

# Release Notes - Rev. A

OmniSwitch 6360, 6465, 6560(E), 6570M, 6860(E),  
6860N, 6865, 6870, 6900, 9900

## Release 8.10R3

These release notes accompany release 8.10R3. 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.

Released in: June 2025

**Contents**

<b>Contents .....</b>	<b>2</b>
<b>Related Documentation.....</b>	<b>3</b>
<b>System Specifications .....</b>	<b>4</b>
<b>[IMPORTANT] *MUST READ*: AOS Release 8.10R3 Prerequisites and Deployment Information .....</b>	<b>14</b>
<b>Licensed Features.....</b>	<b>18</b>
<b>ALE Secure Diversified Code.....</b>	<b>20</b>
<b>New / Updated Hardware Support and Guidelines .....</b>	<b>21</b>
<b>8.10R3 New Feature and Enhancements.....</b>	<b>21</b>
<b>Open Problem Reports and Feature Exceptions .....</b>	<b>36</b>
<b>Hot-Swap/Redundancy Feature Guidelines .....</b>	<b>41</b>
<b>Technical Support .....</b>	<b>44</b>
<b>Appendix A: Feature Matrix.....</b>	<b>46</b>
<b>Appendix B: MACsec Platform Support .....</b>	<b>56</b>
<b>Appendix C: SPB L3 VPN-Lite Service-based (Inline Routing) / External Loopback Support / BVLAN Guidelines .....</b>	<b>58</b>
<b>Appendix D: General Upgrade Requirements and Best Practices .....</b>	<b>61</b>
<b>Appendix E: Standard Upgrade - OmniSwitch Standalone or Virtual Chassis .....</b>	<b>66</b>
<b>Appendix F: ISSU - OmniSwitch Chassis or Virtual Chassis.....</b>	<b>68</b>
<b>Appendix G: FPGA / U-boot Upgrade Procedure .....</b>	<b>72</b>
<b>Appendix H: CPLD Upgrade Procedure for ONIE-Based Devices.....</b>	<b>76</b>
<b>Appendix I: Fixed Problem Reports .....</b>	<b>78</b>
<b>Appendix J: Installing/Removing Packages .....</b>	<b>78</b>
<b>Appendix K: Fixed CVEs .....</b>	<b>102</b>

## **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 6870 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 Specifications Guide
- OmniSwitch AOS Release 8 Transceivers Guide

## System Specifications

### Memory Specifications

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(E)	2GB	2GB
OS6560-24X4/P24X4	1GB	1GB
OS6570M	2GB	8GB
OS6860(E)	2GB	2GB
OS6860N	4GB	16GB
OS6865	2GB	2GB
OS6870	8GB	32GB
OS6900-V72/C32	16GB	16GB
OS6900-X48C6/T48C6/X48C4E/T24C2/X24C2	8GB	32GB <sup>1</sup>
OS6900-V48C8/C32E	16GB <sup>2</sup>	64GB <sup>1</sup>
OS9900	16GB	2GB
1. Size of physical memory. Partitioned to 16GB flash memory. 2. Previous release notes incorrectly listed 8GB.		

### Bootloader and FPGA Specifications

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 8.10.93.R03 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6360-10	8.7.149.R02	8.7.30.R03 <sup>2</sup> 8.9.85.R02 <sup>4</sup> 8.10.115.R01 <sup>6</sup> 8.10.42.R02 <sup>6</sup> 8.10.114.R02 <sup>7</sup>	0.11	0.11 0.12 <sup>5</sup>

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6360-P10	8.7.149.R02	8.7.30.R03 <sup>2</sup> 8.9.85.R02 <sup>4</sup> 8.10.115.R01 <sup>6</sup> 8.10.42.R02 <sup>6</sup> 8.10.114.R02 <sup>7</sup>	0.11	0.11 0.12 <sup>5</sup>
OS6360-P10A (904324-90)	8.8.2.R03	8.8.2.R03 8.9.85.R02 <sup>4</sup> 8.10.115.R01 <sup>6</sup> 8.10.42.R02 <sup>6</sup> 8.10.114.R02 <sup>7</sup>	0.1	0.1 0.2 <sup>5</sup>
OS6360-24	8.7.149.R02	8.7.30.R03 <sup>2</sup> 8.9.85.R02 <sup>4</sup> 8.10.115.R01 <sup>6</sup> 8.10.42.R02 <sup>6</sup> 8.10.114.R02 <sup>7</sup>	0.15	0.17 <sup>1</sup> 0.20 <sup>3</sup>
OS6360-P24	8.7.149.R02	8.7.30.R03 <sup>2</sup> 8.9.85.R02 <sup>4</sup> 8.10.115.R01 <sup>6</sup> 8.10.42.R02 <sup>6</sup> 8.10.114.R02 <sup>7</sup>	0.15	0.17 <sup>1</sup> 0.20 <sup>3</sup>
OS6360-P24X	8.7.149.R02	8.7.30.R03 <sup>2</sup> 8.9.85.R02 <sup>4</sup> 8.10.115.R01 <sup>6</sup> 8.10.42.R02 <sup>6</sup> 8.10.114.R02 <sup>7</sup>	0.12	0.12 0.13 <sup>5</sup>
OS6360-PH24	8.7.149.R02	8.7.30.R03 <sup>2</sup> 8.9.85.R02 <sup>4</sup> 8.10.115.R01 <sup>6</sup> 8.10.42.R02 <sup>6</sup> 8.10.114.R02 <sup>7</sup>	0.12	0.12 0.13 <sup>5</sup>
OS6360-48	8.7.149.R02	8.7.30.R03 <sup>2</sup> 8.9.85.R02 <sup>4</sup> 8.10.115.R01 <sup>6</sup> 8.10.42.R02 <sup>6</sup> 8.10.114.R02 <sup>7</sup>	0.15	0.17 <sup>1</sup> 0.20 <sup>3</sup>
OS6360-P48	8.7.149.R02	8.7.30.R03 <sup>2</sup> 8.9.85.R02 <sup>4</sup> 8.10.115.R01 <sup>6</sup> 8.10.42.R02 <sup>6</sup> 8.10.114.R02 <sup>7</sup>	0.15	0.17 <sup>1</sup> 0.20 <sup>3</sup>
OS6360-P48X	8.7.149.R02	8.7.30.R03 <sup>2</sup> 8.9.85.R02 <sup>4</sup> 8.10.115.R01 <sup>6</sup> 8.10.42.R02 <sup>6</sup> 8.10.114.R02 <sup>7</sup>	0.12	0.12 0.13 <sup>5</sup>
OS6360-PH48	8.8.114.R01	8.8.114.R01 8.9.85.R02 <sup>4</sup> 8.10.115.R01 <sup>6</sup>	0.12	0.12 0.13 <sup>5</sup>

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
		8.10.42.R02 <sup>6</sup> 8.10.114.R02 <sup>7</sup>		
1. FPGA version 0.17 is REQUIRED to address issues CRAOS8X-26370 and CRAOS8X-25033. 2. Optional U-boot update for CRAOS8X-24464, ability to disable/authenticate U-boot 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. 6. Addresses multiple power cycle issues. See <a href="#">FPGA / U-boot Upgrade Procedure</a> . 7. U-boot version 8.10.114.R02 is mandatory to address CRAOS8X-50729.				

### **OmniSwitch 6465 - AOS Release 8.10.93.R03 (GA)**

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6465-P6	8.5.83.R01	8.7.2.R02 <sup>2</sup> 8.7.30.R03 <sup>3</sup> 8.8.33.R01 <sup>4</sup> 8.9.85.R02 <sup>5</sup> 8.10.115.R01 <sup>6</sup> 8.10.42.R02 <sup>6</sup>	0.10	0.10
OS6465-P12	8.5.83.R01	8.7.2.R02 <sup>2</sup> 8.7.30.R03 <sup>3</sup> 8.8.33.R01 <sup>4</sup> 8.9.85.R02 <sup>5</sup> 8.10.115.R01 <sup>6</sup> 8.10.42.R02 <sup>6</sup>	0.10	0.10
OS6465-P28	8.5.89.R02	8.7.2.R02 <sup>2</sup> 8.7.30.R03 <sup>3</sup> 8.8.33.R01 <sup>4</sup> 8.9.85.R02 <sup>5</sup> 8.10.115.R01 <sup>6</sup> 8.10.42.R02 <sup>6</sup>	0.5	0.7 <sup>1</sup>
OS6465T-12	8.6.117.R01	8.7.2.R02 <sup>2</sup> 8.7.30.R03 <sup>3</sup> 8.8.33.R01 <sup>4</sup> 8.9.85.R02 <sup>5</sup> 8.10.115.R01 <sup>6</sup> 8.10.42.R02 <sup>6</sup>	0.4	0.4
OS6465T-P12	8.6.117.R01	8.7.2.R02 <sup>2</sup> 8.7.30.R03 <sup>3</sup> 8.8.33.R01 <sup>4</sup> 8.9.85.R02 <sup>5</sup> 8.10.115.R01 <sup>6</sup> 8.10.42.R02 <sup>6</sup>	0.4	0.4
OS6465-P12 (ENH-240)	8.8.33.R01	8.8.33.R01 8.9.85.R02 <sup>5</sup> 8.10.115.R01 <sup>6</sup> 8.10.42.R02 <sup>6</sup>	0.5	0.5

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
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 U-boot update for CRAOS8X-24464, ability to disable/authenticate U-boot access. 4. Optional U-boot update to support boot from USB feature. 5. Highly recommended to address the NAND flash corruption issue CRAOS8X-35470. 6. Addresses multiple power cycle issues. See <a href="#">FPGA / U-boot Upgrade Procedure</a> .				

### **OmniSwitch 6560 - AOS Release 8.10.93.R03 (GA)**

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6560-24Z24	8.5.22.R01	8.7.2.R02 <sup>3</sup> 8.7.30.R03 <sup>7</sup> 8.9.85.R02 <sup>9</sup> 8.10.115.R01 <sup>10</sup> 8.10.42.R02 <sup>10</sup>	0.7	0.8 <sup>5</sup> 0.9 <sup>9</sup>
OS6560-P24Z24	8.4.1.23.R02	8.7.2.R02 <sup>3</sup> 8.7.30.R03 <sup>7</sup> 8.9.85.R02 <sup>9</sup> 8.10.115.R01 <sup>10</sup> 8.10.42.R02 <sup>10</sup>	0.6	0.7 <sup>1</sup> 0.8 <sup>5</sup> 0.9 <sup>9</sup>
OS6560-24Z8	8.5.22.R01	8.7.2.R02 <sup>3</sup> 8.7.30.R03 <sup>7</sup> 8.9.85.R02 <sup>9</sup> 8.10.115.R01 <sup>10</sup> 8.10.42.R02 <sup>10</sup>	0.7	0.8 <sup>5</sup> 0.9 <sup>9</sup>
OS6560-P24Z8	8.4.1.23.R02	8.7.2.R02 <sup>3</sup> 8.7.30.R03 <sup>7</sup> 8.9.85.R02 <sup>9</sup> 8.10.115.R01 <sup>10</sup> 8.10.42.R02 <sup>10</sup>	0.6	0.7 <sup>1</sup> 0.8 <sup>5</sup> 0.9 <sup>9</sup>
OS6560-24X4	8.5.89.R02	8.7.2.R02 <sup>4</sup> 8.7.30.R03 <sup>7</sup> 8.9.85.R02 <sup>8</sup> 8.10.115.R01 <sup>10</sup> 8.10.42.R02 <sup>10</sup>	0.4	0.4
OS6560-P24X4	8.5.89.R02	8.7.2.R02 <sup>4</sup> 8.7.30.R03 <sup>7</sup> 8.9.85.R02 <sup>8</sup> 8.10.115.R01 <sup>10</sup> 8.10.42.R02 <sup>10</sup>	0.4	0.4
OS6560-P48Z16 (903954-90)	8.4.1.23.R02	8.7.2.R02 <sup>3</sup> 8.7.30.R03 <sup>7</sup> 8.9.85.R02 <sup>9</sup> 8.10.115.R01 <sup>10</sup> 8.10.42.R02 <sup>10</sup>	0.6	0.7 <sup>1</sup> 0.8 <sup>5</sup> 0.9 <sup>9</sup>
OS6560-P48Z16 (all other PNs)	8.5.97.R04	8.7.2.R02 <sup>3</sup> 8.7.30.R03 <sup>7</sup> 8.9.85.R02 <sup>9</sup>	0.3	0.6 <sup>2</sup> 0.7 <sup>6</sup>

