no known workaround at this time. |
| CRAOS8X-39691 | On an OS9912 a BGP neighbor in a VRF may get stuck in idle state after NI reset if the same VLANs are associated to two different NIs. | After approximately 90 seconds the neighbor association will be restored. |
| QoS/Security | | |
| CRAOS8X-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-40948 | On an OS6900 with QMR configured, if the policy server is reloaded the switch is unable retrieve more than approximately 200 quarantined MAC addresses from OmniVista. | There is no known workaround at this time. |
| CRAOS8X-40989 | On an OS99-XNI-P24Z8 the dynamic MACsec port status is down after a reload. | Toggle the MACsec admin state on the port. |
| Services | | |
| CRAOS8X-41214 | When sending traffic on a VPLS, the MACs are not being learned on SAP access and network ports after OSPF interface toggle.  The traffic is successfully received on the egress of the and access ports. Issue is only seen when 1K MAC addresses are sent. | Resend the traffic after the toggle. Issue will not be seen with continuous traffic. |

## Hot-Swap/Redundancy Feature Guidelines

### Hot-Swap Feature Guidelines

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

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

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

**OS6860N-P48M Hot-Swap/Insertion Compatibility**

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

**OS6900 Hot-Swap/Insertion Compatibility**

| Existing Slot | Hot-Swap/Hot-Insert compatibility |
|---|---|
| Empty | All modules can be inserted |
| OS99-CMM | OS99-CMM |
| OS99-CMM2 | OS99-CMM2 |
| OS9907-CFM | OS9907-CFM |

| | |
|---|---|
| OS99-GNI-48 | OS99-GNI-48 |
| OS99-GNI-P48 | OS99-GNI-P48 |
| OS99-XNI-48 | OS99-XNI-48 |
| OS99-XNI-U48 | OS99-XNI-U48 |
| OS99-XNI-P48Z16 | OS99-XNI-P48Z16 |
| OS99-CNI-U8 | OS99-CNI-U8 |
| OS99-GNI-U48 | OS99-GNI-U48 |
| OS99-XNI-U24 | OS99-XNI-U24 |
| OS99-XNI-P24Z8 | OS99-XNI-P24Z8 |
| OS99-XNI-U12Q | OS99-XNI-U12Q |
| OS99-XNI-UP24Q2 | OS99-XNI-UP24Q2 |
| OS99-CNI-U20 | OS99-CNI-U20 |

**OS9900 Hot-Swap/Insertion Compatibility**

## Hot-Swap Procedure

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

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

## VC Hot-Swap / Removal Guidelines

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

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

## Fast/Perpetual PoE Unlike Power Supply Swapping

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

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

## Technical Support

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

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

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

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

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

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

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

### Third Party Licenses and Notices

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

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

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

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

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

## Appendix A: Feature Matrix

The following is a feature matrix for AOS Release 8.9R4.

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

| Feature | 6360 | 6465 | 6560 | OS6570M | 6860(E) | 6860N | 6865 | 6900 | 6900-V72/ C32 | 6900-X48C6/ T48C6/X48C4E/V48C8/C32E T24C2/X24C2 | 9900 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Management Features** | | | | | | | | | | | |
| AOS Micro Services (AMS) | 8.7R2 | 8.6R1 | 8.6R1 | 8.9R2 | 8.6R1 | 8.7R1 | 8.6R1 | 8.6R1 | 8.6R1 | 8.7R1 | 8.6R1 |
| Automatic Remote Configuration Download (RCL) | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.6R2 | 8.7R1 | Y |
| Automatic/Intelligent Fabric | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R2 | Y | Y | Y | Y | Y |
| Automatic VC | 8.7R2 | N | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.6R2 | 8.7R1 | N |
| Bluetooth - USB Adapter with Bluetooth Technology | 8.7R2 | 8.6R2 | 8.6R2 | 8.9R2 | Y | 8.7R1 | 8.6R2 | 8.7R1 | 8.6R2 | N | N |
| Console Disable | 8.7R2 | 8.6R2 | 8.6R2 | 8.9R2 | 8.6R2 | 8.7R1 | 8.6R2 | 8.6R2 | 8.6R2 | 8.7R1 | 8.6R2 |
| Dying Gasp | 8.9R3 | Y | Y | 8.9R3 | Y | 8.7R1 | Y | N | N | N | N |
| Dying Gasp (EFM OAM / Link OAM) | N | 8.6R1 | 8.6R1 | 8.9R3 | 8.6R1 | 8.7R1 | 8.6R1 | N | N | N | N |
| EEE support | Y | 8.9R1 | 8.9R1 | 8.9R2 | Y | 8.7R1 | Y | Y | Y | Y | Y |
| Embedded Python Scripting / Event Manager | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.7R2 | 8.7R2 | Y |
| IP Managed Services | N | N | N | N | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| Hitless Security Patch Upgrade | 8.7R2 | 8.7R1 | 8.7R1 | 8.9R2 | 8.7R1 | 8.7R1 | 8.7R1 | 8.7R1 | 8.7R1 | 8.7R1 | 8.7R1 |
| In-Band Management over SPB | N | N | N | N | 8.5R4 | 8.7R1 | 8.5R4 | 8.5R4 | 8.5R4 | 8.7R1 | 8.5R4 |
| ISSU | 8.7R2 | Y | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| NaaS | 8.8R1 | 8.8R1 | 8.8R1 | 8.9R2 | 8.8R1 | 8.8R1 | 8.8R1 | 8.8R1 | 8.8R1 | 8.8R1 | 8.8R1 |
| NAPALM Support | 8.7R2 | 8.5R1 | 8.5R1 | 8.9R2 | 8.5R1 | 8.7R1 | 8.5R1 | 8.5R1 | 8.7R2 | 8.7R2 | N |
| NTP - Version 4.2.8.p11. | 8.7R2 | 8.5R4 | 8.5R4 | 8.9R2 | 8.5R4 | 8.7R1 | 8.5R4 | 8.5R4 | 8.5R4 | 8.7R1 | 8.5R4 |
| NTP - IPv6 | 8.7R3 | 8.7R3 | 8.7R3 | 8.9R2 | 8.7R3 | 8.7R3 | 8.7R3 | 8.7R3 | 8.7R3 | 8.7R3 | 8.7R3 |
| OpenFlow | N | N | N | N | Y | N | N | Y | N | N | N |
| OV Cirrus – Zero touch provisioning | 8.7R2 | Y | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.7R2 | 8.7R2 | N |
| OV Cirrus – Configurable NAS Address | 8.7R2 | 8.5R4 | 8.5R4 | 8.9R2 | 8.5R4 | 8.7R1 | 8.5R4 | 8.5R4 | 8.5R4 | 8.7R1 | 8.5R4 |
| OV Cirrus – Default Admin Password Change | 8.7R2 | 8.5R4 | 8.5R4 | 8.9R2 | 8.5R4 | 8.7R1 | 8.5R4 | 8.5R4 | 8.5R4 | 8.7R1 | 8.5R4 |

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

| Feature | 6360 | 6465 | 6560 | OS6570M | 6860(E) | 6860N | 6865 | 6900 | 6900-V72/C32 | 6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2 | 9900 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| DHCP Relay | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R4 | 8.7R1 | Y |
| DHCPv6 Server | N | N | N | N | Y | 8.7R1 | Y | Y | 8.7R1 | 8.7R1 | Y |
| DHCPv6 Relay | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.7R1 | 8.7R1 | Y |
| DHCP Snooping / IP Source Filtering | 8.7R2 | 8.5R4 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.6R2 | 8.7R1 | Y |
| ECMP | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| IGMP v1/v2/v3 | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| GRE Tunneling | N | N | N | 8.9R4[7] | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | 8.5R2 |
| IP-IP Tunneling | N | N | N | 8.9R4[7] | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | 8.5R2 |
| IPv6 | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| IPv6 - DHCPv6 Snooping | 8.7R2 | 8.6R1 | 8.6R1 | 8.9R2 | 8.5R3 | 8.7R1 | 8.5R4 | N | 8.6R2 | 8.7R1 | 8.7R1 |
| IPv6 - Source filtering | 8.7R2 | N | 8.6R1 | 8.9R2 | 8.5R3 | 8.7R1 | 8.5R4 | N | 8.6R2 | 8.7R1 | 8.7R1 |
| IPv6 - DHCP Guard | EA | EA | EA | 8.9R2 | EA | N | EA | N | N | N | N |
| IPv6 - DHCP Client Guard | EA | EA | EA | 8.9R2 | EA | N | EA | N | N | N | N |
| IPv6 - RA Guard (RA filter) | Y | Y | 8.5R2 | 8.9R2 | Y | 8.7R1 | Y | Y | Y | Y | Y |
| IPv6 - DHCP relay and Neighbor discovery proxy | 8.7R2 | 8.5R1 | Y | N | Y | 8.7R1 | Y | Y | N | N | Y |
| IP Multinetting | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| IPSec (IPv6) | N | N | N | N | Y | 8.7R1 | Y | Y | Y | Y | Y |
| ISIS IPv4/IPv6 | N | N | N | 8.9R4[7] | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | 8.5R2 |
| M-ISIS | N | N | N | N | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | 8.5R2 |
| OSPFv2 | N | N | 8.9R4[1] | 8.9R4[7] | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| OSPFv3 | N | N | 8.9R4[1] | 8.9R4[7] | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| RIP v1/v2 | N | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| RIPng | N | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| UDP Relay (IPv4) | 8.7R2 | 8.5R4 | 8.5R4 | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R4 | 8.7R1 | 8.5R4 |
| UDP Relay (IPv6) | 8.7R2 | 8.6R1 | 8.6R1 | 8.9R2 | 8.6R1 | 8.7R1 | 8.6R | 8.6R1 | 8.6R1 | 8.7R1 | 8.6R1 |

| Feature | 6360 | 6465 | 6560 | OS6570M | 6860(E) | 6860N | 6865 | 6900 | 6900-V72/C32 | 6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2 | 9900 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| VRRP v2 | 8.7R2 | 8.5R2 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| VRRP v3 | 8.7R2 | 8.5R2 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| Server Load Balancing (SLB) | N | N | N | N | Y | 8.9R4 | Y | Y | 8.9R4 | 8.9R4 | N |
| Static routing | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| | | | | | | | | | | | |
| Multicast Features | | | | | | | | | | | |
| DVMRP | N | N | N | N | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | N |
| IP Multicast VLAN (IPMVLAN) | N | 8.9R3 | 8.9R3 Metro | 8.9R3 | N | N | N | N | N | N | N |
| IPv4 Multicast Switching | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| Multicast *,G | 8.7R2 | Y | 8.5R2 | 8.9R2 | 8.5R2 | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| IPv6 Multicast Switching | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| PIM-DM | N | N | N | 8.9R4[7] | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| PIM-SM | N | N | N | 8.9R4[7] | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| PIM-SSM | N | N | N | 8.9R4[7] | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| PIM-SSM Static Map | N | N | N | N | N | N | N | N | N | N | N |
| PIM-BiDir | N | N | N | 8.9R4[7] | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| PIM Message Packing | N | N | N | 8.9R4[7] | 8.6R1 | 8.7R1 | N | 8.6R1 | 8.6R1 | 8.7R1 | N |
| PIM - Anycast RP | N | N | N | 8.9R4[7] | 8.6R2 | 8.7R1 | 8.6R2 | 8.6R2 | 8.6R2 | 8.7R1 | 8.6R2 |
| | | | | | | | | | | | |
| Monitoring/Troubleshooting Features | | | | | | | | | | | |
| Ping and traceroute | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| Policy based mirroring | N | N | N | N | Y | 8.7R1 | Y | Y | 8.7R1 | 8.7R1 | 8.5R4 |
| Port mirroring | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| Port monitoring | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| Port mirroring - remote | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.7R2 | 8.7R2 | 8.6R1 |
| Port mirroring - remote over linkagg | N | N | 8.9R3 | N | Y | 8.7R1 | Y | Y | 8.7R2 | 8.7R2 | 8.6R1 |

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

| Feature | 6360 | 6465 | 6560 | OS6570M | 6860(E) | 6860N | 6865 | 6900 | 6900-V72/C32 | 6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2 | 9900 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 802.1p / DSCP priority mapping | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| IPv4 | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| IPv6 | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| Auto-Qos prioritization of NMS/IP Phone Traffic | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| Auto-Qos – New MAC range | 8.7R2 | 8.5R2 | 8.5R2 | 8.9R2 | 8.5R2 | 8.7R1 | 8.5R2 | 8.5R2 | 8.5R2 | 8.7R1 | 8.5R2 |
| Groups - Port | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| Groups - MAC | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| Groups - Network | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| Groups - Service | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| Groups - Map | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| Groups - Switch | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| Ingress/Egress bandwidth limit | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| Per port rate limiting | N | N | N | N | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | N |
| Policy Lists | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.7R1 | 8.7R1 | Y |
| Policy Lists - Egress | N | N | N | N | Y | 8.7R1 | Y | Y | 8.7R1 | 8.7R1 | N |
| Policy based routing | N | N | N | 8.9R4 | Y | 8.7R1 | Y | Y | 8.6R2 | 8.7R1 | 8.9R4 |
| Tri-color marking | N | N | N | N | Y | 8.7R1 | Y | Y | N | N | N |
| QSP Profiles 1 | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| QSP Profiles 2/3/4 | N | N | N | QSP-2 Only | Y | QSP-2 only | Y | Y | QSP-2 only | QSP-2 only | N |
| QSP Profiles 5 | 8.7R2 | 8.5R1 | Y | N | 8.7R1 | 8.7R1 | 8.7R1 | 8.7R1 (X72) | N | N | Y |
| RoCEv2 | N | N | N | N | N | N | N | N | 8.7R2 | N | N |
| Custom QSP Profiles | 8.7R2 | Y | Y | 8.9R2 | Y | Y | Y | X72 only (EA) | Y | Y | Y |
| GOOSE Messaging Prioritization | N | 8.7R1 | N | N | N | N | 8.7R1 | N | N | N | N |
| Metro Ethernet Features | | | | | | | | | | | |

| Feature | 6360 | 6465 | 6560 | OS6570M | 6860(E) | 6860N | 6865 | 6900 | 6900-V72/C32 | 6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2 | 9900 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| CPE Test Head | N | 8.6R1 | 8.9R1 Metro | 8.9R2 | N | N | N | N | N | N | N |
| Ethernet Loopback Test | N | Y | 8.9R1 Metro | 8.9R2 | 8.6R1 | 8.7R1 | 8.6R1 | N | N | N | N |
| Ethernet Services (VLAN Stacking) | N | 8.5R1 | 8.9R1 Metro | 8.9R2 | Y | 8.7R2 | Y | Y | 8.5R4 | 8.7R1 | N |
| Ethernet OAM (ITU Y1731 and 802.1ag) | N | 8.5R1 | 8.9R1 Metro | 8.9R2 | Y | 8.7R1 | Y | Y | 8.7R1 | 8.7R1 | EA |
| EFM OAM / Link OAM (802.3ah) | N | 8.6R1 | 8.9R1 Metro | 8.9R2 | 8.5R4 | 8.7R2 | 8.5R4 | N | N | N | N |
| PPPoE Intermediate Agent | N | 8.6R1 | 8.9R1 Metro | 8.9R2 | N | N | 8.6R1 | N | N | N | N |
| 1588v2 End-to-End Transparent Clock | N | 8.5R1 | 8.7R2 | N | Y | 8.9R3 | Y | Y (X72/Q32 ) | N | 8.9R3 (except C32E) | N |
| 1588v2 Peer-to-Peer Transparent Clock | N | 8.8R2 | 8.7R2 | N | N | N | N | N | N | N | N |
| 1588v2 Across VC | N | N | N | N | N | N | N | 8.5R2 (X72) | N | N | N |
| Access Guardian / Security Features | | | | | | | | | | | |
| 802.1x Authentication | 8.7R2 | 8.5R2 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.7R1 | 8.7R1 | Y |
| Access Guardian – Bridge | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.6R1 | 8.7R1 | Y |
| Access Guardian - Access | N | N | N | N | Y | 8.7R1 | Y | Y | 8.5R4 | 8.7R1 | Y |
| Application Fingerprinting | N | N | N | N | N | N | N | Y | N | N | N |
| Application Monitoring and Enforcement (Appmon) | N | N | N | N | Y | 8.7R2 | N | N | N | N | N |
| ARP Poisoning Protection | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R2 | 8.7R1 | Y |
| BYOD - COA Extension support for RADIUS | 8.7R2 | Y | Y | 8.9R2 | Y | 8.7R1 | Y | 8.62 | 8.6R2 | 8.7R1 | Y |
| BYOD - mDNS Snooping/Relay | 8.7R2 | Y | Y | 8.9R2 | Y | 8.7R1 | Y | 8.62 | 8.6R2 | 8.7R1 | Y |
| BYOD - UPNP/DLNA Relay | 8.7R2 | Y | Y | 8.9R2 | Y | 8.7R1 | Y | 8.62 | 8.6R2 | 8.7R1 | Y |
| BYOD - Switch Port location information pass-through in RADIUS requests | 8.7R2 | Y | Y | 8.9R2 | Y | 8.7R1 | Y | 8.62 | 8.6R2 | 8.7R1 | Y |
| Captive Portal | 8.7R2 | 8.5R4 | Y | 8.9R2 | Y | 8.7R1 | Y | 8.62 | 8.6R2 | 8.7R1 | Y |
| IoT Device Profiling | 8.7R2 | 8.5R2 | 8.5R2 | 8.9R2 | 8.5R2 | 8.7R1 | 8.5R2 | 8.5R2 | 8.6R1 | 8.7R1 | 8.5R2 |
| IoT Device Profiling (IPv6) | 8.7R2 | 8.7R1 | 8.7R1 | 8.9R2 | 8.7R1[6] | 8.9R3 | 8.7R1[6] | 8.7R1 | 8.9R3 | 8.9R3 | 8.7R1 |
| Directed Broadcasts – Control | 8.7R2 | 8.5R2 | 8.5R2 | 8.9R2 | 8.5R2 | 8.7R1 | 8.5R2 | 8.5R2 | 8.7R1 | 8.7R1 | Y |

| Feature | 6360 | 6465 | 6560 | OS6570M | 6860(E) | 6860N | 6865 | 6900 | 6900-V72/C32 | 6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2 | 9900 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Interface Violation Recovery | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.7R1 | 8.7R1 | Y |
| Kerberos Snooping (services) | 8.7R2 | Y | 8.6R2 | N | 8.6R2 | Y | 8.6R2 | 8.6R2 | 8.6R2 | Y | 8.6R2 |
| L2 GRE Tunnel Access (Edge) (bridge ports) | N | N | Y | N | Y | 8.9R1 | Y | 8.6R1[3] | N | N | Y |
| L2 GRE Tunnel Access (Edge) (access ports) | N | N | N | N | 8.6R1 | 8.9R1 | 8.6R1 | 8.6R1 | 8.7R1 | 8.7R2 | 8.6R1 |
| L2 GRE Tunnel Aggregation | N | N | N | N | Y | 8.9R1 | Y | Y[3] | 8.7R1 | 8.7R2 | Y |
| Learned Port Security (LPS) | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.5R4 | 8.7R1 | Y |
| MACsec[4] | N | 8.5R1 | 8.5R4 | N | Y | 8.7R1 | N | N | N | X48C4E | 8.5R2 |
| MACsec MKA Support[4] | N | 8.5R2 | 8.5R4 | N | 8.5R2 | 8.7R1 | N | N | N | X48C4E | 8.5R2 |
| MACsec on Network Port for SPB/L2GRE/VxLAN | N | N | N | N | 8.9R1 (6860E) | 8.9R1 | N | N | N | 8.9R1 (X48C4E) | N |
| Quarantine Manager | N | 8.7R2 | 8.7R2 | 8.9R2 | Y | 8.7R2 | Y | 8.7R2 | 8.7R2 | 8.7R2 | 8.7R2 |
| RADIUS - RFC-2868 Support | 8.7R2 | 8.5R4 | 8.5R4 | 8.9R2 | 8.5R4 | 8.7R1 | 8.5R4 | 8.5R4 | 8.5R4 | 8.7R1 | 8.5R4 |
| Role-based Authentication for Routed Domains | N | N | N | N | 8.5R4 | 8.7R1 | 8.5R4 | 8.5R4 | 8.6R1 | 8.7R1 | 8.5R4 |
| Storm Control (flood-limit) | 8.7R2 | Y | Y | 8.9R2 | Y | 8.7R1 | Y | Y | Y | 8.7R1 | Y |
| Storm Control (Unknown unicast with action trap/shutdown) | N | N | N | N | Y | N | Y | Y | N | N | N |
| TACACS+ Client | 8.7R2 | 8.5R1 | Y | 8.9R2 | Y | 8.7R1 | Y | Y | 8.6R1 | 8.7R1 | Y |
| TACACS+ command based authorization | 8.7R2 | N | N | 8.9R2 | Y | 8.7R1 | Y | Y | 8.7R2 | 8.7R2 | N |
| TACACS+ - IPv6 | 8.7R3 | 8.7R3 | 8.7R3 | 8.9R2 | 8.7R3 | 8.7R3 | 8.7R3 | 8.7R3 | 8.7R3 | 8.7R3 | 8.7R3 |
| PoE Features | | | | | | | | | | | |
| 802.3af and 802.3at | 8.7R2 | 8.5R1 | Y | N | Y | 8.7R1 | Y | N | N | N | Y |
| 802.3bt | 8.7R2 | Y | 8.6R2 | N | N | 8.7R1 | N | N | N | N | N |
| Auto Negotiation of PoE Class-power upper limit | 8.7R2 | 8.5R1 | Y | N | Y | 8.7R1 | Y | N | N | N | Y |
| Display of detected power class | 8.7R2 | 8.5R1 | Y | N | Y | 8.7R1 | Y | N | N | N | Y |
| LLDP/802.3at power management TLV | 8.7R2 | 8.5R1 | Y | N | Y | 8.7R1 | Y | N | N | N | Y |
| HPOE support | 8.7R2 (95W) | 8.5R1 (60W) | Y (95W) | N | Y (60W) | 8.7R1 (95W) | Y (75W) | N | N | N | Y (75W) |
| Time Of Day Support | 8.7R2 | 8.5R1 | Y | N | Y | | Y | N | N | N | Y |
| Perpetual PoE | 8.7R2 | N | N | N | Y | Y | Y | N | N | N | N |