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
		8.10.115.R01 <sup>10</sup> 8.10.42.R02 <sup>10</sup>		
OS6560-48X4	8.5.97.R04	8.7.2.R02 <sup>4</sup> 8.7.30.R03 <sup>7</sup> 8.9.85.R02 <sup>8</sup> 8.10.115.R01 <sup>10</sup> 8.10.42.R02 <sup>10</sup>	0.4	0.7 <sup>2</sup> 0.8 <sup>6</sup>
OS6560-P48X4	8.5.97.R04	8.7.2.R02 <sup>4</sup> 8.7.30.R03 <sup>7</sup> 8.9.85.R02 <sup>8</sup> 8.10.115.R01 <sup>10</sup> 8.10.42.R02 <sup>10</sup>	0.4	0.7 <sup>2</sup> 0.8 <sup>6</sup>
OS6560-X10	8.5.97.R04	8.7.2.R02 <sup>4</sup> 8.7.30.R03 <sup>7</sup> 8.9.85.R02 <sup>8</sup> 8.10.115.R01 <sup>10</sup> 8.10.42.R02 <sup>10</sup>	0.5	0.8 <sup>2</sup>
OS6560E-P24Z8	8.9.85.R02	8.9.85.R02 8.10.115.R01 <sup>10</sup> 8.10.42.R02 <sup>10</sup>	0.9	0.9
OS6560E-P48Z16	8.9.85.R02	8.9.85.R02 8.10.115.R01 <sup>10</sup> 8.10.42.R02 <sup>10</sup>	0.7	0.7
<p>1. FPGA version 0.7 is optional to address issue CRAOS8X-7207.</p> <p>2. FPGA versions are optional to address issue CRAOS8X-16452.</p> <p>3. U-boot 8.7.2.R02 is optional to address eUSB issue CRAOS8X-13819.</p> <p>4. U-boot 8.7.2.R02 is optional to address UBIFS error issues CRAOS8X-4813/13440.</p> <p>5. FPGA version 0.8 is optional to address issue CRAOS8X-22857.</p> <p>6. FPGA versions 0.7 and 0.8 are optional to support 1588v2.</p> <p>7. Optional U-boot update for CRAOS8X-24464, ability to disable/authenticate U-boot access.</p> <p>8. Highly recommended to address the NAND flash corruption issue CRAOS8X-35470.</p> <p>9. Ships from factory. No upgrade required, there are no functional changes in this U-boot version for these models.</p> <p>10. Addresses multiple power cycle issues. See <a href="#">FPGA / U-boot Upgrade Procedure</a>.</p>				

### OmniSwitch 6570M - AOS Release 8.10.93.R03 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6570M-12	8.9.25.R02	8.9.25.R02 8.9.92.R02 <sup>1</sup> 8.9.139.R03 <sup>3</sup> 8.9.70.R04 <sup>4</sup> 8.10.115.R01 <sup>5</sup> 8.10.42.R02 <sup>5</sup>	0.11	0.11
OS6570M-12D	8.9.25.R02	8.9.25.R02 8.9.92.R02 <sup>1</sup> 8.9.139.R03 <sup>3</sup> 8.9.70.R04 <sup>4</sup>	0.11	0.11



Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
		8.10.115.R01 <sup>5</sup> 8.10.42.R02 <sup>5</sup>		
OS6570M-U28	8.9.25.R02	8.9.25.R02 8.9.92.R02 <sup>1</sup> 8.9.139.R03 <sup>3</sup> 8.9.70.R04 <sup>4</sup> 8.10.115.R01 <sup>5</sup> 8.10.42.R02 <sup>5</sup>	0.11	0.11 0.12 <sup>2</sup>
<p>1. Adds support for Gowin CPLD.  2. Addresses power supply interrupt issue.  3. Addresses CRAOS8X-40924 for disabling U-boot access.  4. Adds support for signed AOS images.  5. Addresses multiple power cycle issues. See <a href="#">FPGA / U-boot Upgrade Procedure</a>.</p> <p><b>Note:</b> U-boot version 8.9.70.R04 and above supports AOS signed images only (8.9R4 and above). To use AOS releases prior to 8.9R4, before downgrading the AOS image the u-boot must be downgraded to a version earlier than 8.9.70.R04.</p>				

### **OmniSwitch 6860(E) - AOS Release 8.10.93.R03 (GA)**

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6860/OS6860E (except U28/P24Z8)	8.1.1.70.R01	8.7.30.R03 <sup>2</sup> 8.10.115.R01 <sup>3</sup> 8.10.42.R02 <sup>3</sup>	0.9	0.10 <sup>1</sup>
OS6860E-U28	8.1.1.70.R01	8.7.30.R03 <sup>2</sup> 8.10.115.R01 <sup>3</sup> 8.10.42.R02 <sup>3</sup>	0.20	0.20
OS6860E-P24Z8	8.4.1.17.R01	8.7.30.R03 <sup>2</sup> 8.10.115.R01 <sup>3</sup> 8.10.42.R02 <sup>3</sup>	0.5	0.7 <sup>1</sup>
<p>1. FPGA versions .7 and .10 are optional on the PoE models for the fast and perpetual PoE feature support.  2. Optional U-boot update for CRAOS8X-24464, ability to disable/authenticate U-boot access.  3. Addresses multiple power cycle issues. See <a href="#">FPGA / U-boot Upgrade Procedure</a>.</p>				

### **OmniSwitch 6860N - AOS Release 8.10.93.R03 (GA)**

Hardware	Minimum ONIE	Current ONIE	Minimum CPLD	Current CPLD
OS6860N-U28	2019.05.00.10	2019.05.00.11	12	12
OS6860N-P48Z	2019.05.00.10	2019.05.00.11	12	13 <sup>1</sup>
OS6860N-P48M	2019.05.00.10	2019.05.00.11	11	12 <sup>1</sup>
O6860N-P24M	2019.05.00.11	2019.05.00.11	2	3 <sup>1</sup>
OS6860N-P24Z	2019.05.00.11	2019.05.00.11	2	3 <sup>1</sup>
1. Addresses CRAOS8X-29731/30471 - OS6860N power supply issue.				

Hardware	Minimum ONIE	Current ONIE	Minimum CPLD	Current CPLD
<b>Note:</b> These models use the Uosn.img image file.				

### OmniSwitch 6865 - AOS Release 8.10.93.R03 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6865-P16X	8.3.1.125.R01	8.7.2.R02 <sup>2</sup> 8.7.30.R03 <sup>3</sup> 8.8.33.R01 <sup>4</sup> 8.10.115.R01 <sup>5</sup> 8.10.42.R02 <sup>5</sup>	0.20	0.25 <sup>1</sup>
OS6865-U12X	8.4.1.17.R01	8.7.2.R02 <sup>2</sup> 8.7.30.R03 <sup>3</sup> 8.8.33.R01 <sup>4</sup> 8.10.115.R01 <sup>5</sup> 8.10.42.R02 <sup>5</sup>	0.23	0.25 <sup>1</sup>
OS6865-U28X	8.4.1.17.R01	8.7.2.R02 <sup>2</sup> 8.7.30.R03 <sup>3</sup> 8.8.33.R01 <sup>4</sup> 8.10.115.R01 <sup>5</sup> 8.10.42.R02 <sup>5</sup>	0.11	0.14 <sup>1</sup>
<p>1. FPGA versions 0.25 and 0.14 are optional for the fast and perpetual PoE feature support.</p> <p>2. U-boot 8.7.2.R02 is optional to address eUSB issue CRAOS8X-13819.</p> <p>3. Optional U-boot update for CRAOS8X-24464, ability to disable/authenticate U-boot access.</p> <p>4. Optional U-boot update to support boot from USB feature.</p> <p>5. Addresses multiple power cycle issues. See <a href="#">FPGA / U-boot Upgrade Procedure</a>.</p> <p><b>Note:</b> CRAOS8X-4150 for the OS6865-U28X was fixed with FPGA version 0.12 and higher.</p>				

### OmniSwitch 6870 - AOS Release 8.10.93.R03 (GA)

Hardware	Minimum ONIE	Current ONIE	Minimum CPLD	Current CPLD
OS6870-24	2019.05.00.12	2019.05.00.12	CPLD - 0.09 CPLD (LED) - 0.08 CPLD (CPU) - 0.04	CPLD - 0.09 CPLD (LED) - 0.08 CPLD (CPU) - 0.04
OS6870-P24M	2019.05.00.12	2019.05.00.12	CPLD - 0.09 CPLD (LED) - 0.07 CPLD (CPU) - 0.04	CPLD - 0.09 CPLD (LED) - 0.07 CPLD (CPU) - 0.04
OS6870-P24Z	2019.05.00.12	2019.05.00.12	CPLD - 0.07 CPLD (LED) - 0.06 CPLD (CPU) - 0.04	CPLD - 0.07 CPLD (LED) - 0.06 CPLD (CPU) - 0.04
OS6870-48	2019.05.00.12	2019.05.00.12	CPLD - 0.09 CPLD (LED) - 0.08 CPLD (CPU) - 0.04	CPLD - 0.09 CPLD (LED) - 0.08 CPLD (CPU) - 0.04
OS6870-P48M	2019.05.00.12	2019.05.00.12	CPLD - 0.11 CPLD (LED) - 0.09 CPLD (CPU) - 0.04	CPLD - 0.011 CPLD (LED) - 0.09 CPLD (CPU) - 0.04
OS6870-P48Z	2019.05.00.12	2019.05.00.12	CPLD - 0.07 CPLD (LED) - 0.06 CPLD (CPU) - 0.04	CPLD - 0.07 CPLD (LED) - 0.06 CPLD (CPU) - 0.04

Hardware	Minimum ONIE	Current ONIE	Minimum CPLD	Current CPLD
OS6870-V12	2019.05.00.12	2019.05.00.12	CPLD - 0.10 CPLD (LED) - 0.07 CPLD (CPU) - 0.04	CPLD - 0.10 CPLD (LED) - 0.07 CPLD (CPU) - 0.04

### OmniSwitch 6900 - AOS Release 8.10.93.R03 (GA)

Hardware	Minimum ONIE	Current ONIE	Minimum CPLD	Current CPLD
OS6900-V72	2017.08.00.01	2017.08.00.01	CPLD 1 - 5 CPLD 2 - 6 CPLD 3 - 8	CPLD 1 - 5 CPLD 2 - 6 CPLD 3 - 8
OS6900-C32	2016.08.00.03	2018.11.00.02	CPLD 1 - 10 CPLD 2 - 11 CPLD 3 - 11	CPLD 1 - 10 CPLD 2 - 11 CPLD 3 - 11
OS6900-C32E	2020.02.00.01	2020.02.00.01	CPLD 1 - 13 CPLD 2 - 9 CPLD 3 - 9	CPLD 1 - 13 CPLD 2 - 9 CPLD 3 - 9
OS6900-X48C6	2019.08.00.01	2019.08.00.01	CPLD 1 - 2 CPLD 2 - 2 CPLD 3 - 2 CPU CPLD - N/A	CPLD 1 - 3 CPLD 2 - 2 CPLD 3 - 2 CPU CPLD - 2.14 <sup>1</sup>
OS6900-T48C6	2019.08.00.01	2019.08.00.01	CPLD 1 - 2 CPLD 2 - 2 CPLD 3 - 4 CPU CPLD - N/A	CPLD 1 - 3 CPLD 2 - 2 CPLD 3 - 4 CPU CPLD - 2.14 <sup>1</sup>
OS6900-X48C4E	2019.05.00.10	2019.05.00.10	CPLD 1 - 3 CPLD 2 - 2 CPLD 3 - 3 CPU CPLD - N/A	CPLD 1 - 3 CPLD 2 - 2 CPLD 3 - 3 CPU CPLD - 2.14 <sup>1</sup> CPU CPLD - 2.15 <sup>2</sup>
OS6900-V48C8	2020.02.00.01	2020.02.00.01	CPLD 1 - 2 CPLD 2 - 3 CPLD 3 - 2	CPLD 1 - 2 CPLD 2 - 3 CPLD 3 - 2
OS6900-T24C2	2019.08.00.03	2019.08.00.03	CPLD 1 - 2.0 CPLD 2 - 2.0 CPLD CPU - 6.0	CPLD 1 - 2.0 CPLD 2 - 2.0 CPLD CPU - 6.0
OS6900-X24C2	2019.08.00.03	2019.08.00.03	CPLD 1 - 6.0 CPLD 2 - 6.0 CPLD CPU - 6.0	CPLD 1 - 6.0 CPLD 2 - 6.0 CPLD CPU - 6.0
1. Optional CPU CPLD update to address CRAOS8X-30098. 2. Required CPLD update to address CRAOS8X-43968 (Hardware revision 6 only).				

**OmniSwitch 9900 - AOS Release 8.10.93.R03 (GA)**

Hardware	Minimum Coreboot- Uboot	Current Coreboot- Uboot	Minimum Control FPGA	Current Control FPGA	Minimum/ Current Power FPGA
OS99-CMM	8.3.1.103.R01	8.3.1.103.R01 8.7.30.R03 <sup>1</sup> 8.8.152.R01	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	-	-	-	-	-
OS9907-CFM2	-	-	-	-	-
OS9912-CFM	-	-	-	-	-
OS99-GNI-48	8.3.1.103.R01	8.3.1.103.R01 8.8.152.R01 <sup>2</sup>	1.2.4	1.2.4 1.2.5 <sup>2</sup>	0.9
OS99-GNI-P48	8.3.1.103.R01	8.3.1.103.R01 8.8.152.R01 <sup>2</sup>	1.2.4	1.2.4 1.2.5 <sup>2</sup>	0.9
OS99-XNI-48 (903753-90)	8.3.1.103.R01	8.3.1.103.R01 8.8.152.R01 <sup>2</sup>	1.3.0	1.3.0 1.5.0 <sup>2</sup>	0.6
OS99-XNI-48	8.6.261.R01	8.6.261.R01 8.8.152.R01 <sup>2</sup>	1.4.0	1.4.0 1.5.0 <sup>2</sup>	0.7
OS99-XNI-U48 (903723-90)	8.3.1.103.R01	8.3.1.103.R01 8.8.152.R01 <sup>2</sup>	2.9.0	2.9.0 2.11.0 <sup>2</sup>	0.8
OS99-XNI-U48	8.6.261.R01	8.6.261.R01 8.8.152.R01 <sup>2</sup>	2.10.0	2.10.0 2.11.0 <sup>2</sup> 2.12.0 <sup>3</sup>	0.8
OS99-GNI-U48	8.4.1.166.R01	8.4.1.166.R01 8.8.152.R01 <sup>2</sup>	1.6.0	1.6.0 1.7.0 <sup>2</sup> 1.8.0 <sup>3</sup>	0.2
OS99-CNI-U8	8.4.1.20.R03	8.4.1.20.R03 8.8.152.R01 <sup>2</sup>	1.7	1.7 1.9 <sup>2</sup> 1.10 <sup>3</sup>	N/A
OS99-XNI-P48Z16 <sup>4</sup>	8.4.1.20.R03	8.4.1.20.R03 8.8.152.R01 <sup>2</sup>	1.4	1.4 1.6 <sup>2</sup>	0.7
OS99-XNI-U24	8.5.76.R04	8.6.261.R01 8.8.152.R01 <sup>2</sup>	1.0	2.9.0 2.11.0 <sup>2</sup> 2.12.0 <sup>3</sup>	0.8
OS99-XNI-P24Z8 <sup>4</sup>	8.5.76.R04	8.6.261.R01 8.8.152.R01 <sup>2</sup>	1.1	1.4.0 1.6.0 <sup>2</sup>	0.7
OS99-XNI-U12Q <sup>4</sup>	8.6.117.R01	8.6.117.R01 8.8.152.R01 <sup>2</sup>	1.6.0	1.5.0 1.6.0 <sup>2</sup>	N/A
OS99-XNI-UP24Q2 <sup>4</sup>	8.6.117.R01	8.6.117.R01 8.8.152.R01 <sup>2</sup>	1.5.0	1.5.0 1.6.0 <sup>2</sup>	N/A
OS99-CNI-U20	8.9.183.R03	8.9.183.R03	1.2.0	1.2.0	0.4