| **Feature** | **6360** | **6465** | **6560** | **OS6570M** | **6860(E)** | **6860N** | **6865** | **6900** | **6900-V72/C32** | **6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2** | **9900** |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Fast PoE | 8.7R2 | N | N | N | Y | Y | Y | N | N | N | N |
| Delayed Start | 8.9R3 | 8.9R3 | 8.9R3 | N | N | N | N | N | N | N | N |
| Data Center Features (License May Be Required) | | | | | | | | | | | |
| CEE DCBX Version 1.01 | N | N | N | N | N | N | N | Y | N | N | N |
| Data Center Bridging (DCBX/ETS/PFC) | N | N | N | N | N | N | N | Y | N | N | N |
| EVB | N | N | N | N | N | N | N | N | N | N | N |
| FCoE / FC Gateway | N | N | N | N | N | N | N | Y | N | N | N |
| VXLAN[5] | N | N | N | N | N | 8.8R1 | N | Q32/X72 | 8.5R3 | 8.8R1 | N |
| VM/VXLAN Snooping | N | N | N | N | N | N | N | Y | N | N | N |
| FIP Snooping | N | N | N | N | N | N | N | Y | N | N | N |

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

## Appendix B: MACsec Platform Support

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

| MACsec Support<br>(MACsec site license required) | |
|---|---|
| | |
| **OmniSwitch 9900** | |
| OS99-CMM | 4X10G mode only - Static and Dynamic (128-bit) modes |
| OS99-CMM2 | Not Supported |
| OS99-GNI-48/P48 | 10M/100M/1G ports - Static and Dynamic (128-bit) modes |
| OS99-XNI-48/P48 | 10G ports - Static and Dynamic (128-bit) modes |
| OS99-XNI-U48 | 10G ports - Static and Dynamic (128-bit) modes |
| OS99-XNI-P48Z16 | 1G/2.5G/5G/10G (16x) - Static and Dynamic (128-bit) modes<br>1G/10G (32x) - Static and Dynamic (128-bit) modes |
| OS99-GNI-U48 | 1G ports - Static and Dynamic (128-bit) modes |
| OS99-XNI-U24 | 10G ports - Static and Dynamic (128-bit) modes |
| OS99-XNI-P24Z8 | 1G/2.5G/5G/10G (8x) - Static and Dynamic (128-bit) modes<br>1G/10G (16x) - Static and Dynamic (128-bit) modes |
| OS99-XNI-U12Q | 10G / 4x10G Uplink - Static and Dynamic (128-bit) modes |
| OS99-XNI-UP24Q2 | 10G(Fiber)/4x10G Uplink - Static and Dynamic (128-bit) modes<br>10G (Copper) - Static and Dynamic (128-bit) modes |
| OS99-CNI-U8 | Not Supported |
| OS99-CNI-U20 | 40G/100G - Static and Dynamic (128-bit) modes |
| | |
| **OmniSwitch 6900** | |
| OS6900-X48C4E | Dynamic mode only on all ports. Supports 256-bit key length. |
| | |
| **OmniSwitch 6860(E)** | |
| OS6860(E) | All models support MACsec on 10G ports. |
| OS6860E-P24 | 1G/10G ports. |
| OS6860E-P24Z8 | 1G/10G ports (not supported on 2.5G ports). |
| | |
| **OmniSwitch 6860N** | Dynamic mode only. All OS6860N models support 256-bit key length. |
| OS6860N-U28 | SFP (1-24), SFP+ (25-28) and SFP28 (31-34) ports |
| OS6860N-P48Z | SFP28 (51-54) ports |
| OS6860N-P48M | - Expansion modules (Not supported on any 4X10G splitter transceivers).<br>- Multi-rate Gigabit Ports (37-48) |
| OS6860N-P24Z | SFP28 (27-30) ports |
| OS6860N-P24M | - Expansion modules (Not supported on any 4X10G splitter transceivers)<br>- Multi-rate Gigabit Ports (1-24) |
| | |
| **OmniSwitch 6560** | |
| OS6560-P24X4/24X4 | - Ports 1-24 (Static and Dynamic modes)<br>- Ports 25-30 (Not Supported) |
| OS6560-P48X4/48X4 | - Ports 1-48 (Static and Dynamic modes)<br>- Ports 49-52 (Dynamic mode only)<br>- Ports 53-54 (Not Supported) |
| OS6560-P48Z16<br>(904044-90 only) | - Ports 1-32 (Static and Dynamic Modes)<br>- Ports 33-48 (Static and Dynamic modes)<br>- Ports 49-52 (Dynamic mode only)<br>- Ports 53-54 (Not Supported) |
| OS6560-X10 | - Ports 1-8 (10G ports only. Dynamic mode only)<br>- Ports 9-10 (Not Supported) |
| | |
| **OmniSwitch 6465** | - OS6465-P28 - supported on all ports except ports 27 and 28. |

| | |
|---|---|
| | - OS6465T-12 and OS6465T-P12 – Not supported on ports 11 and 12.<br>- All other models support MACsec on all ports. |

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

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

| Inline Routing Support | | | | | | | |
|---|---|---|---|---|---|---|---|
| | OmniSwitch 9900 | OmniSwitch 6900-V72/C32 (Front panel port) | OmniSwitch 6900-T48C6/X48C6 | OmniSwitch 6900-X48C4E/V48C8 | OmniSwitch 6900-C32E | OmniSwitch 6860N | OmniSwitch 6900-X/T24C2 |
| **IPv4 Protocols** | | | | | | | |
| Static Routing | Y | 8.6R2 | 8.7R2 | 8.7R3 | 8.8R1 | 8.7R2 | 8.9R1 |
| RIP v1/v2 | Y | 8.6R2 | 8.7R2 | 8.7R3 | 8.8R1 | 8.7R2 | 8.9R1 |
| OSPF | Y | 8.6R2 | 8.7R2 | 8.7R3 | 8.8R1 | 8.7R2 | 8.9R1 |
| BGP | Y | 8.6R2 | 8.7R2 | 8.7R3 | 8.8R1 | 8.7R2 | 8.9R1 |
| VRRP | Y | 8.7R1 | 8.7R2 | 8.7R3 | 8.8R1 | 8.7R2 | 8.9R1 |
| IS-IS | N | N | N | N | N | N | N |
| PIM-SM/DM | 8.5R3 | 8.6R2 | Y | Y | 8.8R1 | Y | 8.9R1 |
| DHCP Relay | 8.5R3 | 8.6R2 | 8.7R2 | 8.7R3 | 8.8R1 | 8.7R2 | 8.9R1 |
| UDP Relay | 8.5R4 | 8.6R2 | 8.7R2 | 8.7R3 | 8.8R1 | 8.7R2 | 8.9R1 |
| DVMRP | N | N | N | N | N | N | N |
| BFD | 8.7R2 | 8.7R2 | 8.7R2 | 8.7R3 | 8.8R1 | 8.7R2 | 8.9R1 |
| IGMP Snooping | Y | 8.6R2 | 8.7R2 | 8.7R3 | 8.8R1 | 8.7R2 | 8.9R1 |
| IP Multicast Headend Mode | Y | 8.6R2 | 8.7R2 | 8.7R3 | 8.8R1 | 8.7R2 | 8.9R1 |
| IP Multicast Tandem Mode | 8.5R4 | 8.6R2 | 8.8R1 | 8.8R1 | 8.8R1 | 8.8R1 | 8.9R1 |
| | | | | | | | |
| **IPv6 Protocols** | | | | | | | |
| Static Routing | 8.5R4 | 8.6R2 | 8.7R2 | 8.7R3 | 8.8R1 | 8.7R2 | 8.9R1 |
| RIPng | 8.5R4 | 8.6R2 | 8.7R2 | 8.7R3 | 8.8R1 | 8.7R2 | 8.9R1 |
| OSPFv3 | 8.5R4 | 8.6R2 | 8.7R2 | 8.7R3 | 8.8R1 | 8.7R2 | 8.R1 |
| BGP | 8.5R4 | 8.6R2 | 8.7R2 | 8.7R3 | 8.8R1 | 8.7R2 | 8.9R1 |
| VRRPv3 | 8.5R4 | 8.7R1 | 8.7R2 | 8.7R3 | 8.8R1 | 8.7R2 | 8.9R1 |
| IS-IS | N | N | N | N | N | N | N |
| PIM-SM/DM | 8.5R4 | 8.6R2 | 8.8R1 | 8.8R1 | 8.8R1 | 8.8R1 | 8.9R1 |
| DHCP Relay | 8.6R1 | 8.7R2 | 8.7R2 | 8.7R3 | 8.8R1 | 8.7R2 | 8.9R1 |
| UDP Relay | 8.6R1 | 8.7R2 | 8.7R2 | 8.7R3 | 8.8R1 | 8.7R2 | 8.9R1 |
| BFD | 8.7R2 | 8.7R2 | 8.7R2 | 8.7R3 | 8.8R1 | 8.7R2 | 8.9R1 |
| IPv6 MLD Snooping | Y | 8.7R2 | 8.7R2 | 8.7R3 | 8.8R1 | 8.7R2 | 8.9R1 |
| IPv6 Multicast Headend Mode | Y | 8.7R2 | 8.7R2 | 8.7R3 | 8.8R1 | 8.7R2 | 8.9R1 |
| IPv6 Multicast Tandem Mode | 8.5R4 | 8.7R2 | 8.8R1 | 8.8R1 | 8.8R1 | 8.8R1 | 8.9R1 |