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

Hardware	Minimum Coreboot- Uboot	Current Coreboot- Uboot	Minimun Control FPGA	Current Control FPGA	Minimum/ Current Power FPGA
<ul style="list-style-type: none"><li>2. Optional U-boot/FPGA update for CMM2 and OS9912 compatibility.</li><li>3. Optional FPGA upgrade to address CRAOS8X-43592: 1G/10G SFP not recognized.</li><li>4. Not currently supported in an OS9912 chassis.</li></ul> <p><b>Note:</b> Existing OS9900 NIs that are to be used with a CMM2 or in an OS9912 chassis must first have the Uboot and FPGA upgraded before using them with a CMM2 or inserting them into an OS9912 chassis. See footnote #2.</p>					

---

**[IMPORTANT] \*MUST READ\*: AOS Release 8.10R3 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 may ship from the factory with a diag.img file. This file is for internal switch diagnostic purposes only and can be safely removed.
- 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 use the **reset-fo-factory** command.
- 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<sup>1</sup>. 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.

## **Deprecated Features / Functionality Changes**

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

<b>AOS Release 8.5R4</b>
EVb - Beginning in 8.5R4, support for EVb is being removed. Any switches with an EVb configuration cannot be upgraded to 8.5R4 or above.
NTP - Beginning with AOS Release 8.5R4, OmniSwitches will not synchronize with an unsynchronized NTP server (stratum 16), as per the RFC standard. Existing installations where OmniSwitches are synchronizing from another OmniSwitch, or any other NTP server which is not synchronized with a valid NTP server, will not be able to synchronize their clocks. The following NTP commands have been deprecated:
- ntp server synchronized
- ntp server unsynchronized
<b>AOS Release 8.6R1</b>
DHCPv6 Guard - Configuration via an IPv6 interface name is deprecated in 8.6R1. Commands entered using the CLI must use the new 'ipv6 dhcp guard vlan vlan-id' format of the command. The old format will still be accepted if present in a vcboot.cfg to preserve backwards compatibility.
IP Helper - The 'ip helper' commands have been deprecated in 8.6R1 and replaced with 'ip dhcp relay'. The old format will still be accepted if present in a vcboot.cfg to preserve backwards compatibility.
SAA - The vlan-priority and drop-eligible parameters have been deprecated from all SAA commands beginning in 8.6R1.
MACsec is now supported on ports 33-48 of the 6560-(P)48X4. CRAOS8X-7910 was resolved in 8.6R1.
<b>AOS Release 8.6R2</b>
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.

<b>AOS Release 8.7R1</b>
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 <a href="#">Appendix C</a> for additional information.
<b>AOS Release 8.7R2</b>
There are new default user password policies being implemented in 8.7R2. This change does not affect existing users.
<ul style="list-style-type: none"> <li>- cannot-contain-username: enable</li> <li>- min-uppercase: 1</li> <li>- min-lowercase: 1</li> <li>- min-digit: 1</li> <li>- min-nonalpha: 1</li> </ul>
<p>The OmniSwitch 6360 does not contain a real-time clock.</p> <ul style="list-style-type: none"> <li>- It is recommended to use NTP to ensure time synchronization on OS6360s.</li> <li>- When the switch is reset, the switch will boot up from an approximation of the last known good time.</li> <li>- 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.</li> </ul>
<b>AOS Release 8.7R3</b>
The Kerberos Snooping is not supported in bridge mode in this release.
<b>AOS Release 8.8R1</b>
<p>Unsupported commands (Part of AOS 88R1 but not supported)</p> <ul style="list-style-type: none"> <li>- mrp interconnect</li> <li>- show mrp interconnect</li> <li>- clear mrp interconnect</li> </ul>
<p>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.</p> <p><b>OS6560-BP-PH</b> - This OS6560 600W power supply, OS6560-BP-PH (904072-90), requires a minimum AOS version of 8.8R1.</p> <p><b>OS6560-BP-PX</b> - This OS6560 920W power supply, OS6560-BP-BX (904073-90), requires a minimum AOS version of 8.8R1.</p> <p>Refer to the OmniSwitch 6560 Hardware Guide for additional power supply information.</p>
<b>AOS Release 8.8R2</b>
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.
<b>AOS Release 8.9R1</b>
Metro License Features - Some Metro features are now licensed on the OS6560 beginning in 8.9R1. See <a href="#">Metro License</a> for information on re-enabling them after upgrading to 8.9R1.
<b>AOS Release 8.9R4</b>
OmniSwitch 6570 signed AOS image support with proper u-boot was added.
<b>AOS Release 8.10R1</b>
CRAOS8X-46556 (CVE-2024-6387) fix has been implemented by default in 8.10R1. See <a href="#">Appendix K: Fixed CVEs</a> .
<b>AOS Release 8.10R2</b>
<ul style="list-style-type: none"> <li>- Support for OVSDDB removed.</li> <li>- The administrative state for the automatic fabric feature is disabled by default.</li> </ul>



- The U-boot version on the OS6570M models shipping from the factory is 8.10.42.R02. This U-boot version supports signed AOS images only (8.9R4 and above). To use AOS releases prior to 8.9R4 the u-boot version must first be downgraded to a version below 8.9.70.R04 before downgrading AOS.

#### **AOS Release 8.10R3**

Starting with release 8.10R3, it is mandatory to configure VXLAN BGP EVPN services and associated configurations within the VRF context. Therefore, after upgrading to 8.10R3, any existing EVPN configurations from earlier releases must be manually reconfigured under the appropriate VRF context. See [EVPN - VRF-based Tenancy Model for AOS EVPN Services](#).

## 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
Licensed Features	
DCB (PFC,ETS,DCBx)	Not Supported
FIP Snooping	Not Supported
FCoE VxLAN	Not Supported

	Feature/Performance License Required								
	OS6360	OS6465	OS6560	OS6570M	OS6860	OS6860N	OS6870	OS6900	OS9900
Licensed Features									
MACsec (OS-SW-MACSEC)	N/A	Yes	Yes	Yes	Yes	Yes	Yes	Yes <sup>3</sup>	Yes
10G Support (OS6560-SW-PERF)	N/A	N/A	Yes <sup>1</sup>	N/A	N/A	N/A	N/A	N/A	N/A
10G Support (OS6360-SW-PERF)	Yes <sup>2</sup>	N/A	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 <sup>4</sup>	N/A	N/A	N/A	N/A	N/A
MPLS Support (OS####-MPLS-#)	N/A	N/A	N/A	N/A	N/A	Yes	N/A	Yes	N/A
50G Support (OS6870-SW-PERF)	N/A	N/A	N/A	N/A	N/A	N/A	Yes <sup>5</sup>	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. 5. Performance software license is optional allowing the OS6870-LNI-U6 ports to operate at 50G speed. Ports support up to 25G 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
<b>Note:</b> 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)
PIM Multicast Routing (IPv4 & IPv6)	Yes	Yes
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
BGP	Yes	Not Supported
<b>Note:</b> The table above lists the features supported with the Advanced Routing license.		

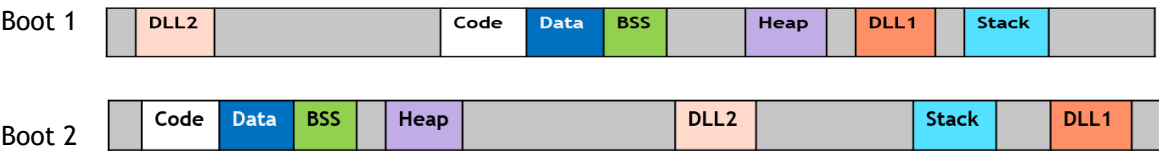
**ALE Secure Diversified Code**

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.

### **8.10R3 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
<b>Management Features</b>	
Lightning Configuration Enhancements	All (except 9900)
Reset to Factory Default	All (except 9900)
Change Password on First Access Warning	All
Toggle Switch Port Enhancement	All
Importable Certificate for Webview HTTPS	All
Weak Cryptographic User Warning	All
Clearing AOS Alarms Automatically	6465
Support HTTP-based File Transfer for Appmon for OVC Management	6860(E), 6860N, 6870
Profinet Support and Certification	6465
Support for FDB Double Tag Learning/Lookup	6570M
AAA IPv6 Address Support	All
<b>Layer 3 Features</b>	
Lightweight DHCPv6 Relay Agent (LDRA) (RFC 6221)	6560, 6570M
OSPFv3 CLI to Enable Default-originate	6560, 6570M, 6860(E), 6860N, 6865, 6870, 6900, 9900
RIPv2 RFC-4822 Support	All (except 6360)
IPv6 Ready Logo	All
<b>Service Features</b>	
QinQ Support	9900
Extended Hashing Mechanism in SPB Fabric	9900
Strict CVLAN Filtering on SAP UNI (BUM Traffic)	6860(E), 6860N, 6870, 6900
Support of Switch Supplicant for SAP Ports	All
QoS Support for Services	6860N, 6870, 6900, 9900
EVPN - Route Redistribution for Prefix Route Advertisement for Symmetric IRB	6900 (except V72/C32)
EVPN - BGP NBR Template and Scalability	6900 (except V72/C32)
EVPN - VRF-based Tenancy Model for AOS EVPN Services	6900 (except V72/C32)
IPv6 SPB Management Support	6860(E), 6860N, 6865, 6870, 6900, 9900
DHCPv6 Snooping/Guard on SPB/L2GRE Services	6860N, 6870, 6900, 9900
MLD Snooping Support on VxLAN/MPLS SAPs	6860N, 6900
<b>QoS/Security Features</b>	
MACsec Dynamic Support Using RADIUS	6465, 6560, 6570, 6870, 6860, 6860N, 6900-X48C4E, 9900

Feature	OmniSwitch Platform
Anti-Spoofing Support for IPv6	6560, 6570M, OS6870, 6860N, 6900, 9900
UNP Trust Tag Enhancement	All
Policy Condition Destination Port Parity	6560, 6570M
MACsec 256-bit Support	6570M, 6870, 6860N, OS6900-X48C4E, OS99-CMM2
UNP AP Mode Support for Celona AP	All
WAN MACsec Support	6570M, 6870
Security Enhancements	All
<b>Other Features</b>	
IPv4 Multinetting Interfaces Enhancement	6560, 9900
sFlow Extended Data Enhancement	All
sFlow Sampling Rate of 1	9900
PPPoE Intermediate Agent - Circuit ID Enhancement	6465, 6560, 6860, 6865, 6870
<b>Parity Features</b>	
Ethernet Loopback Test	6870
EEE support	6870
NAPALM Support	6870
Server Load Balancing (SLB)	6870
IoT Device Profiling	6870
IoT Device Profiling (IPv6)	6870
TDR	6870
Thin Client	6870
Multi-gig 10M Support	6870
1588v2 PTP	6570M
PVLAN	6560
Forward Error Correction (FEC)	6870
<b>EA Features</b>	
CPE Testhead	6870
RoCEv2 Support	6900
EVPN - Multicast Routing Over an EVPN Fabric (RFC 9625) - OISM & PIM Support	6900 (except V72/C32)

## Management Features

### Lightning Configuration Enhancements

Added options for Multicast Zapping and enabling 802.3bt for PoE under Lightning Configuration.

- Lightning configuration is now supported on the OmniSwitch 6465, 6560, and 6570M switches using front panel ports 1/1/1 and 1/1/2.
- Lightning configuration is now supported on the OmniSwitch 6860(E), 6865, 6860N, 6870, and 6900 using the EMP port or USB-Ethernet dongle.
  - A USB-Ethernet dongle can be used for models without a physical EMP port.
  - Front panel ports are not supported.
  - HTTPS/Webview and SSH are supported but the Lightning Configuration Wizard is not supported.
  - Lightning configuration will be enabled for a duration of 1 hour.

### Reset to Factory Default

This feature can be used to remove all or a subset of custom configurations on the switch and restore them to the original factory settings.

- The **all** parameter removes all switch configurations, licenses, certificates, packages etc. The images in the certified and working directories are retained.
- The **config** parameter removes all switch configurations only. The images in the certified and working directory, switch licenses, packages and certificates will be retained.
- The **retain-vc** parameter removes all switch configurations except the VC configuration. The images in the certified and working directories, switch licenses, packages and certificates will be retained.

The following CLI commands are associated with this feature:

- `reset-to-factory [all | config [retain-vc]] [in seconds] [cancel]`

### Change Password on First Access Warning

Beginning in 8.10R3 a warning message will be displayed urging for the default password to be changed when logging in using the 'admin' account. Beginning in 8.10R4 changing the default password will be mandatory.