| External Loopback Support | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | OmniSwitch 9900 | OmniSwitch 6860/6865 | OmniSwitch 6860N | OmniSwitch 6900 | OmniSwitch 6900-V72/ C32 | OmniSwitch 6900-X48C6/ T48C6 | OmniSwitch 6900-X48C4E | OmniSwitch 6900-V48C8 | OmniSwitch 6900- X/T48C2 |
| **IPv4 Protocols** | | | | | | | | | |
| Static Routing | 8.5R4 | Y | 8.7R1 | Y | 8.5R4 | 8.7R1 | 8.7R2 | 8.7R3 | 8.9R1 |
| RIP v1/v2 | 8.5R4 | Y | 8.7R1 | Y | 8.5R4 | 8.7R1 | 8.7R2 | 8.7R3 | 8.9R1 |
| OSPF | 8.5R4 | Y | 8.7R1 | Y | 8.5R4 | 8.7R1 | 8.7R2 | 8.7R3 | 8.9R1 |
| BGP | 8.5R4 | Y | 8.7R1 | Y | 8.5R4 | 8.7R1 | 8.7R2 | 8.7R3 | 8.9R1 |
| VRRP | 8.6R1 | 8.5R4 | 8.7R1 | Y | 8.7R1 | 8.7R2 | 8.7R2 | 8.7R3 | 8.9R1 |
| IS-IS | Y | Y | Y | Y | Y | Y | 8.7R2 | 8.7R3 | 8.9R1 |
| PIM-SM/DM | 8.5R4 | Y | 8.7R1 | Y | 8.5R4 | 8.7R1 | 8.7R2 | 8.7R3 | 8.9R1 |
| DHCP Relay | 8.5R4 | 8.5R4 | 8.7R1 | 8.5R4 | 8.5R4 | 8.7R1 | 8.7R2 | 8.7R3 | 8.9R1 |
| UDP Relay | 8.5R4 | 8.5R4 | 8.7R1 | 8.5R4 | 8.5R4 | 8.7R1 | 8.7R2 | 8.7R3 | 8.9R1 |
| DVMRP | N | N | N | N | N | N | N | N | N |
| BFD | Y | Y | Y | Y | Y | Y | 8.7R2 | 8.7R3 | 8.9R1 |
| IGMP Snooping | 8.5R4 | Y | 8.7R1 | Y | 8.6R1 | 8.7R1 | 8.7R2 | 8.7R3 | 8.9R1 |
| IP Multicast Headend Mode | 8.5R4 | Y | 8.7R1 | Y | 8.6R1 | 8.7R1 | 8.7R2 | 8.7R3 | 8.9R1 |
| IP Multicast Tandem Mode | 8.5R4 | Y | 8.7R1 | Y | 8.6R1 | Y | Y | Y | 8.9R1 |
| | | | | | | | | | |
| **IPv6 Protocols** | | | | | | | | | |
| Static Routing | 8.5R4 | Y | 8.7R1 | Y | 8.5R4 | 8.7R1 | 8.7R2 | 8.7R3 | 8.9R1 |
| RIPng | 8.5R4 | Y | 8.7R1 | Y | 8.5R4 | 8.7R1 | 8.7R2 | 8.7R3 | 8.9R1 |
| OSPFv3 | 8.5R4 | Y | 8.7R1 | Y | 8.5R4 | 8.7R1 | 8.7R2 | 8.7R3 | 8.9R1 |
| BGP | 8.5R4 | Y | 8.7R1 | Y | 8.5R4 | 8.7R1 | 8.7R2 | 8.7R3 | 8.9R1 |
| VRRPv3 | 8.5R4 | 8.5R4 | 8.7R1 | Y | 8.7R1 | 8.7R2 | 8.7R2 | 8.7R3 | 8.9R1 |
| IS-IS | Y | Y | Y | Y | Y | Y | 8.7R2 | 8.7R3 | 8.9R1 |
| PIM-SM/DM | 8.5R4 | 8.5R4 | 8.7R1 | 8.5R4 | 8.5R4 | 8.7R1 | 8.7R2 | 8.7R3 | 8.9R1 |
| DHCP Relay | 8.6R1 | 8.6R1 | 8.7R1 | 8.6R1 | 8.6R1 | 8.7R1 | 8.7R2 | 8.7R3 | 8.9R1 |
| UDP Relay | 8.6R1 | 8.6R1 | 8.7R1 | 8.6R1 | 8.6R1 | 8.7R1 | 8.7R2 | 8.7R3 | 8.9R1 |
| BFD | Y | Y | Y | Y | Y | Y | 8.7R2 | 8.7R3 | 8.9R1 |
| IPv6 MLD Snooping | 8.5R4 | Y | 8.7R1 | Y | Y | 8.7R2 | 8.7R2 | 8.7R3 | 8.9R1 |
| IPv6 Multicast Headend Mode | 8.5R4 | Y | 8.7R1 | Y | Y | 8.7R2 | 8.7R2 | 8.7R3 | 8.9R1 |
| IPv6 Multicast Tandem Mode | 8.5R4 | Y | 8.7R1 | Y | Y | Y | Y | Y | 8.9R1 |

## SPB BVLAN Scalability and Convergence Guidelines

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

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

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

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

```
OS6860-> show spb isis bvlans
SPB ISIS BVLANS:
                                                              Services  Num    Tandem
Root Bridge
BVLAN   ECT-algorithm     In Use  mapped    ISIDS  Multicast  (Name : MAC Address)
-------+-----------------+-------+---------+------+----------+-------------------------------
---------
  4000  00-80-c2-01       YES     YES           5  SGMODE
  4001  00-80-c2-02       NO      NO            0  SGMODE
```

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

## Appendix D: General Upgrade Requirements and Best Practices

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

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

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

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

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

## Supported Upgrade Paths and Procedures

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

| Platform | AOS Releases Supporting ISSU to 8.9.94.R04 (GA) |
|---|---|
| OS6360 | 8.9.221.R03 (Major GA)<br>8.9.107.R02 (Minor GA)<br>8.9.73.R01 (Major GA)<br>8.8.56.R02 (Minor GA)<br>8.8.152.R01 (Major GA) |
| OS6360-P10A | 8.9.221.R03 (Major GA)<br>8.9.107.R02 (Minor GA)<br>8.9.73.R01 (Major GA)<br>8.8.8.R03 (Minor GA) –<br>Note: Uses same image file as other OS6360 platforms. |
| OS6465 | 8.9.221.R03 (Major GA)<br>8.9.107.R02 (Minor GA)<br>8.9.73.R01 (Major GA)<br>8.8.56.R02 (Minor GA)<br>8.8.152.R01 (Major GA) |
| OS6560 | 8.9.221.R03 (Major GA)<br>8.9.107.R02 (Minor GA)<br>8.9.73.R01 (Major GA)<br>8.8.56.R02 (Minor GA)<br>8.8.152.R01 (Major GA) |
| OS6570M | 8.9.221.R03 (Major GA)<br>8.9.107.R02 (Minor GA)<br>8.9.63.R02 (Major GA) |
| OS6860(E) | 8.9.92.R04 (Major GA)<br>8.9.221.R03 (Major GA)<br>8.9.107.R02 (Minor GA)<br>8.9.73.R01 (Major GA)<br>8.8.56.R02 (Minor GA)<br>8.8.152.R01 (Major GA) |
| OS6860N | 8.9.92.R04 (Major GA)<br>8.9.221.R03 (Major GA)<br>8.9.107.R02 (Minor GA)<br>8.9.73.R01 (Major GA)<br>8.8.56.R02 (Minor GA)<br>8.8.153.R01 (Major GA) |
| OS6865 | 8.9.92.R04 (Major GA)<br>8.9.221.R03 (Major GA)<br>8.9.107.R02 (Minor GA)<br>8.9.73.R01 (Major GA)<br>8.8.56.R02 (Minor GA)<br>8.8.152.R01 (Major GA) |
| OS6900-X20/X40/T20/T40/Q32/X72 | 8.9.92.R04 (Major GA)<br>8.9.221.R03 (Major GA)<br>8.9.107.R02 (Minor GA) |

| | |
|---|---|
| | 8.9.78.R01 (Major GA)<br>8.8.56.R02 (Minor GA)<br>8.8.152.R01 (Major GA) |
| OS6900-V72/C32/C32E X48C6/T48C6/V48C8 | 8.9.92.R04 (Major GA)<br>8.9.221.R03 (Major GA)<br>8.9.107.R02 (Minor GA)<br>8.9.78.R01 (Major GA)<br>8.8.56.R02 (Minor GA)<br>8.8.153.R01 (Major GA)<br>8.8.152.R01 (Major GA) |
| OS6900-X24C2/T24C2 | 8.9.92.R04 (Major GA)<br>8.9.221.R03 (Major GA)<br>8.9.107.R02 (Minor GA)<br>8.9.78.R01 (Major GA) |
| OS9900 (OS9907) | 8.9.221.R03 (Major GA) |

**8.9R4 ISSU Supported Releases**

## Prerequisites

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

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

- The AOS Switch Management Guide
    - Chapter – Getting Started
    - Chapter - Logging Into the Switch
    - Chapter - Managing System Files
    - Chapter - Managing CMM Directory Content
    - Chapter - Using the CLI
    - Chapter - Working With Configuration Files
    - Chapter - Configuring Virtual Chassis

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

## Switch Maintenance

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1. Download the Upgrade Files

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

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

2. FTP the Upgrade Files to the Switch

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

3. Upgrade the image file

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

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

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

4. Verify the Software Upgrade

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

```
OS6900-> show microcode
/flash/working
Package           Release                 Size     Description
-----------------+-----------------------+--------+------------------------------------
Tos.img           8.9.94.R04             239607692 Alcatel-Lucent OS


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

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

5. Certify the Software Upgrade

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

```
OS6900-> copy running certified

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

## Appendix F: ISSU – OmniSwitch Chassis or Virtual Chassis

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

1. Download the Upgrade Files

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

- OS6360 – Nosa.img
  - Refer to Appendix G for recommended/required FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6465 – Nos.img
  - Refer to Appendix G for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6560 – Nos.img
  - Refer to Appendix G for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6570M – Wos.img
  - Refer to Appendix G for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6860 – Uos.img
  - Refer to Appendix G for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6860N – Uosn.img
  - Refer to Appendix H for recommended CPLD upgrades. AOS must be upgraded prior to upgrading the CPLD.
- OS6865 – Uos.img
  - Refer to Appendix G for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6900 **-** Tos.img
  - Refer to Appendix G for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6900-V72/C32/X48C6/T48C6/X48C4E/V48C8 – Yos.img.
  - Refer to Appendix H for recommended CPLD upgrades. AOS must be upgraded prior to upgrading the CPLD.
- OS9900 – Mos.img, Mhost.img, Meni.img
- ISSU Version File – issu_version
- imgsha256sum (not required) –This file is only required when running in Common Criteria mode. Please refer to the Common Criteria Operational Guidance Document for additional information.

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

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

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

3. Clean up existing ISSU directories
(**Note**: If upgrading a standalone (VC-of-1), modular OS9900 with dual CMMs, skip to step 7).

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

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

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

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

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

```
6900-> rm –r /flash/issu_dir
```

6. Log out of the Slave chassis:

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

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

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

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

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

9. Upgrade the image files using ISSU:

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

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

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

This indicates that the ISSU is completed

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

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

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

10. Verify the Software Upgrade

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

```
OS6900-> show microcode

/flash/working

Package           Release                 Size      Description

-----------------+-----------------------+--------+----------------------------------

Tos.img           8.9.94.R04              239607692 Alcatel-Lucent OS
```

11. Certify the Software Upgrade

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

```
OS6900-> write memory flash-synchro

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

## Appendix G: FPGA / U-boot Upgrade Procedure

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

| CR / Feature | Summary | |
|---|---|---|
| CRAOS8X-12042 | Description | Switch does not shutdown after crossing danger threshold temperature. |
| | FPGA Version | 0.7 |
| | Platforms | OS6465-P28 |
| CRAOS8X-7207 | Description | Chassis reboots twice to join a VC. |
| | FPGA Version | 0.7 |
| | Platforms | OS6560-P24Z24,P24Z8,P48Z16 (903954-90) |
| CRAOS8X-4150 | Description | VC LED status behavior. |
| | U-boot Version | 0.12 |
| | Platforms | OS6865-U28X |
| 8.7R1 Release | | |
| CRAOS8X-16452 | Description | Port remains UP when only SFP is connected. |
| | FPGA Version | - 0.6 (OS6560-P48Z16 (904044-90))<br>- 0.7 (OS6560-48X4, OS6560-P48X4)<br>- 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<br>- FPGA version 0.1.11 |
| | Platforms | OS6900-X72 |
| Fast/Perpetual PoE | Description | Fast and Perpetual PoE Support |
| | FPGA Version | 0.7 (OS6860E-P24Z8)<br>0.10<br>0.14 (OS6865-U28X)<br>0.25 (OS6865-P16X/U12X) |
| | Platforms | OS6860/OS6865 |
| 8.7R2 Release | | |
| CRAOS8X-4813/13440 | Description | Uboot unable to mount NAND flash with UBIFS errors |
| | U-boot Version | 8.7.2.R02 |
| | Platforms | OS6465(T), 6560-24X4/P24X4/48X4/P48X4/X10 |
| CRAOS8X-13819 | Description | Uboot unable to mount eUSB flash |
| | U-boot Version | 8.7.2.R02 |
| | Platforms | OS6560-24Z24/P24Z24/24Z8/P24Z8/P48Z16 (all PNs), 6865 |
| CRAOS8X-22857 | Description | OS6560-P24Z24 reloads continuously with pmds |
| | FPGA Version | 0.8 |
| | Platforms | OS6560-24Z24/P24Z24/24Z8/P24Z8/P48Z16 (903954-90) |
| 1588v2 Support | Description | 1588v2 Support |
| | FPGA Version | 0.7 (OS6560-P48Z16 (904044-90))<br>0.8 (OS6560-48X4/P48X4) |
| | Platforms | OS6560-48X4/P48X4/P48Z16(904044-90)<br>Supported on 1G and 10G ports only.  Not supported 2.5G ports. |

| | | |
|---|---|---|
| U-boot Password Authentication | Description | U-boot password support (Early Availability) |
| | U-boot Version | 8.7.2.R02 |
| | Platforms | OS6465 |
| 8.7R3 Release | | |
| CRAOS8X-26370<br>CRAOS8X-25033 | Description | Required upgrade to enable 12V Power Fail Interrupt (CRAOS8X-26370).<br>Required upgrade to address fan speed issue. (CRAOS8X-25033) |
| | FPGA Version | 0.17 |
| | Platforms | OS6360-24/P24/48/P48 |
| CRAOS8X-24464 | Description | Uboot update for CRAOS8X-24464, ability to disable / authenticate uboot access. |
| | Uboot Version | 8.7.30.R03 |
| | Platforms | OS6360, 6465, 6560, 6860, 6865, 6900, 9900. (Not applicable for platforms that use ONIE) |
| 8.8R1 Release | | |
| Boot from USB | Description | Uboot update to allow switch to boot from USB. |
| | Uboot Version | 8.8.33.R01 |
| | Platforms | OS6465, OS6865 |
| 8.8R2 Release | | |
| Future compatibility | Description | Uboot/FPGA update to allow future CMM2/OS9912 NI compatibility. |
| | Uboot/FPGA Versions | See OS9900 Table for versions. |
| | Platforms | 9907 |
| 8.9R1 Release | | |
| N/A | There are no Uboot/FPGA upgrade requirements in this release. | |
| 8.9R2 Release | | |
| Fan Speed | Description | Reduced fan speed at boot-up |
| | FPGA Version | 0.20 |
| | Platforms | OS6360-(P)24/(P)48/PH48 |
| CRAOS8X_35470 and CPLD Support | Description | Uboot fix for NAND flash bad file system block.<br>Support of Gowin CPLD[1] |
| | Uboot | 8.9.85.R02 |
| | Platforms | OS6360 (All) |
| CPLD Support | Description | Support of Gowin CPLD[1] |
| | Uboot | 8.9.92.R02 |
| | Platforms | OS6570M-12/12D/U28 |
| CRAOS8X_35470 | Description | Uboot fix for NAND flash bad file system block |
| | Uboot/FPGA Versions | 8.9.85.R02 |
| | Platforms | OS6465 (All), OS6560-(P)24X4/(P)48X4/X10 |
| 1. Existing switches do not contain the new CPLD component and do not need to upgrade. Switches with the new CPLD component will ship from the factory with the correct version. | | |
| 8.9R3 Release | | |
| CRAOS8X-40924 | Description | Address issue when disabling uboot access. |
| | Uboot Version | 8.9.139.R03 |
| | Platforms | OS6570M-12/12D/U28 |

| | | |
|---|---|---|
| Power Supply Interrupt | Description | Address power supply interrupt issue. |
| | FPGA Version | 0.12 |
| | Platforms | OS6570M-U28 |
| 8.9R4 Release | | |
| Signed AOS Images | Description | Adds support for signed images when used with AOS 8.9R4 GA release. |
| | Uboot Version | 8.9.70.R04 |
| | Platforms | OS6570M-12/12D/U28 |
| | | |

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

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

- CPLD File - fpga_kit_8405
- U-boot.8.9.R04.70.tar.gz

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

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

```
-> update fpga-cpld cmm all file fpga_kit_8405
Parse /flash/fpga_kit_8405
fpga file: OS6360-10_CPLD_V19_20230110.vme
Please wait...
fpga file: OS6360-10_CPLD_V19_20230110.vme
update chassis 1
Starting CMM ALL FPGA Upgrade
CMM 1/1
Successfully updated
Reload required to activate new firmware.
```

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

```
-> update uboot cmm all file /flash/u-boot.8.9.R04.70.tar.gz
Starting CMM ALL UBOOT Upgrade
Please wait...
CMM 1/1
u-boot-ppc_2040.bin: OK
U-boot successfully updated
Successfully updated
```

5. Once complete, a reboot is required.

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

The following CRs or features can be addressed by performing a CPLD upgrade on the respective models. Follow the guidelines in the General Upgrade Requirements and Best Practices appendix prior to upgrading.

| | | |
|---|---|---|
| 8.8R2 Release | | |
| **OS6860N-P48M/P48Z/P24M/P24Z** | | |
| CRAOS8X-29731/30471 | Description | OS6860N power supplies |
| | CPLD File | os6860n_p48m_p48z_u28_maincpu_20220318.updater<br>os6860n_p24m_p24z_maincpld_22020309.updater |
| 8.9R1 Release | | |
| **OS6900-T48C6** | | |
| CRAOS8X-30098 | Description | Fixed I2C lockup issue on CPU board.<br>(Please refer to CRAOS8X-30098 for additional details) |
| | CPLD File | denverton_cpucpld_v0b.02.0eh_20211124.jbc.updater |
| No CR | Description | Improved power down sequence when PSU shut down. |
| | CPLD File | os6900_t48c6_mainpld_v1.03.02.04.jbc.updater |
| **OS6900-X48C6** | | |
| CRAOS8X-30098 | Description | Fixed I2C lockup issue on CPU board.<br>(Please refer to CRAOS8X-30098 for additional details) |
| | CPLD File | denverton_cpucpld_v0b.02.0eh_20211124.jbc.updater |
| No CR | Description | Improved power down sequence when PSU shut down. |
| | CPLD File | os6900_x48c6_mainpldall_bp_v1.03.02.02h.jbc.updater |
| **OS6900-X48C4E** | | |
| CRAOS8X-30098 | Description | Fixed I2C lockup issue on CPU board.<br>(Please refer to CRAOS8X-30098 for additional details) |
| | CPLD File | OS6900_XC48C4E_MAIN_CPU_FAN_CPLD_2e3228_20220322.updater |
| 8.9R4 Release | | |
| **OS6900-X48C4E** | | |
| CRAOS8X-43968 | Description | Fixed temperature error on OS6900-X48C4E (Hardware revision: 6) with a single power supply. |
| | CPLD File | updater_kit_8629 (version 2.15) |
| **No other CPLD upgrades are available or required.** | | |
| **Notes:**<br>1. Upgrading the CPLD on ONIE-based models using an updater kit is supported beginning with AOS Release 8.9.R03.<br>2. The updater kit contains all the necessary individual updater files.<br>3. CPLD versions are compatible with previous AOS releases. Downgrading to a previous AOS release is supported:<br>a. Backup the configuration files from previous release.<br>b. Upgrade to AOS Release 8.9.R03.<br>c. Upgrade the CPLD.<br>d. Downgrade to previous release. (ISSU is not supported when downgrading AOS)<br>e. Restore the configuration. | | |

**Note: AOS must be upgraded to 8.9R4 prior to performing a CPLD upgrade using the updater kit.**

ONIE-based platforms contain multiple CPLDs. The upgrade process will pick the correct updater file from the kit based on the platform and the CPLD type. The procedure will check for a version mismatch and upgrade the CPLD one at a time (i.e. Main board or CPU board). The CPLD will be upgraded one at a time so it may be necessary to run the command multiple times. If no upgrade is required, the command will display a message indicating there are no pending upgrades. See example below (file and product names will vary).

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

- CPLD Kit – updater_kit_8629

2. Ensure the configuration is certified and synchronized prior to upgrading the CPLD. It's recommended to have a console connection in case there are any issues during the CPLD upgrade procedure.

3. FTP (Binary) the updater kit to the **/flash** directory on the primary CMM.

4. Enter the following to upgrade the CPLD. Use the '**all**' parameter to upgrade each element in a VC, for example:

```
-> update fpga-cpld all 1/1 file updater_kit_8629
Starting CMM 1/1  FPGA Upgrade
CMM 1/1
starting onie update
Removing firmware update results: OS6900_XC48C4E_MAIN_CPU_FAN_CPLD_2f3238_20240315.updater
Staging firmware update: /flash/ OS6900_XC48C4E_MAIN_CPU_FAN_CPLD_2f3238_20240315.updater
onie update successful
Successfully updated
Reload required to activate new firmware.
```

5. If multiple CPLDs have to be upgraded the command must be run several times.
6. Once the CPLDs have been upgraded a manual reload is required. This will boot each of the units to "ONIE: Update ONIE" mode. **Note**: Do not press any keys while in ONIE mode.
7. The switch will update the CPLD and then reboot to the *Certified* directory. **Note**: The switch will not boot back to the last running directory.
8. OS6860N models (except U28) will then automatically power cycle. For all other models manually power cycle the units to refresh the CPLD image. The switch will then again boot back to the *Certified* directory.
9. Reload to the running-directory.

## Appendix I: Fixed Problem Reports

The following problem reports were closed in this release.

| **CR/PR NUMBER** | **Description** |
|---|---|
| **Case:**<br>**00654252**<br>*CRAOS8X-36622* | **Summary:**<br>User authentication takes a long time to complete, requiring a reboot of the OS6560 switch.<br>**Explanation:**<br>The UnrepliedAuthrequest count maintained in Access Guardian was not properly updated when 802.1x EAP logoff packet is received from clients during Onex Authentication progress state. This resulted in reaching a maximum value of this count and further authentication -MAC or 802.1x supplicant authentication requests are not forwarded to RADIUS server.<br>Fix is given to update the Access Guardian properly when EAP Logoff packets are received to clear the counters.<br>🔒 Click for Additional Information |
| **Case:**<br>**00711332**<br>*CRAOS8X-41739* | **Summary:**<br>Applied QoS configuration is missing in the configuration snapshot command.<br>**Explanation:**<br>A policy service group name should be less than 32 characters in length. However, even with a policy service group name of 31 characters in length may trigger a restart of the qoscmmd process with a pmd file generation.<br>Fix is given to ensure the policy names are allowed to be configured up to 31 characters beyond this length an error will be thrown.<br>🔒 Click for Additional Information |
| **Case:**<br>**00727147**<br>CRAOS8X-43159 | **Summary:**<br>The updated cloudagent.cfg file is not synchronized from Master unit in VC to Slave units in the VC when "write memory flash-synchro" command is still issued. This caused the VC to be not up with OVC when Slave unit took over as new Master.<br>The cloudagent.cfg file is updated in Master unit in VC in situation when HTTP proxy configuration is used onsite.<br>**Explanation:**<br>Fix is given to synchronized cloudagent.cfg file from Master's running directory to certified directory and all units of Slave unit directories using "write memory flash-synchro" commands.<br>🔒 Click for Additional Information |
| **Case:**<br>**00712856**<br>*CRAOS8X-41956* | **Summary:**<br>The command ->show configuration snapshot takes approximately 10sec to display the output after executing the command in OS6900-C32E switch.<br>**Explanation:**<br>For OS6900-C32E, all the user ports are splitter capable ( QSFP28 ports (Ports 1-32 - 4X10G/40G/4X25G/100G) ) and API related to splitter capability detection are called multiple times causing a time delay.<br>Fix is done to optimize this API by retrieving the splitter capability status for all 32 ports in one shot and thus reducing the delay in snapshot call. |

| | |
|---|---|
| | 🔒 Click for Additional Information |
| **Case:**<br>**00706070**<br>*CRAOS8X-41033* | **Summary:**<br>The switch is not responding to the SNMP walk from the Solarwinds. In the “show snmp statistics” output it is noticed “snmpInGetRequests” counters are not getting incremented while performing the SNMP walk. SNMP requests received on the switch but no response sent back to the server.<br>**Explanation:**<br>The aluSubagent which handles SNMP request on the switch is queued heavily during SNMP walk and causes congestion to stop process the incoming requests resulting in SNMP timeout.<br>Fix is given to handle the queueing without getting congested.<br>🔒 Click for Additional Information |
| **Case:**<br>**00702219**<br>*CRAOS8X-40485* | **Summary:**<br>**CVE-2023-3446**<br>Vulnerability check for AOS 8X switches. CVE-2023-3446: OpenSSL vulnerabilities.<br>**Explanation:**<br>Fix is given to mitigate this vulnerability.<br>🔒 Click for Additional Information |
| **Case:**<br>**00714477**<br>*CRAOS8X-41835* | **Summary:**<br>**CVE-2023-3817**<br>Vulnerability check for AOS 8X switches. CVE-2023-3817: OpenSSL vulnerabilities.<br>**Explanation:**<br>Fix is given to mitigate this vulnerability.<br>🔒 Click for Additional Information |
| **Case:**<br>**00707340**<br>*CRAOS8X-41370* | **Summary:**<br>OS6560-48X4: CLI command throws an ERROR: specified application not loaded or “Please wait..”<br>**Explanation:**<br>According to the process, the ‘mip_gw’ socket should have sent an ACK packet to the ChassisSupervisor (‘new_cs’) side when show command is executed. However, in this scenario, ‘mip_gw’ did not respond with an ACK packet to ‘new_cs’, and as a result, the connection was terminated.<br>Fix is given to implement a reconnection procedure on the ChassisSupervisor (new_cs) and get the command issued successfully.<br>🔒 Click for Additional Information |

| | |
|---|---|
| **Case:**<br>**00723653**<br>*CRAOS8X-42519* | **Summary:**<br>While uploading a custom certificate via SFTP to the directory "/flash/switch/cert.d", it fails and displays "permission denied" error.<br>**Explanation:**<br>According to CLI guide, it is mentioned that the CRL file should be copied in PEM format to the /flash/switch/cert.d directory via SFTP. This is the document issue.<br>The CLI document will be corrected with the below information in 8.9R04:<br>"The custom CA server certificate should be copied in PEM format to /flash/ via SFTP and then the copied CA certificate file from /flash/ to /flash/switch/cert.d in the SU (root) shell".<br>🔒 Click for Additional Information |
| **Case:**<br>**00724314**<br>*CRAOS8X-42653* | **Summary:**<br>New command is required to add Untagged VLAN to CVLAN-Tag.<br>**Explanation:**<br>The following commands are introduced:<br>Example:<br>ethernet-service untagged-cvlan-insert enable<br>ethernet-service sap 100 uni port 1/1/3 untagged-cvlan 30<br>This helps to insert untagged traffic into the CVLAN, ensuring that dual-tagging traffic is transmitted on the NNI port, carrying both CVLAN (Untagged) and SVLAN tags.<br>🔒 Click for Additional Information |
| **Case:**<br>**00724314**<br>*CRAOS8X-42653* | **Summary:**<br>Issue of multiple alarm messages being generated for a single event in OS6465-P12 with AOS version 8.9.221.R03.<br>**Explanation:**<br>Fix is given such there will be a difference in the switch log information for Data(1) log indicates Alarm ON and Data(0) log indicates Alarm OFF.<br>Also, the trap message could be seen for Alarm ON ("ALARM IN TRAP is ON") and Alarm OFF ("ALARM IN TRAP is OFF").<br>🔒 Click for Additional Information |
| **Case:**<br>**00729858,**<br>**00730855**<br>*CRAOS8X-43250* | **Summary:**<br>The command “user <username> expiration <day> / <date>" does not work in AOS version 8.9.221.R03.<br>**Explanation:**<br>Fix is given to take effect of this expiration date and day as per the configuration.<br>🔒 Click for Additional Information |

| | |
|---|---|
| **Case:**<br>**00660912**<br>CRAOS8X-38329 | **Summary:**<br>Traffic passing through internal loopback port is capped at around 3Gbps or lower throughput.<br><br>**Explanation:**<br>An internal loopback is configured using a 10G interface for inline routing. When traffic traverses the loopback port 'without a physical cable connection', the throughput is limited to around 3Gbps or less.<br><br>🔒 Click for Additional Information |
| **Case:**<br>**00705779**<br>CRAOS8X-42082 | **Summary:**<br>BGP adjacency is reset upon reception of a BGP update message which contains path attribute 35.<br><br>**Explanation:**<br>The Omniswitch models OS6900-V72, OS6900-X48, and OS6900-C32 lack support for BGP Path Attribute 35. Upon receipt of a BGP update message containing this attribute, the BGP adjacency toggles, accompanied by the error message "Duplicate Attribute code [35]."<br><br>🔒 Click for Additional Information |
| **Case:**<br>**00716316**<br>CRAOS8X-42209 | **Summary:**<br>OS6860N-P24M: OS68-CNI-U1: Jumbo frames are dropped on 100G ports while macsec is enabled.<br><br>**Explanation:**<br>Packets of size 1500 and more are are dropped on 100G ports when macsec is enabled. The problem is confined to the 100G daughter module OS68-CNI-U1.<br><br>🔒 Click for Additional Information |
| **Case:**<br>**00712357**<br>CRAOS8X-41740 | **Summary:**<br>OS6860N: After successful authentication, all traffic received on UNP port is dropped.<br><br>**Explanation:**<br>When a device is connected to a dynamic UNP port, it passes the authentication and expected UNP profile is assigned. After that all packets received on the port are not forwarded.<br><br>🔒 Click for Additional Information |
| **Case:**<br>**00697131**<br>CRAOS8X-40656 | **Summary:**<br>ARP request was not getting forward to uplink.<br><br>**Explanation:**<br>OS6860E should be performing routing in the network and during this process the ARP request to specific destination ip-address is not getting to forward out from this switch. The observed issue has been identified as a bug and fixed the same.<br><br>🔒 Click for Additional Information |

| | |
|---|---|
| **Case:**<br>**00719711**<br>CRAOS8X-42712 | **Summary:**<br>SNMPv3 issue with BGP.<br>**Explanation:**<br>There is an issue when probing AOS switch through SNMPv3.<br>While performing MIBWalk, below error is thrown half way:<br>**Error: OID not increasing:**<br>iso.3.6.1.2.1.6.19.1.7.1.4.10.255.218.1.179.1.4.10.255.218.2.10791<br>🔒 Click for Additional Information |
| **Case:**<br>**00720786**<br>CRAOS8X-42542 | **Summary:**<br>ICMP issue between BEB nodes.<br>**Explanation:**<br>The ICMP request from one BEB was not reaching its adjacent BEB node. The issue was due to static ARP entry missing as this communication should happen via mgmt ip created on bvlan.<br>🔒 Click for Additional Information |
| **Case:**<br>**00720793**<br>CRAOS8X-42528 | **Summary:**<br>SPB ipvpn tags are not visible on remote node.<br>**Explanation:**<br>Route-tag info is not seen in corresponding BEB node and was with only for default route info.<br>🔒 Click for Additional Information |
| **Case:**<br>**00717519**<br>*CRAOS8X-42055* | **Summary:**<br>When BGP is configured in a different VRF than the default one and in case a BGP state transition happens (eg: from idle to established).<br>**Explanation:**<br>The two concerned log are misleading as, for the same state transition, in the first log, there's no mention of VRF, indicating that the routing is done within the default VRF. In the second log, a VRF ID is provided instead of the VRF name. This suggests that the routing is occurring within a specific VRF instance, but the name of the VRF is not explicitly mentioned. The VRF ID serves as a reference to the specific VRF instance being used for the routing. Typically, the VRF ID correlates to a configured VRF name in the router's configuration.<br>🔒 Click for Additional Information |
| **Case:**<br>**000074418**<br>*CRAOS8X-41925* | **Summary:**<br>The QSFP-4X10G-SR transceiver in the OS6900-V48 switch failed to establish a connection when set to operate in 40G mode with a single MPO fiber cable. Improvement done in 8.9R04GA to allows the QSFP-4X10G-SR transceiver to function properly in 40G mode with a single MPO fiber cable.<br>**Explanation:**<br>Unlike for 6900X72, the QSFP-4X10G-SR transceiver in the OS6900-V48 switch failed to establish a connection when set to operate in 40G mode with a single MPO fiber cable. It only functioned properly when set to 4x 10G mode with a splitter fiber cable.<br>🔒 Click for Additional Information |

| | |
|---|---|
| **Case:**<br>**00732242**<br>*CRAOS8X-43566* | **Summary:**<br>Static and dynamic dhcp-snooping binding lost after power cycle the switch.<br>**Explanation:**<br>Static or dynamic dhcp-snooping binding configuration is lost after power cycle of the switch due to racing condition and dhcpBind.db file corruption.<br>🔒 Click for Additional Information |
| **Case:**<br>**00703166**<br>*CRAOS8X-40623* | **Summary:**<br>OS6900-C32E - Issuing “show configuration snapshot” on core switch , takes about 12 seconds to output the config.<br>**Explanation:**<br>In 6900C32E, all ports are splitter capable. Hence the AOS calls certain splitter support related APIs(whose time complexity is high) for all the 32 ports during the snapshot execution.<br>Multiple calls to these APIs is causing a delay in snapshot display.<br>🔒 Click for Additional Information |
| **Case:**<br>**00699477**<br>*CRAOS8X-40251* | **Summary:**<br>OS6860N - One or more of the VC units did not join after power-cycle/reload.<br>**Explanation:**<br>The issue was seen after migrating layer 2 network from AOS6x to AOS8x. Customer leveraged auto-VC to deploy hundreds of Virtual-chassis consisting of 2 or more units.<br>Migration was successful and was working fine for some time, until customer did a planned power outage. After the power was back, some of the VCs observed one or more of their VC units not joining the VC. This was noticed only when the clients connected to the not-joined unit were trying to connect to the network.<br>Once the VC was reloaded again either hard reboot or soft reboot using "reload from working ...", everything started working again.<br>🔒 Click for Additional Information |
| Case:<br>**00711438**<br>*CRAOS8X-41937* | **Summary:**<br>Newly configured "ip service source-ip interface" is not used for syslog tls.<br>**Explanation:**<br>• When setting the tls method in syslog, it does not take correct outgoing interface as per the command "ip service source-ip "interface-2" all" if it is changed from interface-1 and interface-2.<br>• When setting the UDP method in syslog, it does take the correct outgoing interface as per the source-ip command.<br>The reason is "The code for supporting source-ip is not set in the syslog tls".<br>🔒 Click for Additional Information |