### Toggle Switch Port Enhancement

This enhancement toggles a switch or PoE port or range of ports without changing the RUNNING configuration on the switch. This can be used without having to administratively disable and re-enable a port which avoids having to perform a write memory to re-synchronize the configuration.

The following CLI commands are associated with this feature:

- `interfaces {slot chassis/slot | port chassis/slot/port[-port2]} reset`

- `lanpower port chassis/slot/port[-port2] reset`

### Importable Certificate for Webview HTTPS

Use this feature to update the custom CA-signed certificate intended for Webview authentication. By using this command, you can replace the default WebView certificate that is originally included within the AOS images.

The following CLI commands are associated with this feature:

- `aaa certificate install-certificate webview web-certificate`

### Weak Cryptographic User Warning

A warning message will be displayed if a weak cryptographic algorithm (SHA, MD5, SHA+DES, MD5+DES, SHA+AES) is being used for a user account. These algorithms are not secure and are susceptible to attack. They will be disabled by default in a future release.

The following CLI commands are associated with this feature:

- `user username password password {sha | md5 | sha+des | md5+des | sha+aes}`

### Clearing AOS Alarms Automatically

The current AOS behavior is to clear reported OS6465 alarms after a default or configured duration of time, starting from the time of the alarm condition. This enhancement clears the alarm status, for the events listed below, as soon as the alarm is no longer present. The CLI will continue to support manually clearing the alarm.

- Port-Health - When the port crosses the threshold on receive/transmit or receive average.
- System-Health - When switch crosses the threshold on CPU, memory or flash.
- Power-Supply - When one of the power supply fails.
- Temperature - When the temperature crosses above threshold.
- Authentication-Failure - When console/telnet/ftp/https/ssh session authentication fails.
- Port-Violation - When the port is violated due to storm, etc.
- Link-Down - When there is a link failure on a port or range of ports.
- Alarm Input - When the alarm input is triggered.

### Support HTTP-based File Transfer for AppMon for OVC Management

The OmniSwitch supports the downloading of the OVC signature kit and upload of CSV files using the HTTP, this avoids the use of OVC or OVE interface. The HTTP interface can be used since a VPN is already established from AOS and AP devices to OVC. By using the HTTP URL from OVC, the switch can:

- Download the Appmon Signature Kits.
- Upload the Appmon CSV Flow Record Files.

The following new CLIs have been introduced to configure this feature:

- `app-mon signature-kit url url checksum checksum status-url status-url`
- `app-mon upload file file-name url url`
- `app-mon install signature-kit`



## Profinet Support and Certification

PROFINET support in OmniSwitch platform brings industrial-grade Ethernet communication to enterprise-class network infrastructure. With the ability to handle real-time automation traffic, device discovery, redundancy, and diagnostics, OmniSwitch becomes a critical backbone for modern Industrial Ethernet environments. By leveraging AOS features such as VLAN management, QoS, CLI-based configuration, and extensive monitoring, PROFINET deployment on OmniSwitch ensures:

- Reliable and deterministic communication for industrial applications.
- Seamless integration with automation controllers and field devices.
- Improved network security and segmentation using VLANs.
- Ease of management and troubleshooting via AOS CLI.
- The `nos-pnet-v1.deb` package is required.

The following CLI commands are associated with this feature:

- `pkgmgr {install | remove | verify} <package_name>`
- `profinet admin-state {enable | disable}`
- `profinet vlan <vlan_id>`
- `profinet device-name`
- `show profinet status`
- `show profinet sessions`

**Note:** Profinet certification is currently pending.

## Support for FDB Double Tag Learning/Lookup

This enhancement allows to configure FDB (Forwarding Database) Double-Tag Learning. FDB (Forwarding Database) Double-Tag Learning enables learning and lookup of MAC addresses based on both SVLAN (Service VLAN) and CVLAN (Customer VLAN) tags.

The following CLI is introduced to enable the FBD-Double-Tag-Lookup:

- `ethernet-service double-tag-lookup {enable | disable}`

The following show CLI are modified to display the configuration:

- `show ethernet-service`
- `show mac-learning`

## AAA IPv6 Address Support

The enhancement includes IPv6 address support for syslog servers in AAA configurations.

The following CLI commands are associated with this feature:

- `aaa accounting`
- `aaa profile`
- `show aaa profile`

## **Layer 3 Features**

### **Lightweight DHCPv6 Relay Agent (LDRA) (RFC 6221)**

This enhancement introduces Lightweight DHCPv6 Relay Agent (LDRA) functionality on VLAN domains where only VLANs are configured without an IPv6 interface. LDRA enables an OmniSwitch to act as a lightweight DHCPv6 relay agent by converting client solicit messages into relay-forward messages. It uses Interface-ID to ensure accurate DHCPv6 message processing. This ensures secure client-server communication.

The following CLI commands are associated with this feature:

- `ipv6 dhcp guard vlan ldra admin-state {enable | disable}`
- `show ipv6 dhcp guard`

### **OSPFv3 CLI to Enable Default-originate**

The enhancement allows to advertise a default route into an OSPFv3 routing domain. This is helpful when a router must propagate a default route dynamically based on the presence of an existing default route or unconditionally. This enhances optimal path selection based on the network design.

The following CLI commands are associated with this feature:

- `ipv6 ospf default-originate {only | always} [metric-type {type1 | type2}] [metric value]`

### **RIPv2 RFC-4822 Support**

Enhances SHA256 authentication for RIPv2, improves security by aligning with RFC-4822 - RIPv2 Cryptographic Authentication. This update allows the use of SHA256 in key-chain-based authentication along with the previously supported MD5 method. The enhancement includes a new configuration parameter “key-chain” to configure key-chain authentication mechanism.

The following CLI commands are associated with this feature:

- `ip rip interface auth-type`

### **IPv6 Ready Logo**

This enhancement introduces support for configurable lifetime values in IPv6 Router Advertisement (RA) options for:

- RDNSS (Recursive DNS Server)
- DNSSL (DNS Search List)

Users can now specify the lifetime (in seconds) for both RDNSS and DNSSL groups, particularly for vendors and deployments requiring flexible RA lifetimes. This allows greater control over DNS option validity and RA behavior.

The following CLI are modified:

- `ipv6 ra-dnssl-group groupname [lifetime <num>]`
- `ipv6 ra-rdnss-group groupname [lifetime <num>]`
- `show ipv6 router ra-options`

**Note:** The IPv6 Ready Logo certification is currently pending.

---

## Services Features

### QinQ Support

The following features will be supported on the OmniSwitch 9900 from this release.

- Basic QinQ functionality
- Uni profile with basic protocol support
- Uni profile with Custom protocol support
- Transparent Bridging
- QinQ IP interface on CVLAN

The following CLI commands are associated with this feature.

- Basic QinQ functionality
  - ethernet-service svlan
  - ethernet-service service-name
  - ethernet-service nni
  - ethernet-service svlan nni
  - ethernet-service sap
  - ethernet-service sap uni
  - ethernet-service sap cvlan
  - ethernet-service sap-profile
  - ethernet-service sap sap-profile
  - ethernet-service uni-profile
  - ethernet-service uni-profile inbound 802.1ab
  - ethernet-service uni uni-profile
  - show ethernet-service vlan
  - show ethernet-service
  - show ethernet-service sap
  - show ethernet-service port
  - show ethernet-service nni
  - show ethernet-service uni
  - show ethernet-service uni-profile
  - show ethernet-service sap-profile
- Uni profile with basic protocol support
  - ethernet-service uni-profile L2-protocol
- Uni profile with Custom protocol support
  - ethernet-service custom-L2-protocol
  - ethernet-service uni-profile custom-L2-protocol
  - show ethernet-service custom-l2-protocol
- Transparent Bridging
  - ethernet-service transparent-bridging
- QinQ IP interface on CVLAN
  - ip interface <name> [address <ipaddr>] [mask <ipmask>] [mapped-cvlan <cvlanId>]
- MAC-Tunneling
  - ethernet-service mac-tunneling
  - ethernet-service svlan mac-tunneling
  - show ethernet-service mac-tunneling
- L2PT Statistics
  - show ethernet-service nni l2pt-statistics
  - clear ethernet-service nni l2pt-statistics

- show ethernet-service uni l2pt-statistics  
clear ethernet-service uni l2pt-statistics
- show ethernet-service uni-profile l2pt-statistics  
clear ethernet-service uni-profile l2pt-statistics

### **Extended Hashing Mechanism in SPB Fabric**

This feature extends the hashing mechanism in SPB fabric on OS9900. This feature incorporates source or destination IPs and ports within SPB packets into the hashing algorithm.

The following CLI commands are associated with this feature:

- hash-control extended spb-payload
- hash-control extended no spb-payload
- show hash-control

### **Strict CVLAN Filtering on SAP UNI (BUM Traffic)**

This feature supports enabling or disabling the mechanism to prevent flooding of BUM traffic received on NNI port towards unwanted SAP.

The following CLI commands are associated with this feature.

- ethernet-service strict-vlan-filter {enable|disable}
- show ethernet-service strict-vlan-filter

### **EVPN - Route Redistribution for Prefix Route Advertisement for Symmetric IRB**

When a Fabric-vpn service is created on a particular VRF, it triggers BGP EVPN to auto import all routes exported by fabric-service VRF. A redistribution configuration is required to support importing of routes so that BGP EVPN can register for route imports from additional VRFs.

Route Redistribution for prefix route advertisement for Symmetric IRB is supported using the following command. The following CLI commands are associated with this feature.

- service redistrib source-vrf

### **EVPN - BGP NBR Template and Scalability**

The purpose of the BGP neighbor template is to simplify the BGP peer configuration and reduce the configuration snapshot size drastically in a case where higher number of peers use the similar configuration. The individual BGP peer configuration will take precedence over the BGP neighbor template configuration. New CLI commands are provided to create new BGP neighbor template. This can be used to create the fields for the template. This template can be modified or deleted. The template can be later applied on the on the BGP neighbor.

This template can be used especially for the spines to configure the number of peers as Route Reflector clients in Route Reflector topology (spine and leaf topology) in the EVPN network.

The following CLI commands are associated with this feature.

- ip bgp nbr-template
- ip bgp neighbor nbr-template
- show ip bgp nbr-template

- show configuration snapshot bgp

## EVPN - VRF-based Tenancy Model for AOS EVPN Services

The EVPN service follows the VRF-based Tenancy model, which mandates the EVPN configurations to be executed under non-default VRF context, including the show commands to view the EVPN specific configuration. For example, the configuration syntax will be in the VRF context:

```
-> vrf create vrf1
vrf1:-> service 50 vxlan vnid 50 bgp-evpn enable
vrf1:-> service 50 sap linkagg 120:10
```

- There is no change to the syntax for provisioning a service and its parameters, and the SAP association. It must be executed in the context of a non-default VRF.
- EVPN based services and the attachment to these services (BD to Service Mapping) are provisioned within the context of a VRF. Layer 3 configuration on EVPN services is executed in the VRF context.
- The access port configuration for the EVPN service is done in the default VRF instance.

**Note:** Starting with release 8.10R3, it is mandatory to configure the VXLAN BGP EVPN service and associated configurations within the VRF context. Therefore, after upgrading to 8.10R3, any existing EVPN configurations from earlier releases must be manually reconfigured under the appropriate VRF context.

The following CLI commands can be used to display the VRFs and the BDs associated with a EVPN service, and list of EVPN services and the BDs associated with the service for a specific VRF.

- show service tenancy service service\_id
- show service tenancy vrf vrf\_name [vlan {all | vlan\_id}]

## Support of Switch Supplicant for SAP Ports

As part of this feature, switch supplicant secure mode feature will be supported on UNP bridge and access ports and Linkagg. This feature will be supported on SPB, L2GRE, and VxLAN service types. Switch supplicant secure mode is used to avoid the multiple authentication of the clients connected to supplicant switch.

When this feature is enabled on the UNP bridge or access port or linkagg, the clients of the supplicant switch will be directly learnt in trust-tag mode (in case of bridge port or linkagg) or classification mode (in case of access port or linkagg) without the user being subjected to 802.1x or MAC authentication.

The following CLI commands are associated with this feature.

- unp sw-supp-secure-mode
- unp port-template
- show unp port config
- show unp port-template

## QoS Support for Services

This feature enhancement adds the following:

- Supports policy rule logging for traffic ingressing on the SAP/SDP ports on the edge nodes for services.
- Policy condition qualifier with source service-id (ingress ACL) to filter traffic based on service ID is supported. This enhancement can be used along with the current policy condition support.

- Marking of service packets in the edge nodes will be carried end to end, and queuing will be based on the marked 802.1p value.

The following CLI commands are associated with this feature:

- policy condition source service-id
- show policy condition

### **IPv6 SPB Management Support**

This enhancement adds support for SPB Management over IPv6.

### **DHCPv6 Snooping/Guard on SPB/L2GRE Services**

DHCPv6 Guard and DHCPv6 Snooping commands are supported on SPB service and L2GRE service as a part of this feature.

The following CLI commands are associated with this feature.

- ipv6 dhcp guard service
- dhcpv6-snooping service admin-state
- dhcpv6-snooping binding service

No specific modification done for this release in the following commands. However, the existing service field will display the configured service details for SPB and L2 GRE also, which is common to all the services.

- show ipv6 dhcp guard
- show ipv6 dhcp guard service <serviceld>
- show dhcpv6-snooping
- show dhcpv6-snooping interfaces
- show dhcpv6-snooping binding

### **MLD Snooping Support on VxLAN/MPLS SAPs**

As part of this feature, IPMSv6 (MLD snooping ) is extended to VPLS service . The existing IPMSv6 commands are supported over VPLS service as well.

The following CLI commands are associated with this feature.

- ipv6 multicast admin-state
- ipv6 multicast flood-unknown
- ipv6 multicast version
- ipv6 multicast port max-group
- ipv6 multicast max-group
- ipv6 multicast static-neighbor
- ipv6 multicast static-querier
- ipv6 multicast static-group
- ipv6 multicast query-interval
- ipv6 multicast last-member-query-interval
- ipv6 multicast query-response-interval
- ipv6 multicast unsolicited-report-interval

- ipv6 multicast router-timeout
- ipv6 multicast source-timeout
- ipv6 multicast robustness
- ipv6 multicast spoofing
- ipv6 multicast spoofing static-source-ip
- ipv6 multicast zapping
- ipv6 multicast querier-forwarding
- ipv6 multicast proxying
- ipv6 multicast helper-address
- ipv6 multicast zero-based-query
- ipv6 multicast forward-mode
- ipv6 multicast update-delay-interval
- ipv6 multicast fast-join
- ipv6 multicast profile
- ipv6 multicast apply-profile
- show ipv6 multicast
- show ipv6 multicast port
- show ipv6 multicast forward
- show ipv6 multicast neighbor
- show ipv6 multicast querier
- show ipv6 multicast group
- show ipv6 multicast source
- show ipv6 multicast tunnel
- show ipv6 multicast bridge
- show ipv6 multicast bridge-forward
- show ipv6 multicast profile

## **QoS/Security Features**

### **MACsec Dynamic Support Using RADIUS**

Introduces support for dynamic MACsec keying using RADIUS for host-based authentication. When a supplicant host connects to a UNP-enabled port with MACsec mode set to dynamic RADIUS, MACsec sessions are established dynamically based on RADIUS-supplied keys after successful 802.1X authentication using EAP-TLS.

The enhancement enables per-host MACsec session establishment based on 802.1X authentication and RADIUS-supplied policies and keys. Each authenticated host can establish a separate MACsec session with individualized security parameters.

The following CLIs are related to this feature:

- interfaces macsec admin-state
- show interface macsec
- show interface macsec statistics description

### **Anti-Spoofing Support for IPv6**

Introduces IPv6 Anti-Spoofing support, extending the existing IPv4 protection. This feature blocks unauthorized IPv6 traffic by verifying source IPv6 addresses against VLAN subnets. The **spoofv6** parameter is introduced to filter and shutdown the IPv6 spoofing traffic and ports.

The OS6860N and OS6900 platforms support this feature in default mode. The OS9900, OS6560, OS6570, and OS6870 platforms support this feature in enhanced mode (with source-IPv6 TCAM profile).

The following CLI commands are associated with this feature:

- qos user-port
- show qos config
- show qos statistics

### **UNP Trust Tag Enhancement**

The enhancement introduces a new feature to enhance User Network Profile (UNP) user learning by adding a configurable "trust-tagged-vlans" parameter. This allows administrators to specify VLANs that should be considered trusted for learning users, even if their VLAN tag does not match the UNP profile's primary VLAN mapping. This enhances UNP user learning by allowing the configuration of trusted VLANs within a UNP profile to address security concerns with tagged packets.

A new RADIUS Vendor specific attribute "Alcatel-Trust-Tagged-vlans" is added in the RADIUS Attributes definition list. This attribute is of type "string" and is of a maximum length of 255 characters including the VSA tag and length of the attribute. This attribute contains list of continuous or non-contiguous VLAN or VLAN-range(s).

The following CLI commands are associated with this feature:

- unp profile trust-tagged-vlans
- show unp profile trust-tagged-vlans

### **Policy Condition Destination Port Parity**

This enhancement provides support for destination port and destination VLAN qualifiers in the egress policy list for OS6570M and OS6560 platforms. This allows applying QoS policies at the egress level based on destination ports and VLANs.

### **MACsec 256-bit Support**

This enhancement adds support for 256-bit encryption and 64-bit extended packet numbering which can be configured on higher bandwidth interfaces to help avoid frequent SA Key rotation. The following encryption algorithms can be configured with the cipher-suite parameter and are supported on the 6570M, 6870, OS6900-X48C4E, OS99-CMM2 only.

- **gcm-aes-128** - gcm-aes-128-bit encryption with 32-bit packet numbering.
- **gcm-aes-256** - gcm-aes-256-bit encryption with 32-bit packet numbering.
- **gcm-aes-xpn-128** - gcm-aes-128-bit encryption with 64-bit packet numbering.
- **gcm-aes-xpn-256** - gcm-aes-256 encryption with 64-bit packet numbering.

The following CLI commands are associated with this feature:

- interfaces macsec mode dynamic cipher-suite

### **UNP AP Mode Support for Celona AP**



Support for MAC-OUI-based Access Point (AP) detection has been introduced in the Access Guardian (AG) module to extend UNP AP Mode functionality to APs which do not advertise the required LLDP TLVs. This enhancement ensures that APs can be correctly classified as AP devices and that Trust-tag-based learning is enforced for client devices connecting through them.

The following CLI are introduced to include this feature:

- `unp ap-mode mac-oui [mac_oui1 | mac_oui2 | mac_oui3]`
- `show unp global configuration`

## WAN MACsec Support

WAN MACSEC provides end-to-end Layer-2 encryption over untrusted intermediate nodes (e.g., SP MPLS networks) where only the endpoints are MACSEC-capable. This allows ethernet services to be securely extended across WANs. The following enhancements are made to implement this feature:

- Clear-Tag mode is introduced to ensure intermediate switch classification.
- Confidentiality Offset can be configured to allow partial encryption.
- Control Protocol Bypass Profile can be configured to bypass encryption for selected L2 protocols.
- Custom MKA Profile can be configured to include customized ethernet type and destination MAC for MKA packet.
- Replay Protection Window is introduced to support out-of-order packet tolerance.

The following new CLI are introduced to support configuration:

- `interfaces macsec clear-tag-mode`
- `interfaces macsec confidentiality-offset`
- `interface macsec control-protocol-bypass-profile`
- `interface macsec mka-profile`
- `interfaces macsec replay-protection-window`
- `show interface macsec control-protocol-bypass-profile`
- `show interface macsec mka-profile`
- `show interface macsec wan-macsec`

## Security Enhancements

This enhance allows and administrator to enforce a password refresh for a specific user or all users upon their next login.

- `user password-refresh`
- `user <string> password-refresh`

This enhancement provides the ability to convert certificates in DER, PEM, PKCS#12, and P7B to PEM format.

- `aaa certificate convert-cert`

This enhance provides the ability to check a certificate's revocation status using either CRL (Certificate Revocation List) or OCSP (Online Certificate Status Protocol). Currently supported for Radius and Syslog over TLS.

- `ssl pki check-revocation`

## **Other Features**

### **IPv4 Multinetting Interfaces Enhancement**

The number of IPv4 interface per VLAN (Multinetting) is increased to 16 for the OS6560 and 32 for the OS9900.

### **Enhancement of sFlow Extended Data**

This update enhances sFlow monitoring by introducing extended data fields for improved network visibility and analytics. Key Enhancements:

- **Extended Ethernet Frame Data** - Captures MAC packet length, source and destination MAC address, Ethernet packet type.
- **Extended IPv4/IPv6 Data** - Captures Length of IP packet, IP Protocol (TCP/UDP), Source IP Address, Destination IP Address, Source Port, Destination Port, TCP Flag (8-bit), TCP TOS (precedence 3-bit + DSCP 5-bit).
- **Extended Switch Data** - Captures VLAN ID & priority for incoming/outgoing traffic.
- **Extended Router Data** - Adds next-hop IP and subnet mask details.

The following CLI commands are associated with this feature:

- sflow extended switch-info
- sflow extended router-info
- show sflow detail

### **sFlow Sampling Rate of 1**

This feature enhancement enables an sFlow sampling rate of 1 on the OS9900.

A sampling rate of 1 does not guarantee that all packets will be sent to the sFlow collector. The system includes a built-in backoff mechanism that may be triggered based on system load to ensure reliable operation.

### **PPPoE Intermediate Agent - Circuit ID Enhancement**

The enhancement allows to modify PPPoE Circuit ID authentication formatting in AOS8 for compatibility with older authentication servers. Users can switch between AOS6 (*chassis/port*) and AOS8 (*chassis/slot/port*) formats.

The following CLI commands are associated with this feature:

- pppoe-ia ignore-slot

## **Parity Features**

### **Ethernet Loopback Support**

Ethernet Loopback is now supported on the OmniSwitch 6870 starting in 8.10R3 using the inbuilt custom TCAM profile to “metro-service-2” option.

The following CLI commands are associated with this feature.

- tcam profile
- show tcam profile

### **EEE Support**

Energy Efficient Ethernet (EEE) is supported on the OS6870 beginning in 8.10R3.

### **NAPALM Support**

NAPALM is supported on the OS6870 beginning in 8.10R3.

### **Server Load Balancing (SLB) Support**

This enhancement adds Server Load Balancing (SLB) functionality to the OS6870 starting in 8.10R3.

- For OS6870, an IP interface must be configured on the ingress VLAN for SLB and PBR to function.

### **IoT Device Profiling**

IoT Device Profiling for IPv4 and IPv6 is supported on the OS6870 beginning in 8.10R3.

### **TDR**

TDR is supported on the OS6870 on the following ports beginning in 8.10R3.

- OS6870-24 - Ports 1-24
- OS6870-48 - Ports 1-48
- OS6870-P24M - Ports 1-24
- OS6870-P48M - Ports 1-48
- OS6870-P24Z - Ports 1-24
- OS6870-P48Z - Ports 1-48

### **Thin Client**

Thin Client is supported on the OS6870 beginning in 8.10R3.

### **Multi-gig 10M Support**

Support for 10M speed on the multi-gig ports for the OS6870-P24M/P48M/P24Z/P48Z platforms was added in 8.10R3.

### **1588v2 Precision Time Protocol (PTP)**

1588v2 PTP End-to-End and Peer-to-Peer Transparent Clock is now supported on all ports of the OS6570M-12/12D/U28 models in a VC-of-1 configuration.

## PVLAN

PVLAN is now supported on the OmniSwitch 6560 starting in 8.10R3.

## Forward Error Correction (FEC)

FEC is now supported on the OmniSwitch 6870 starting in 8.10R3.

## EA Features

### CPE Testhead Support

To support CPE Testhead functionalities on the OS6870 platform, it is mandatory to configure the built-in custom TCAM profile to “metro-service-2” option. To support this, a new parameter is introduced in the TCAM profile command.

The following CLI commands are associated with this feature.

- tcam profile
- show tcam profile

### EVPN - Multicast Routing Over an EVPN Fabric (RFC 9625) - OISM & PIM Support

Optimized Inter-Subnet Multicast(OISM) is an EVPN-based solution that optimizes how IP multicast traffic is forwarded across different subnets within a network. OISM is standardized in RFC9625. It specifies a solution for multicast routing across different IP subnets of a tenant using fabric IRB routing interface. This does not require any native multicast routing protocols, like PIM (Protocol Independent Multicast). In RFC 9625, fabric IRB is referred as SBD (Supplemental Bridge Domain) and the user services as BD (Bridge Domain).

The following CLI commands are associated with this feature.

- service service\_id oism {enable | disable}
- service bgp-evpn
- show service debug-info

### EVPN - PIM EVPN Gateway

PIM-EVPN Gateway (PEG) feature is to enable the border leaf nodes in the EVPN network to interwork with external PIM enabled networks so that multicast receivers or senders in the EVPN will be able to receive or send multicast traffic from or to the senders/receivers in external PIM network.

The following CLI commands are associated with this feature.

- Existing CLI can be used to enable PIM on EVPN fabric interface on the border leaf.

### RoCEv2 Support

RoCEv2 is partially supported as an early availability feature on the following models in 8.10R3:

- ECN marking is supported on the OS6900-V48C8/C32E/X48C6/T48C6.
- ECN marking is not supported on the OS6900-T24C2 and X24C2 models.
- PFC is not supported any of these platforms.

## 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-23137	When 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-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-48631	PTP 1588v2 E2E TC - Issue of high "2-way time error mean" observed on OS6870-P24Z/P48Z and OS6870-P24M/P48M with expansion modules when PTP packets ingress at copper port and egress out of fiber ports and vice versa.	There is no known workaround at this time.
CRAOS8X-52700	Compared to previous releases, there can be a slight increase in time taken by the 'write memory flash-synchro' and 'copy running certified flash-synchro' commands. This is due to the increase in size of the AOS images compared to the previous releases.	There is no known workaround at this time, wait for the flash-synchro command to complete.
CRAOS8X-52134	<p>PTP time stamping does not happen correctly when PTP packets ingress on PHY-based ports and egress on PHYLESS ports and vice versa.</p> <p>PTP traffic ingressing on OS6870-V12 ports 1/1/1-12 and egressing on ports 1/1/13-14, CNI-U2 or LNI-U6 ports or vice versa, PTP timestamping does not happen correctly and causes the high 2wayTimeError.</p> <p>PTP traffic ingressing on OS6570-U28 ports 1/1/1-24 and egressing on ports 1/1/25-30 ports or vice versa, PTP timestamping does not happen correctly and causees the high 2wayTimeError.</p>	There is no known workaround at this time.
CRAOS8X-51085	On an OS9900, after successful supplicant switch authentication some MAC addresses may be randomly flushed. The MAC addresses will eventually be learned again.	There is no known workaround at this time.