| | |
|---|---|
| Case:<br>**00718517**<br>*CRAOS8X-42137* | **Summary:**<br>In a VC of 6XOS6860N-P48Z, Chassis-3 nd 5 went into hung state.<br>**Explanation:**<br>The issue started with continuous VFL flaps[Down and up events in 1 to 2 sec] on chassis 1 and chassis 2. There is no manual trigger for the flaps.<br>debug cli command to increase the Wait-to-Shutdown timer for vfl ports in 8.9.R04 has been implemented. Please contact TAC before increasing the WTS for VFL ports.<br>The command: debug interfaces vfl-wts enable count 2 wts 600<br>• Count 2 refers the number of chassis.<br>• Wts in Milli Seconds.<br>🔒 Click for Additional Information |
| Case:<br>**00719120**<br>*CRAOS8X-42163* | **Summary:**<br>Interface of chassis-4 is invisible and the chassis-4 specific commands throws an error message as "ERROR: NI 1 is not ready yet. Try it later!"<br>**Description:**<br>This issue is started with VFL flaps without any manual trigger in 4XOS6860N-P48Z VC. Chassis-4 interfaces were shutdown due to duplicate master and vc takeover.<br>debug cli command to increase the Wait-to-Shutdown timer for vfl ports in 8.9.R04 has been implemented. Please contact Technical Support Team before implementing the command.<br>Command: debug interfaces vfl-wts enable count 2 wts 600<br>• Count refers the number of chassis.<br>• wts is in Milli Seconds<br>🔒 Click for Additional Information |
| Case:<br>**00719908**<br>*CRAOS8X-42270* | **Summary:**<br>Wireless connection shows no internet connect on mobile devices and ARP not learnt in Distributing switches [2XOS6900-V48C8 VC].<br>**Explanation:**<br>During the issue time, ARP entry for the end device is not learned on the gateway switch. Switch was sending the ARP replies for the ARP requests received from the end devices; However, the ARP entry is not saved in the arp table of the switch.<br>After 248 days of switch uptime, the expiry value for incomplete arp entries is calculated higher[Larger Expiry value]. So, it cannot expire, which will make the ARP entries to be accumulated and reach the threshold.<br>This issue applies to all AOS 8X switches and has been present since the 8.8.R01 code.<br>🔒 Click for Additional Information |
| Case:<br>**00724780**<br>*CRAOS8X-42270* | **Summary:**<br>6900: Inter-vlan routing doesn't happen as the gateway isn't reachable.<br>**Explanation:**<br>Inter-vlan routing doesn't happen between wired vlans if the ping is initiated from one vlan to another vlan, no issue with Intra-vlan[Same vlans]. |

| | |
|---|---|
| | ARP was not learnt in Gateway switch OS6900 which is the reason for inter-vlan routing failure.<br>After 248 days of switch uptime, the expiry value for incomplete arp entries is calculated higher[Larger Expiry value]. So, it cannot expire, which will make the ARP entries to be accumulated and reach the threshold.<br>**This is fixed in 8.9.R04 release.**<br>🔒 Click for Additional Information |
| Case:<br>**00726330**<br>*CRAOS8X-36622* | **Summary:**<br>MAC does not learn in some of the ports which cause UNP auth failure.<br>**Explanation:**<br>UNP users were stuck in “In Progress” state.<br>It is identified that the Unreplied AuthReqCount is maximum and hence the 802.1x auth and mac auth for the particular users gets congested, and the authentication request was not forwarded to server.<br>The workaround to reset the unreplied count to 0 can applied to resolve the issue. Please contact TAC to apply the workaround.<br>The rootcause is “not decrementing the unreplied count” though Context of AAA and AG is cleared. Fix is in 8.9.R04.<br>🔒 Click for Additional Information |
| Case:<br>**00722585**<br>*CRAOS8X-42411* | **Summary:**<br>In a VC of OS6900-C32E, chassis-2 rebooted<br>**Explanation:**<br>It is due to VFL flaps happened in micro seconds. When both VFLs went down, duplicate master detected. And the chassis-2 rebooted to join the master when both the VFL came up.<br>debug cli command to increase the Wait-to-Shutdown timer for vfl ports in 8.9.R04 has been implemented, Hence, VFL flaps are not considered till the secs mentioned in WTS command. Please contact TAC before increasing the WTS for VFL ports.<br>The command: debug interfaces vfl-wts enable count 2 wts 600<br>• Count 2 refers the number of chassis.<br>• wts is in Milli Seconds<br>🔒 Click for Additional Information |
| Case:<br>**00728333**<br>*CRAOS8X-43062* | **Summary:**<br>High CPU noticed in some of OS6860N VCs- Top task-appMonCmm2.<br>**Explanation:**<br>During reboot, CMM sends appmonvcboot.cfg and it is not received to all NIs. It keeps requesting for those config after 5 sec of timeout. CMM is busy in writing it in socket and processing the packets.This is the reason for CPU spike in Master.<br>Interim fix through software will be provided in 8.9.R04. Complete enhancement regards to packet processing will be implemented in 8.10 software.<br>🔒 Click for Additional Information |

| | |
|---|---|
| Case Number:<br>**00729482**<br>*CRAOS8X-43268* | **Summary:**<br>802.1x and MAC authentication failure after the switch upgrade from 8.8.56.R02 to 8.9.221.R03.<br>**Explanation:**<br>Post rebooting the VC, the key got changed, hence 802.1x and mac, ssh authentication is failed. Found the value 75 appended to the key which caused the authentication to fail. Encrypted salt in the customer config is corrupted even before the upgrade itself.<br>During decryption due to the incorrect salt[Junk characters], last two characters "75" got prepended to the original key. Defensive mechanism to avoid adding the extra characters to the key will be provided in 8.9.R04.<br>🔒 Click for Additional Information |
| **Case:**<br>**00732975**<br>*CRAOS8X-43603* | **Summary:**<br>Power supply flaps with wrong chassis information displayed in swlog.<br>**Explanation:**<br>If a flapping PS is in chassis 2+, log messages show PS 1/1 flapping. Now, chassis # is detected and included in the log message.<br>🔒 Click for Additional Information |
| **Case:**<br>**00725567**<br>*CRAOS8X-42688* | **Summary:**<br>New feature: FPGA Update cleans up .bin files when finished.<br>**Explanation:**<br>On earlier AOS, the FPGA upgrade process adds several files to the switch. The process did not clean up after itself for the OS6360 and OS6860E models. In 8.9R04, the FGPA upgrade process will clean up when finished.<br>🔒 Click for Additional Information |
| **Case:**<br>**00706202**<br>*CRAOS8X-41065* | **Summary:**<br>After upgrade/reload/link-flap the OS6860E switch stopped updating Route in hardware.<br>**Explanation:**<br>When adjacency between multiple routers are established simultaneously during reload, the host route of one of the routers is distributed and installed in router database through the other router. To correct this issue, the same logic of removing the host route to the adjacent route is extended in few more places during the adjacency formation and route database exchange.<br>🔒 Click for Additional Information |
| **Case:**<br>**00732338**<br>*CRAOS8X-43647* | **Summary:**<br>OS6560 - unp-template is not applied on the range of ports.<br>**Explanation:**<br>UNP port configured with "dynamic-service none" does not accept port-template configuration, if the port range has few of ports already configured with port-template.<br>🔒 Click for Additional Information |

| | |
|---|---|
| **Case:**<br>**00724364**<br>*CRAOS8X-42550* | **Summary:**<br>OS6560 switch does not establish SSH to Master switch in the VC via Management/Internal IP.<br>**Explanation:**<br>Console access to the Master switch is also not possible with the local 'admin' credentials. From chassis-6 (Slave) of the VC via console, SSH to the internal IP (127.10.1.65) is tried to the master switch; however, the SSH connection never established. A reload is required in the complete VC to stabilize the issue.<br>🔒 Click for Additional Information |
| **Case:**<br>**00726493**<br>*CRAOS8X-42844* | **Summary:**<br>Swlogs to understand if the reboot in the switch was due to watchdog reset.<br>**Explanation:**<br>Log improvement is done to record the last watchdog reset time which will help to understand if the reboot was due to watchdog reset. Also, last reset type is logged at info level to understand if reboot is due to any flash failure cases. Last watchdog kicktime and last reset type will be fetched from nvram and will be displayed in the boot up swlogs.<br>🔒 Click for Additional Information |
| **Case:**<br>**00718174**<br>*CRAOS8X-42106* | **Summary:**<br>Traffic mirrored by RP-MIR placed in the same QoS egress queue as the user traffic.<br>**Explanation:**<br>If the traffic mirrored by RP-MIR uses the same queue as user traffic, then during congestion scenario in AOS 8.x both the user and RPMIR traffic would be dropped. In AOS 6.x, the RPMIR traffic uses Queue-0 and not the same queue as user traffic.<br>🔒 Click for Additional Information |
| **Case:**<br>**00701620**<br>*CRAOS8X-40583* | **Summary:**<br>The DDM values are not updated on OS6465.<br>**Explanation**:<br>The DDM values are not updated, and stale values are shown even after the SFP is removed. The issue is seen due i2c read failure. This issue is seen in AOS 8.9.R02 / AOS 8.9 R03 and is fixed in AOS 8.9 R04.<br>🔒 Click for Additional Information |
| **Case:**<br>**00723870**<br>*CRAOS8X-42636* | **Summary:**<br>The switches are unable to install the NaaS license and an error “There is not enough room in the EERPOM to save data” is seen.”<br>**Explanation:**<br>The cause of this problem is that the switch's current EEPROM does not have enough space to install the NAAS license. A fix to free the EEPROM is provided in AOS 8.9 R04.<br>🔒 Click for Additional Information |
| **Case:**<br>**00722569**<br>*CRAOS8X-42723* | **Summary:**<br>The switches are going in the NaaS license Degraded mode.<br>**Explanation:**<br>Due to the power outage the switches reboot multiple times (in grace period) due |

| | |
|---|---|
| | to which the NaaS database is corrupted, and the switches go in degraded mode. Multiple enhancements are made to avoid the switch going into degraded mode and avoid NaaS database corruption.<br>🔒 Click for Additional Information |
| **Case:**<br>**00736614**<br>CRAOS8X-44187 | **Summary:**<br>OS6900-C32: 25gig links connected to edge OS6860N failed to come up.<br>**Explanation:**<br>Upon the reload of VC OS6900-C32, the "->interfaces port 2/1/1A & 1B fec fc" commands would be lost and incase if the VC consists more than 2 units, rest of the slave units too would lose the above configuration which would not make the ports to come up until reconfigured.<br>Only Master unit retains the commands and ports part of Master would be UP upon a VC reboot. This issue has been fixed under AOS 8.9R04 GA.<br>🔒 https://myportal.al-enterprise.com/alebp/s/tkc-redirect?000074539 |
| **Case:**<br>**00734217**<br>CRAOS8X-43746 | **Summary:**<br>The Service type field missing in during aaa authentication for SSH /Telnet access<br>**Explanation:**<br>From OV 2500 4.8 R01 UPAM is expecting the service type Atrribute in the Access request packet from the NAS device. This attribute is sent 802.1x/mac authentication, however in case of AAA SSH/Telnet authentication it is missing.<br>This is fixed in AOS 8.9R04<br>🔒 https://myportal.al-enterprise.com/alebp/s/tkc-redirect?000074660 |
| **Case:**<br>**00710070**<br>CRAOS8X-41594 | **Summary:**<br>GTTS works for only 1 Tunnel at a time.<br>**Explanation:**<br>On Yukon - Yos image based switches, if L2GRE is used as GTTS, only one service is working at a time with auto-discovery enabled. The reason for the same is due to HW limitation.<br>🔒 https://myportal.al-enterprise.com/alebp/s/tkc-redirect?000074483 |
| **Case:**<br>**CRAOS8X-42185**<br>**CRAOS8X-41999** | **Summary:**<br>When logged in under user 'su', CLI commands were only being audited in Common Criteria Mode.<br>**Explanation:**<br>Beginning in 8.9R4, when logged in under user 'su' all CLI commands will be audited regardless of mode. |
| **Case:**<br>**CRAOS8X-41815** | **Summary:**<br>Web audit logs did not contain the IP address or username when separate sessions were active and could not determine who initiated a change.<br>**Explanation:**<br>Beginning in 8.9R4 web audit logs include both IP address and username. |
| **Case:**<br>**CRAOS8X-41814** | **Summary:**<br>The switch only utilized lower case and numerical characters for Session ID generation and did not include upper case characters. |

| | |
|---|---|
| | **Explanation:**<br>Beginning in 8.9R4 the switch uses A-Z, a-z, and 0-9 for session ID generation. |
| **CRAOS8X-43968** | **Summary:**<br>On an OS6900-X48C4E (Hardware revision: 6), with a single power supply in PS1, a temperature error message may sometimes be displayed on the console.<br>**Explanation:**<br>An updated CPLD version 2.15 is available to address this issue. |
| **CRAOS8X-44637** | **Summary:**<br>Users are not able to perform SSH connections to the switch using some of the latest versions of SSH clients such as Putty, MobaXterm, and Tera Term.<br>**Explanation:**<br>Issue was due to a MAC (Message Authentication Code) exchange between the latest version of SSH clients and the OmniSwitch. It has been fixed in the 8.9.94.R04 GA build. |

## Appendix J: Installing/Removing Packages

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

| Package | Package Description |
|---|---|
| MRP (mrp-v#.deb) | MRP Application |
| ams / ams-apps (ams-v#.deb/ams-apps-v#.deb) | AOS Micro Services Application |
| OVSDB (aos-ovsdb-v#.deb) | OVSDB Application |
| uosn-mpls-v1.deb<br>uosn-sitemgr-v1.deb<br>uosn-siteend-v1.deb | MPLS Application and Licensing |
| nutanix-v1.deb | Nutanix Prism Plug-in Package |
| ovng-agent-v.1.10.deb | OmniVista Cirrus 10 |
| - If a package is not committed it can result in image validation errors when trying to reload the switch.<br>- Some packages are included as part of the AOS release and do not have to be installed separately.<br>- Applications should be stopped prior to upgrading a package. | |

### Installing Packages

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