CRAOS8X-51052	Frequent and numerous VRF deletion and creation when configuring 40 or more VRFs may result in the restriction of subsequent VRF creation to preserve system resources.	There is no workaround at this time, and users are recommended to avoid repeated deletion and creation of VRF instances.
Hardware / Transceivers		
CRAOS8X-35816	SFP-10G-T supports only 10G peer links. Link will be down when peer speed is either 1G or 100M. If peer 1G or 100M is left connected, after some idle time, some quick down>up toggles may be seen locally. When peer is changed to 10G, port will operate as expected. However, it has been observed, if peer is left at 100M for a lengthy period, and multiple down>up toggles are seen, port may not recover even after reverting back to 10G.	Recommend peer end to be strictly at 10G.
CRAOS8X-36381	It is possible with SFP-GIG-T, when speed is configured to 10M, multiple admin disable/enable toggles can cause port instability (including false local linkup and no traffic through port). Issue is seen with repeated consecutive local admin disable/enable toggles. Issue is not seen with 1G and 100M speed configurations.	There is no known workaround at this time.
CRAOS8X-36440	OS6570M-U28 port 25 with SFP-10G-T transceiver may see a local only linkup or a LED up with link down when peer side is admin toggled repeatedly.	There is no known workaround at this time.
CRAOS8X-36589	SFP-100-BX-U/D Source Photonics_SPL-35(53)-03-EBX-IDFM-A2 may have a linkup without cable on some random ports. Port number and number of ports displaying issue appear to vary by switch (ranging from none up to two ports).	Normal operation is expected when cable is inserted.
CRAOS8X-41611	On an OS99-CNI-U8 with 4x25G DAC link sometimes does not come up for certain lanes.	Use the QSFP-100G-SR4 fiber transceiver with 4X25G capability.
CRAOS8X-46185	Fiber ports with SFP-GIG-T connected to peer at 10M speed is operational as expected. However, when the peer link changes from 10M to 100M or 1G speed, user may (intermittently) see link down with peer side link up.	On OS6570M-U28 a hot-swap of the SFP-GIG-T recovers the port. On OS6570M-12/12D a switch reload may be required to recover port.

CRAOS8X-46195	VFL links using 4X25G splitters require additional configuration to prevent CRC errors being seen on the link.	The preferred method is configuring inter-frame-gap to 13 on both sides of the link. An alternate method is configuring FEC to FC and autonegotiation disable on both sides of the link. Note: Configuring FEC and disabling auto-negotiation will cause link to reset.
CRAOS8X-49127	An issue of slow increment of CRC errors has been observed for random packets with the SFP-GIG-T transceivers on OS6870-P24Z/P48Z 25G ports and OS6870-LNI-U6 50G ports.	There is no known workaround at this time.
CRAOS8X-49465	SFP-DUAL-BX-U/D transceivers do not link up on OS6870-P24Z/P48Z/LNI-U6. They may be used on 6870-24/48/V12 ports at 1G speed.	There is no known workaround at this time.
CRAOS8X-51603	On OS6900 and OS6870 platforms, a link-up delay of approximately 5 seconds may occur when using optical, copper, or DAC transceivers. If auto-negotiation is enabled this delay may extend by a few additional seconds. Due to the system's 5-second polling interval, it is advisable to avoid removing and reinserting transceivers in rapid succession (within 5 seconds), as this may lead to unexpected behavior.	Wait for the link up to occur, the transceiver will operate as expected.
Layer 2		
CRAOS8X-41707	When configuring erp ring and verify convergence with port down/up and node down/up events, the convergence number is high for an average 10 iterations.	There is no known workaround at this time.
Layer 3		
CRAOS8X-44230	When IPMVLAN is enabled on a switch with rvlan configured on the receiver port, after a write memory flashsynchro and reload, when the ipmvlan configs are removed the slave unit still retains the routing mode on it. Now if IPMVLAN is enabled without rvlan on receiver port and the current slave becomes the master due to VC-takeover, it starts behaving like L3 mode with forward and source table getting populated when source traffic flows.	There is no known workaround at this time.

Services		
CRAOS8X-51356	The 'show ip multicast evpn' and 'show ip multicast evpn details' CLI commands show display the same output.	There is no known workaround at this time.
Virtual Chassis		
CRAOS8X-41294	After 2nd vc-takeover, sometimes sdp or sap MACs are missing from 'show mac-learning' output.	Re-send traffic for missing macs.
QoS / Security		
CRAOS8X-34758	Port violation recovery takes additional 5 secondss sometimes.	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.The issue is only specific to the first 8 ports.	Toggle the MACsec admin state on the port.
CRAOS8X-41038	When configuring static MACsec without encryption and keys are mismatched, the traffic can still go through. Works as expected with encryption enabled.	There is no known workaround at this time.
CRAOS8X-52283	Compared to previous releases, there can be a behavior change for CLI 'policy mac group alaPhones <>' on CMM2 NI cards of OS9912 where traffic of MAC addresses that are part of the policy mac group alaPhones are not trusted for ingress 802.1p priority as per its default behavior.	Applying the CLI command 'qos apply' resolves the issue.
CRAOS8X-52698	With double tag lookup feature enabled, LPS and Static MAC configuration are not supported on SVLAN in the current release.	There is no known workaround at this time.
CRAOS8X-52811	When a Stellar AP acts as an 802.1x client to a switch port and MACsec is enabled on that switch port; then the MACsec link does not work and the AP remains disconnected.	Reboot the AP after enabling MACsec on the switch port.



## **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.
- 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	All modules can be inserted
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 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**

Existing Expansion Slot	Hot-Swap/Hot-Insert compatibility
Empty	All modules can be inserted
OS6870-LNI-U6	OS6870-LNI-U6
OS6870-CNI-U2	OS6870-CNI-U2

**OS6870 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-V72 must be replaced with an OS6900-V72).
- Replacing an element with a different model element requires a VC reboot.

### **Fast/Perpetual PoE Unlike Power Supply Swapping**

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

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

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

## Technical Support

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

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

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

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

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

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

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

## Third Party Licenses and Notices

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

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

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

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

The Alcatel-Lucent name and logo are trademarks of Nokia used under license by ALE. To view other trademarks used by affiliated companies of ALE Holding, visit: [www.al-enterprise.com/en/legal/trademarks-copyright](http://www.al-enterprise.com/en/legal/trademarks-copyright). All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Neither ALE Holding nor any of its affiliates assumes any responsibility for inaccuracies contained herein. © Copyright 2024 ALE International, ALE USA Inc. All rights reserved in all countries.

**Appendix A: Feature Matrix**

The following is a feature matrix for AOS Release 8.10R3.

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	6870	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
<b>Management Features</b>											
AAA IPv6 Address Support	8.10R3	8.10R3	8.10R3	8.10R3	8.10R3	8.10R3	8.10R3	8.10R3	8.10R3	8.10R3	8.10R3
AOS Micro Services (AMS)	8.7R2	8.6R1	8.6R1	8.9R2	8.6R1	8.7R1	8.6R1	8.10R2	8.6R1	8.7R1	8.6R1
Automatic Remote Configuration Download (RCL)	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.6R2	8.7R1	Y
Automatic/Intelligent Fabric	8.7R2	8.5R1	Y	8.9R2	Y	8.7R2	Y	8.10R2	Y	Y	Y
Automatic VC	8.7R2	N	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.6R2	8.7R1	N
Bluetooth - USB Adapter with Bluetooth Technology	8.7R2	8.6R2	8.6R2	8.9R2	Y	8.7R1	8.6R2	8.10R2	8.6R2	N	N
Certify On Reboot	8.10R2	8.10R2	8.10R2	8.10R2	8.10R2	N	8.10R2	8.10R2	N	N	N
Console Disable	8.7R2	8.6R2	8.6R2	8.9R2	8.6R2	8.7R1	8.6R2	8.10R2	8.6R2	8.7R1	8.6R2
Dying Gasp	8.9R3	Y	Y	8.9R3	Y	8.7R1	Y	8.10R2	N	N	N
Dying Gasp (EFM OAM / Link OAM)	N	8.6R1	8.6R1	8.9R3	8.6R1	8.7R1	8.6R1	8.10R2	N	N	N
EEE support	Y	8.9R1	8.9R1	8.9R2	Y	8.7R1	Y	8.10R3	Y	Y	Y
Embedded Python Scripting / Event Manager	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.7R2	8.7R2	Y
IP Managed Services	N	N	N	N	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Hitless Security Patch Upgrade	8.7R2	8.7R1	8.7R1	8.9R2	8.7R1	8.7R1	8.7R1	8.10R2	8.7R1	8.7R1	8.7R1
IPv4 In-Band Management over SPB	N	N	N	N	8.5R4	8.7R1	8.5R4	8.10R2	8.5R4	8.7R1	8.5R4
IPv6 In-Band Management over SPB	N	N	N	N	8.10R3	8.10R3	8.10R3	8.10R3	8.10R3	8.10R3	8.10R3
ISSU	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Lightning Configuration	8.9R4	8.10R3	8.10R3	8.10R3	8.10R3	8.10R3	8.10R3	8.10R3	8.10R3	8.10R3	N
NaaS	8.8R1	8.8R1	8.8R1	8.9R2	8.8R1	8.8R1	8.8R1	8.10R2	8.8R1	8.8R1	8.8R1
NAPALM Support	8.7R2	8.5R1	8.5R1	8.9R2	8.5R1	8.7R1	8.5R1	8.10R3	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	8.10R2	8.5R4	8.7R1	8.5R4
NTP - IPv6	8.7R3	8.7R3	8.7R3	8.9R2	8.7R3	8.7R3	8.7R3	8.10R2	8.7R3	8.7R3	8.7R3

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6870	6900-V72/C32	6900-X48C6/ T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
OpenFlow	N	N	N	N	Y	N	N	N	N	N	N
OV Cirrus - Zero touch provisioning	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	8.10R3	8.7R2	8.7R2	N
OV Cirrus - Configurable NAS Address	8.7R2	8.5R4	8.5R4	8.9R2	8.5R4	8.7R1	8.5R4	8.10R3	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	8.10R3	8.5R4	8.7R1	8.5R4
OV Cirrus - Managed	8.7R2	8.5R4	8.5R4	8.9R2	8.5R4	8.7R1	8.5R4	8.10R3	8.5R4	8.7R1	8.5R4
OVSDDB	N	N	N	N	N	N	N	N	N	N	N
Package Manager	8.7R2	8.6R2	8.6R2	8.9R2	8.6R2	8.7R1	8.6R2	8.10R2	8.6R2	8.7R1	8.6R2
Profinet	N	8.10R3	N	N	N	N	N	N	N	N	N
Readable Event Log	8.7R2	8.6R1	8.6R1	8.9R2	8.6R1	8.7R1	8.6R1	8.10R2	8.6R1	8.7R1	8.6R1
Remote Chassis Detection (RCD)	N	N	N	N	8.6R2	8.7R1	N	8.10R2	N	8.7R1	Y
Reset to Factory Default	8.10R3	8.10R3	8.10R3	8.10R3	8.10R3	8.10R3	8.10R3	8.10R3	8.10R3	8.10R3	
SAA	8.7R2	8.5R1	8.9R1 Metro	8.9R2	Y	8.7R2	Y	8.10R2	8.7R1	8.7R1	Y
SAA SPB	N	N	N	N	Y	8.7R2	Y	8.10R2	8.7R1	8.7R1	8.6R2
SAA UNP	N	Y	N	N	Y	N	Y	N	N	N	N
Signed AOS Image	8.10R1	8.10R1	8.10R1	8.9R4	8.10R1	8.10R1	8.10R1	8.10R2	8.10R1	8.10R1	8.10R1
SNMP v1/v2/v3	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Thin Client	8.8R1	8.8R1	8.8R1	8.9R2	8.8R1	8.8R1	8.8R1	8.10R3	8.8R1	8.8R1	8.8R1
U-boot Enable/Disable/Authenticate	8.7R3	8.7R3	8.7R3	8.9R2	8.7R3	N	8.7R3	N	N	N	8.7R3
UDLD	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	N	X48C4E	EA
USB Disaster Recovery	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1 (onie)	Y	8.10R2 (onie)	8.7R1 (onie)	8.7R1 (onie)	Y
USB Flash (AOS)	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	N	N	N
Virtual Chassis (VC)	8.7R2	8.5R2	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y (9907) N (9912)
Virtual Chassis Split Protection (VCSP)	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
VRF	N	N	N	8.9R4	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
VRF - IPv6	N	N	N	8.9R4	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
VRF - DHCP Client	N	N	N	8.9R4	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6870	6900-V72/C32	6900-X48C6/ T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
Web Services & CLI Scripting	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.7R1	8.7R1	Y
Layer 3 Feature Support											
ARP	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
BFD	N	N	N	N	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
BGP/MP-BGP	N	N	N	8.10R2 <sup>6</sup>	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
DHCP Client / Server	8.7R2	8.6R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R4	8.7R1	Y
DHCP Relay	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R4	8.7R1	Y
DHCPv6 Server	N	N	N	N	Y	8.7R1	Y	8.10R2	8.7R1	8.7R1	Y
DHCPv6 Relay	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.7R1	8.7R1	Y
DHCP Snooping / IP Source Filtering	8.7R2	8.5R4	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.6R2	8.7R1	Y
ECMP	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
IGMP v1/v2/v3	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
GRE Tunneling	N	N	N	8.9R4 <sup>6</sup>	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	8.5R2
IP-IP Tunneling	N	N	N	8.9R4 <sup>6</sup>	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	8.5R2
IPv6	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
IPv6 - DHCPv6 Snooping	8.7R2	8.6R1	8.6R1	8.9R2	8.5R3	8.7R1	8.5R4	8.10R2	8.6R2	8.7R1	8.7R1
IPv6 - Source filtering	8.7R2	N	8.6R1	8.9R2	8.5R3	8.7R1	8.5R4	8.10R2	8.6R2	8.7R1	8.7R1
IPv6 - DHCP Guard	EA	EA	EA	8.9R2	EA	N	EA	8.10R2	N	N	N
IPv6 - DHCP Client Guard	EA	EA	EA	8.9R2	EA	N	EA	8.10R2	N	N	N
IPv6 - RA Guard (RA filter)	Y	Y	8.5R2	8.9R2	Y	8.7R1	Y	8.10R2	Y	Y	Y
IPv6 - DHCP relay and Neighbor discovery proxy	8.7R2	8.5R1	Y	N	Y	8.7R1	Y	8.10R2	N	N	Y
IP Multinetting	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
IPSec	N	N	N	N	Y	8.7R1	Y	8.10R2	Y	Y	N
ISIS IPv4/IPv6	N	N	N	8.9R4 <sup>6</sup>	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	8.5R2



Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6870	6900-V72/C32	6900-X48C6/ T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
M-ISIS	N	N	N	N	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	8.5R2
OSPFv2	N	N	8.9R4 <sup>1</sup>	8.9R4 <sup>6</sup>	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
OSPFv3	N	N	8.9R4 <sup>1</sup>	8.9R4 <sup>6</sup>	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
RIP v1/v2	N	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
RIPv2 RFC-4822	N	8.10R3	8.10R3	8.10R3	8.10R3	8.10R3	8.10R3	8.10R3	8.10R3	8.10R3	8.10R3
RIPng	N	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
UDP Relay (IPv4)	8.7R2	8.5R4	8.5R4	8.9R2	Y	8.7R1	Y	8.10R2	8.5R4	8.7R1	8.5R4
UDP Relay (IPv6)	8.7R2	8.6R1	8.6R1	8.9R2	8.6R1	8.7R1	8.6R	8.10R2	8.6R1	8.7R1	8.6R1
VRRP v2	8.7R2	8.5R2	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
VRRP v3	8.7R2	8.5R2	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Server Load Balancing (SLB)	N	N	N	N	Y	8.9R4	Y	8.10R3	8.9R4	8.9R4	N
Static routing	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
<b>Multicast Features</b>											
DVMRP	N	N	N	N	Y	8.7R1	Y	N	8.5R2	8.7R1	N
IP Multicast VLAN (IPMVLAN)	N	8.9R3	8.9R3 Metro	8.9R3	N	N	N	8.10R2	N	N	N
IPv4 Multicast Switching	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Multicast *,G	8.7R2	Y	8.5R2	8.9R2	8.5R2	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
IPv6 Multicast Switching	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
PIM-DM	N	N	8.10R1 <sup>6</sup>	8.9R4 <sup>6</sup>	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
PIM-SM	N	N	8.10R1 <sup>6</sup>	8.9R4 <sup>6</sup>	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
PIM-SSM	N	N	8.10R1 <sup>6</sup>	8.9R4 <sup>6</sup>	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
PIM-SSM Static Map	N	N	N	N	N	N	N	N	N	N	N
PIM-BiDir	N	N	8.10R1 <sup>6</sup>	8.9R4 <sup>6</sup>	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
PIM Message Packing	N	N	8.10R1 <sup>6</sup>	8.9R4 <sup>6</sup>	8.6R1	8.7R1	N	8.10R2	8.6R1	8.7R1	N

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6870	6900-V72/C32	6900-X48C6/ T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
PIM - Anycast RP	N	N	8.10R1 <sup>6</sup>	8.9R4 <sup>6</sup>	8.6R2	8.7R1	8.6R2	8.10R2	8.6R2	8.7R1	8.6R2
Monitoring/Troubleshooting Features											
Ping and traceroute	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Policy based mirroring	N	N	N	N	Y	8.7R1	Y	8.10R2	8.7R1	8.7R1	8.5R4
Port mirroring	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Port monitoring	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Port mirroring - remote	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.7R2	8.7R2	8.6R1
Port mirroring - remote over linkagg	N	N	8.9R3	N	Y	8.7R1	Y	8.10R2	8.7R2	8.7R2	8.6R1
RMON	8.7R2	8.5R1	Y	8.9R2	Y	8.8R2	Y	8.10R2	8.8R2	8.8R2	N
SFlow	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.7R1	8.7R1	Y
Switch logging / Syslog	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
TDR	8.9R3	8.9R3	8.9R3	N	Y	8.9R3	Y	8.10R3	N	N	N
Layer 2 Feature Support											
802.1q	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
DHL	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	N	Y	N
ERP v2	8.9R3	8.5R1	8.5R2	8.9R2	Y	8.7R1	Y	8.10R2	8.7R1	8.7R1	8.5R3
HAVLAN	N	EA	N	N	Y	8.8R1	Y	8.10R2	8.6R2	8.7R1	EA
Link Aggregation (static and LACP)	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
LLDP (802.1ab)	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Loopback detection - Edge (Bridge)	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.6R2	8.7R1	Y
Loopback detection - SAP (Access)	N	N	N	N	Y	8.7R1	Y	8.10R2	8.6R2	8.7R1	Y
MAC Forced Forwarding / Dynamic Proxy ARP	8.7R2	8.7R1	N	8.9R2	8.6R1	N	8.6R1	8.10R2	N	N	N
MPLS - VPLS	N	N	N	N	N	8.9R3	N	N	N	8.10R2	N
MPLS - VPWS	N	N	N	N	N	8.10R2	N	N	N	8.10R2	N

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6870	6900-V72/C32	6900-X48C6/ T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
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	8.10R2	8.5R2	8.7R1	N
Private VLANs (PVLAN)	N	N	8.10R3	N	Y	8.7R2	Y	8.10R2	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	8.10R2	8.5R2	8.7R1	Y
Spanning Tree (PVST+, Loop Guard)	N	Y	Y	8.9R2	Y	Y	Y	8.10R2	Y	Y	Y
MVRP	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R4	8.7R1	Y
SPB <sup>2</sup>	N	N	N	N	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
SPB - Over Shared Ethernet	N	N	N	N	8.7R1	8.7R1	8.7R1	8.10R2	8.7R1	8.7R1	8.7R1
SPB - HW-based LSP flooding	N	N	N	N	8.6R1	N	8.6R1	8.10R2	N	N	8.5R4
QoS Feature Support											
802.1p / DSCP priority mapping	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
IPv4	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
IPv6	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Auto-Qos prioritization of NMS/IP Phone Traffic	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Auto-Qos - New MAC range	8.7R2	8.5R2	8.5R2	8.9R2	8.5R2	8.7R1	8.5R2	8.10R2	8.5R2	8.7R1	8.5R2
Groups - Port	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Groups - MAC	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Groups - Network	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Groups - Service	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Groups - Map	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Groups - Switch	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Groups - VLAN	8.10R1	8.10R1	8.10R1	8.10R1	8.10R1	8.10R1	8.10R1	8.10R2	8.10R1	8.10R1	8.10R1
Ingress/Egress bandwidth limit	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Per port rate limiting	N	N	N	N	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	N
Policy Lists	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.7R1	8.7R1	Y

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6870	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
Policy Lists - Egress	N	N	N	N	Y	8.7R1	Y	8.10R2	8.7R1	8.7R1	N
Policy based routing	N	N	Y	8.9R4	Y	8.7R1	Y	8.10R2	8.6R2	8.7R1	8.9R4
Tri-color marking	N	N	N	N	Y	8.7R1	Y	8.10R2	N	N	N
QSP Profiles 1	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
QSP Profiles 2/3/4	N	N	N	QSP-2 Only	Y	QSP-2 only	Y	QSP-2 only	QSP-2 only	QSP-2 only	N
QSP Profiles 5	8.7R2	8.5R1	Y	Same as QSP-2	8.7R1	Same as QSP-2	8.7R1	Same as QSP-2	Same as QSP-2	Same as QSP-2	Y
RoCEv2	N	N	N	N	N	N	N	N	8.7R2	8.10R3 (EA)	N
Custom QSP Profiles	8.7R2	Y	Y	8.9R2	Y	Y	Y	8.10R2	Y	Y	Y
GOOSE Messaging Prioritization	N	8.7R1	N	N	N	N	8.7R1	N	N	N	N
Services Support	N	N	N	N	N	Y	N	Y	Y	Y	Y
<b>Metro Ethernet Features</b>											
CPE Test Head	N	8.6R1	8.9R1 Metro	8.9R2	N	N	N	8.10R3 (EA)	N	N	N
Ethernet Loopback Test	N	Y	8.9R1 Metro	8.9R2	8.6R1	N	8.6R1	8.10R3	N	N	N
Ethernet Services (VLAN Stacking)	N	8.5R1	8.9R1 Metro	8.9R2	Y	8.7R2	Y	8.10R2	8.5R4	8.7R1	N
Ethernet OAM (ITU Y1731 and 802.1ag)	N	8.5R1	8.9R1 Metro	8.9R2	Y	8.7R1	Y	8.10R2	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	8.10R2	N	N	N
Transparent Bridging	N	N	N	N	Y	Y	Y	8.10R2	Y	Y	N
PPPoE Intermediate Agent	N	8.6R1	8.9R1 Metro	8.9R2	N	N	8.6R1	N	N	N	N
Precision Time Protocol (PTP 1588v2) End-to-End Transparent Clock	N	8.5R1	8.7R2	8.10R3	Y	8.9R3	Y	8.10R2	N	8.9R3 (except C32E)	N
Precision Time Protocol (PTP 1588v2) Peer-to-Peer Transparent Clock	N	8.8R2	8.7R2	8.10R3	N	N	N	N	N	N	N
Precision Time Protocol (PTP 1588v2) Across VC	N	N	N	N	N	N	N	N	N	N	N
<b>Access Guardian / Security Features</b>											
802.1x Authentication	8.7R2	8.5R2	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.7R1	8.7R1	Y

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6870	6900-V72/C32	6900-X48C6/ T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
Access Guardian - Bridge	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.6R1	8.7R1	Y
Access Guardian - Access	N	N	N	N	Y	8.7R1	Y	8.10R2	8.5R4	8.7R1	Y
Application Fingerprinting	N	N	N	N	N	N	N	N	N	N	N
Application Monitoring and Enforcement (Appmon / DPI)	N	N	N	N	Y	8.7R2	N	8.10R2 <sup>7</sup> (EA)	N	N	N
ARP Poisoning Protection	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
BYOD - COA Extension support for RADIUS	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.6R2	8.7R1	Y
BYOD - mDNS Snooping/Relay	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	8.10R3	8.6R2	8.7R1	Y
BYOD - UPNP/DLNA Relay	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	8.10R3	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	8.10R2	8.6R2	8.7R1	Y
Captive Portal	8.7R2	8.5R4	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.6R2	8.7R1	Y
IoT Device Profiling	8.7R2	8.5R2	8.5R2	8.9R2	8.5R2	8.7R1	8.5R2	8.10R3	8.6R1	8.7R1	8.5R2
IoT Device Profiling (IPv6)	8.7R2	8.7R1	8.7R1	8.9R2	8.7R1 <sup>5</sup>	8.9R3	8.7R1 <sup>5</sup>	8.10R3	8.9R3	8.9R3	8.7R1
Directed Broadcasts - Control	8.7R2	8.5R2	8.5R2	8.9R2	8.5R2	8.7R1	8.5R2	8.10R2	8.7R1	8.7R1	Y
Interface Violation Recovery	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.7R1	8.7R1	Y
Kerberos Snooping	8.7R2	Y	8.6R2	N	8.6R2	Y	8.6R2	8.10R2	8.6R2	Y	8.6R2
L2 GRE Tunnel Access (Edge) (bridge ports)	N	N	Y	N	Y	8.9R1	Y	8.10R2	N	N	Y
L2 GRE Tunnel Access (Edge) (access ports)	N	N	N	N	8.6R1	8.9R1	8.6R1	8.10R2	8.7R1	8.7R2	8.6R1
L2 GRE Tunnel Aggregation	N	N	N	N	Y	8.9R1	Y	8.10R2	8.7R1	8.7R2	Y
Learned Port Security (LPS)	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R4	8.7R1	Y
MACsec <sup>3</sup>	N	8.5R1	8.5R4	8.10R2	Y	8.7R1	N	8.10R2	N	X48C4E	8.5R2
MACsec on Network Port for SPB/L2GRE/VxLAN	N	N	N	N	8.9R1 (6860E)	8.9R1	N	8.10R2	N	8.9R1 (X48C4E)	N
Quarantine Manager	N	8.7R2	8.7R2	8.9R2	Y	8.7R2	Y	8.10R2	8.7R2	8.7R2	8.7R2
RADIUS - RFC-2868 Support	8.7R2	8.5R4	8.5R4	8.9R2	8.5R4	8.7R1	8.5R4	8.10R2	8.5R4	8.7R1	8.5R4
Role-based Authentication for Routed Domains	N	N	N	N	8.5R4	8.7R1	8.5R4	8.10R2	8.6R1	8.7R1	8.5R4
Storm Control (flood-limit)	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	8.10R2	Y	8.7R1	Y