```
-> pkgmgr verify nos-mrp-v1.deb
  Verifying MD5 checksum.. OK
-> pkgmgr install nos-mrp-v1.deb
-> write memory
-> show pkgmgr
Legend: (+) indicates package is not saved across reboot
        (*) indicates packages will be installed or removed after reload
Name                Version           Status            Install Script
---------------+--------------------+------------------+--------------------------------
  ams           default               installed          default
  ams-apps      default               installed          default
  mrp         8.7.R03-xxx         installed        /flash/working/pkg/mrp/install.sh
```

### Removing Packages

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

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

### Package(s) Committed

```
-> show pkgmgr
Legend: (+) indicates package is not saved across reboot
        (*) indicates packages will be installed or removed after reload
Name                Version           Status            Install Script
---------------+--------------------+------------------+--------------------------------
  ams           default               installed          default
  ams-apps      default               installed          default
  mrp         8.7.R03-xxx          removed          /flash/working/pkg/mrp/install.sh
```

```
Remove the Debian package installation file. For example:
 -> rm /flash/working/pkg/nos-mrp-v#.deb
```

## AOS Upgrade with Encrypted Passwords

### AMS

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

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

### IoT-Profiler

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

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

## Appendix K: Fixed CVEs

The following CVE CRs were fixed in this release.

| CVE CRs | Module | CVE | NVD CVSS |
|---|---|---|---|
| CRAOS8X-28184 | PHP | CVE-2021-21704 | 5.9 |
| | | CVE-2021-21705 | 5.3 |
| | | CVE-2021-21706 | 6.5 |
| | | CVE-2021-21707 | 5.3 |
| | | CVE-2021-21708 | 9.8 |
| | | CVE-2022-31625 | 8.1 |
| | | CVE-2022-31626 | 8.8 |
| | | CVE-2022-31627 | 9.8 |
| | | CVE-2022-31628 | 5.5 |
| | | CVE-2022-31629 | 6.5 |
| | | CVE-2021-32610 | 7.1 |
| | | CVE-2019-11041 | 7.1 |
| | | CVE-2019-11042 | 7.1 |
| | | CVE-2019-11048 | 5.3 |
| | | CVE-2020-7059 | 9.1 |
| | | CVE-2020-7060 | 9.1 |
| | | CVE-2022-31631 | NA |
| CRAOS8X-36565 | PHP | CVE-2022-31630 | NA |
| | | CVE-2022-37454 | 9.8 |
| CRAOS8X-35847 | OpenSSH | CVE-2023-25136 | 6.5 |
| CRAOS8X-36871 | OpenSSH | CVE-2021-41617 | 7.0 |
| | | CVE-2021-36368 | 3.7 |
| CRAOS8X-39416 | OpenSSL | CVE-2023-2650 | 6.5 |
| CRAOS8X-36768 | Linux | CVE-2022-2308 | 6.5 |
| | | CVE-2022-3564 | 7.1 |
| | | CVE-2022-3543 | 5.5 |
| | | CVE-2022-4095 | 6.3 |
| | | CVE-2022-41850 | 4.7 |
| | | CVE-2022-42895 | 5.5 |

| | | | |
|---|---|---|---|
| | | CVE-2022-42896 | 8.8 |
| | | CVE-2022-43945 | 7.5 |
| CRAOS8X-36797 | Busybox | CVE-2022-30065 | 7.8 |
| CRAOS8X-39579 | cURL | CVE-2023-28319 | 7.5 |
| | | CVE-2023-28320 | 5.9 |
| | | CVE-2023-28321 | 5.9 |
| | | CVE-2023-28322 | 3.7 |
| CRAOS8X-36564 | cURL | CVE-2022-32221 | 9.8 |
| | | CVE-2022-35260 | 6.5 |
| | | CVE-2022-42915 | 8.1 |
| | | CVE-2022-42916 | 7.5 |
| CRAOS8X-37057 | cURL | CVE-2022-43551 | 7.5 |
| | | CVE-2022-43552 | 5.9 |
| CRAOS8X-37803 | cURL | CVE-2023-23914 | 9.1 |
| | | CVE-2023-23915 | 6.5 |
| | | CVE-2023-23916 | 6.5 |
| CRAOS8X-38112 | cURL | CVE-2023-27533 | 8.8 |
| | | CVE-2023-27534 | 8.8 |
| | | CVE-2023-27535 | 5.9 |
| | | CVE-2023-27536 | 5.9 |
| | | CVE-2023-27537 | 5.9 |
| | | CVE-2023-27538 | 5.5 |
| CRAOS8X-38938 | ncurses | CVE-2023-29491 | 7.8 |
| CRAOS8X-40926 | Linux | CVE-2022-48425 | 7.8 |
| | | CVE-2023-34256 | 5.5 |
| CRAOS8X-41378 | Python | CVE-2023-24329 | 7.5 |
| CRAOS8X-35841 | Lighttpd | CVE-2022-37797 | 7.5 |
| | | CVE-2022-41556 | 7.5 |
| CRAOS8X-40798 | OpenSSH | CVE-2023-38408 | 9.8 |
| CRAOS8X-38040 | OpenSSH | No CVE | 7.5 |
| CRAOS8X-40485 | OpenSSL | CVE-2023-2975 | 5.3 |
| | | CVE-2023-3446 | 5.3 |

| | | | |
|---|---|---|---|
| CRAOS8X-40929 | OpenSSL | CVE-2023-2975 | 5.3 |
| CRAOS8X-40930 | OpenSSL | CVE-2023-3446 | 5.3 |
| CRAOS8X-40931 | OpenSSL | CVE-2023-3817 | 5.3 |
| CRAOS8X-41957 | cURL | CVE-2023-38545 | 9.8 |
| | | CVE-2023-38546 | 3.7 |
| CRAOS8X-42079 | cURL | CVE-2023-38039 | 7.5 |
| CRAOS8X-42075 | Busybox | CVE-2022-48174 | 9.8 |
| CRAOS8X-43037 | OpenSSH | CVE-2023-48795 | 5.9 |
| | | CVE-2023-51384 | 5.5 |
| | | CVE-2023-51385 | 6.5 |