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6870	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
Storm Control (Unknown unicast with action trap/shutdown)	N	N	N	N	Y	N	Y	8.10R2	N	N	N
TACACS+ Client	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.6R1	8.7R1	Y
TACACS+ command based authorization	8.7R2	N	N	8.9R2	Y	8.7R1	Y	8.10R2	8.7R2	8.7R2	N
TACACS+ - IPv6	8.7R3	8.7R3	8.7R3	8.9R2	8.7R3	8.7R3	8.7R3	8.10R2	8.7R3	8.7R3	8.7R3
PoE Features											
802.3af and 802.3at	8.7R2	8.5R1	Y	N	Y	8.7R1	Y	8.10R2	N	N	Y
802.3bt	8.7R2	Y	8.6R2	N	N	8.7R1	Y	8.10R2	N	N	N
Auto Negotiation of PoE Class-power upper limit	8.7R2	8.5R1	Y	N	Y	8.7R1	Y	8.10R2	N	N	Y
Display of detected power class	8.7R2	8.5R1	Y	N	Y	8.7R1	Y	8.10R2	N	N	Y
LLDP/802.3at power management TLV	8.7R2	8.5R1	Y	N	Y	8.7R1	Y	8.10R2	N	N	Y
HPOE support	8.7R2 (95W)	8.5R1 (60W)	Y (95W)	N	Y (60W)	8.7R1 (95W)	Y (75W)	8.10R2	N	N	Y (75W)
Time Of Day Support	8.7R2	8.5R1	Y	N	Y		Y	8.10R2	N	N	Y
Perpetual PoE	8.7R2	N	N	N	Y	Y	Y	8.10R2	N	N	N
Fast PoE	8.7R2	N	N	N	Y	Y	Y	8.10R2	N	N	N
Delayed Start	8.9R3	8.9R3	8.9R3	N	N	N	N	8.10R2	N	N	N
Data Center Features (License May Be Required)											
CEE DCBX Version 1.01	N	N	N	N	N	N	N	N	N	N	N
Data Center Bridging (DCBX/ETS/PFC)	N	N	N	N	N	N	N	N	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	N	N	N	N
VxLAN <sup>4</sup>	N	N	N	N	N	8.8R1	N	8.10R2	8.5R3	8.8R1	N
EVPN VxLAN	N	N	N	N	N	N	N	N	N	8.10R1	N
EVPN - Route Redistribution for Prefix Route Advertisement for Symmetric IRB	N	N	N	N	N	N	N	N	N	8.10R3	N
EVPN - BGP NBR Template and Scalability	N	N	N	N	N	N	N	N	N	8.10R3	N
EVPN - VRF-based Tenancy Model for AOS EVPN Services	N	N	N	N	N	N	N	N	N	8.10R3	N
EVPN - Multicast Routing Over an EVPN Fabric (RFC 9625) - OISM & PIM Support	N	N	N	N	N	N	N	N	N	8.10R3 (EA)	N
VM/VxLAN Snooping	N	N	N	N	N	N	N	N	N	N	N

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6870	6900- V72/ C32	6900- X48C6/ T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
FIP Snooping	N	N	N	N	N	N	N	N	N	N	N
Notes: 1. OS6560 supports 2 OSPF areas with Advanced Routing license. 2. See protocol support table in Appendix C. 3. Site license required beginning in 8.6R1. 4. L2 head-end only on OS6900-V72/C32. 5. HTTP IPv6 only supported on OS6860(E) and OS6865 6. Advanced Routing license required. 7. Monitoring functionality only. Enforcement is not supported.											

## Appendix B: MACsec Platform Support

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

MACsec Support (MACsec site license required)	
<b>OmniSwitch 9900</b>	
OS99-CMM	4X10G mode only - Static and Dynamic (128-bit) modes
OS99-CMM2	Ports 1-4 (40G, 100G, 4x10G, 4x25G) - Dynamic (256-bit) mode
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 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 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 10G (Copper) - Static and Dynamic (128-bit) modes
OS99-CNI-U8	Not Supported
OS99-CNI-U20	40G/100G - Static and Dynamic (256-bit) modes
<b>OmniSwitch 6900</b>	
OS6900-X48C4E	Dynamic mode only on all ports. Supports 256-bit key length.
<b>OmniSwitch 6870</b>	
OS6870-24	Dynamic (256-bit) mode Port 1-24 (10M, 100M, 1G) Port 25-26 - Not Supported Port 27-30 (10G, 25G)
OS6870-P24M	Port 1-24 (1G, 2.5G, 5G, 10G) Port: 25-26 (40G, 100G, 200G, 4X10G, 4X25G)
OS6870-P24Z	Port 1-24 (100M, 1G, 2.5G) Port: 25-26 (40G, 100G, 4x10G, 4x25G) Port 27-32 (10G, 25G)
OS6870-48	Port 1-48 (10M, 100M, 1G) Port 49-50 - Not Supported Port 51-54 (10G, 25G)
OS6870-P48M	Port 1-48 (1G, 2.5G, 5G, 10G) Port: 49-50 (40G, 100G, 200G, 4X10G, 4X25G)
OS6870-P48Z	Port 1-48 (100M, 1G, 2.5G) Port: 49-50 (40G, 100G, 4x10G, 4x25G) Port 51-56 (10G, 25G)
OS6870-V12	Port 1-12 (10G, 25G) Port: 13-14 (40G, 100G, 200G, 4X10G, 4X25G)
OS6870-CNIU2	Port 1-2 (40G, 100G, 4x10G, 4x25G)
OS6870-LNIU6	Port 1-6 (10G, 25G, 50G)
Note: The OS6870 does not support MACsec on ports in VFL mode.	
<b>OmniSwitch 6860(E)</b>	
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).



<b>OmniSwitch 6860N</b>	Dynamic mode only. All OS6860N models support 128-bit key length.
OS6860N-U28	SFP (1-24), SFP+ (25-28) and SFP28 (31-34) ports
OS6860N-P48Z	SFP28 (51-54) ports
OS6860N-P48M	- Expansion modules (Not supported on any 4X10G splitter transceivers). - Multi-rate Gigabit Ports (37-48)
OS6860N-P24Z	SFP28 (27-30) ports
OS6860N-P24M	- Expansion modules (Not supported on any 4X10G splitter transceivers) - Multi-rate Gigabit Ports (1-24)
<b>OmniSwitch 6570M</b>	Dynamic (256-bit) mode
OS6570M-12/12D	Ports 1-8 (10M/100M/1G) Ports 9-10 (1G) Ports 11-12 (1G/10G)
OS6570M-U28	Ports 1-24 (1G) Ports 25-30 (1G/10G)
<b>OmniSwitch 6560(E)</b>	
OS6560-P24X4/24X4	- Ports 1-24 (Static and Dynamic modes) - Ports 25-30 (Not Supported)
OS6560-P48X4/48X4	- Ports 1-48 (Static and Dynamic modes) - Ports 49-52 (Dynamic mode only) - Ports 53-54 (Not Supported)
OS6560-P48Z16 (904044-90 only)	- Ports 1-32 (Static and Dynamic Modes) - Ports 33-48 (Static and Dynamic modes) - Ports 49-52 (Dynamic mode only) - Ports 53-54 (Not Supported)
OS6560E-P48Z16	- Ports 1-32 (Static and Dynamic Modes) - Ports 33-48 (Static and Dynamic modes) - Ports 49-52 (Dynamic mode only) - Ports 53-54 (Not Supported)
OS6560-X10	- Ports 1-8 (10G ports only. Dynamic mode only) - Ports 9-10 (Not Supported)
<b>OmniSwitch 6465</b>	- OS6465-P28 - Supported on all ports except ports 27 and 28. - OS6465T-12 and OS6465T-P12 - Not supported on ports 11 and 12. - All other models support MACsec on all ports.

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

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

OmniSwitch Inline Routing Support								
	9900	6900- V72/C32 (Front panel port)	6900- T48C6/X48C6	6900- X48C4E/V48C8	6900-C32E	6860N	6900- X/T24C2	6870
<b>IPv4 Protocols</b>								
Static Routing	Y	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
RIP v1/v2	Y	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
OSPF	Y	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
BGP	Y	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
VRRP	Y	8.7R1	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
IS-IS	N	N	N	N	N	N	N	N
PIM-SM/DM	8.5R3	8.6R2	Y	Y	8.8R1	Y	8.9R1	8.10R2
DHCP Relay	8.5R3	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
UDP Relay	8.5R4	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
DVMRP	N	N	N	N	N	N	N	N
BFD	8.7R2	8.7R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
IGMP Snooping	Y	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
IP Multicast Headend Mode	Y	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
IP Multicast Tandem Mode	8.5R4	8.6R2	8.8R1	8.8R1	8.8R1	8.8R1	8.9R1	8.10R2
<b>IPv6 Protocols</b>								
Static Routing	8.5R4	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
RIPng	8.5R4	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
OSPFv3	8.5R4	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
BGP	8.5R4	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
VRRPv3	8.5R4	8.7R1	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
IS-IS	N	N	N	N	N	N	N	N
PIM-SM/DM	8.5R4	8.6R2	8.8R1	8.8R1	8.8R1	8.8R1	8.9R1	8.10R2
DHCP Relay	8.6R1	8.7R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
UDP Relay	8.6R1	8.7R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
BFD	8.7R2	8.7R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
IPv6 MLD Snooping	Y	8.7R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
IPv6 Multicast Headend Mode	Y	8.7R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
IPv6 Multicast Tandem Mode	8.5R4	8.7R2	8.8R1	8.8R1	8.8R1	8.8R1	8.9R1	8.10R2

External Loopback Support								
	OmniSwitch 9900	OmniSwitch 6860/6865	OmniSwitch 6860N	OmniSwitch 6900-V72/ C32	OmniSwitch 6900-X48C6/ T48C6	OmniSwitch 6900-X48C4E	OmniSwitch 6900-V48C8	OmniSwitch 6900-X/T48C2
<b>IPv4 Protocols</b>								
Static Routing	8.5R4	Y	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
RIP v1/v2	8.5R4	Y	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
OSPF	8.5R4	Y	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
BGP	8.5R4	Y	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
VRRP	8.6R1	8.5R4	8.7R1	8.7R1	8.7R2	8.7R2	8.7R3	8.9R1
IS-IS	Y	Y	Y	Y	Y	8.7R2	8.7R3	8.9R1
PIM-SM/DM	8.5R4	Y	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
DHCP Relay	8.5R4	8.5R4	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
UDP Relay	8.5R4	8.5R4	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
DVMRP	N	N	N	N	N	N	N	N
BFD	Y	Y	Y	Y	Y	8.7R2	8.7R3	8.9R1
IGMP Snooping	8.5R4	Y	8.7R1	8.6R1	8.7R1	8.7R2	8.7R3	8.9R1
IP Multicast Headend Mode	8.5R4	Y	8.7R1	8.6R1	8.7R1	8.7R2	8.7R3	8.9R1
IP Multicast Tandem Mode	8.5R4	Y	8.7R1	8.6R1	Y	Y	Y	8.9R1
<b>IPv6 Protocols</b>								
Static Routing	8.5R4	Y	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
RIPng	8.5R4	Y	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
OSPFv3	8.5R4	Y	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
BGP	8.5R4	Y	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
VRRPv3	8.5R4	8.5R4	8.7R1	8.7R1	8.7R2	8.7R2	8.7R3	8.9R1
IS-IS	Y	Y	Y	Y	Y	8.7R2	8.7R3	8.9R1
PIM-SM/DM	8.5R4	8.5R4	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
DHCP Relay	8.6R1	8.6R1	8.7R1	8.6R1	8.7R1	8.7R2	8.7R3	8.9R1
UDP Relay	8.6R1	8.6R1	8.7R1	8.6R1	8.7R1	8.7R2	8.7R3	8.9R1
BFD	Y	Y	Y	Y	Y	8.7R2	8.7R3	8.9R1
IPv6 MLD Snooping	8.5R4	Y	8.7R1	Y	8.7R2	8.7R2	8.7R3	8.9R1
IPv6 Multicast Headend Mode	8.5R4	Y	8.7R1	Y	8.7R2	8.7R2	8.7R3	8.9R1
IPv6 Multicast Tandem Mode	8.5R4	Y	8.7R1	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 BVLAN is active even if the services are not configured on the local node.

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

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

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

---

## **Appendix D: General Upgrade Requirements and Best Practices**

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

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

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

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

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

**Supported Upgrade Paths and Procedures**

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

Platform	AOS Releases Supporting ISSU to 8.10R3 (GA)
OS6360	8.10.105.R02 (GA) 8.10.115.R01 (MR) 8.10.102.R01 (GA) 8.9.130.R04 (MR) 8.9.94.R04 (GA)
OS6465	8.10.105.R02 (GA) 8.10.115.R01 (MR) 8.10.102.R01 (GA) 8.9.130.R04 (MR) 8.9.94.R04 (GA)
OS6560	8.10.105.R02 (GA) 8.10.115.R01 (MR) 8.10.102.R01 (GA) 8.9.130.R04 (MR) 8.9.94.R04 (GA)
OS6560E	8.10.105.R02 (GA) 8.10.115.R01 (MR) 8.10.102.R01 (GA)
OS6570M	8.10.105.R02 (GA) 8.10.115.R01 (MR) 8.10.102.R01 (GA) 8.9.130.R04 (MR) 8.9.94.R04 (GA)
OS6860(E)	8.10.105.R02 (GA) 8.10.115.R01 (MR) 8.10.102.R01 (GA) 8.9.130.R04 (MR) 8.9.94.R04 (GA) 8.9.92.R04 (GA)
OS6860N	8.10.105.R02 (GA) 8.10.115.R01 (MR) 8.10.102.R01 (GA) 8.9.130.R04 (MR) 8.9.94.R04 (GA) 8.9.92.R04 (GA)
OS6865	8.10.105.R02 (GA) 8.10.115.R01 (MR) 8.10.102.R01 (GA) 8.9.130.R04 (MR) 8.9.94.R04 (GA) 8.9.92.R04 (GA)

OS6870	8.10.105.R02 (GA)
OS6900-V72/C32/C32E X48C6/T48C6/V48C8/ X24C2/T24C2/X48C4E	8.10.105.R02 (GA) 8.10.115.R01 (MR) 8.10.102.R01 (GA) 8.9.130.R04 (MR) 8.9.94.R04 (GA) 8.9.92.R04 (GA)
OS9900	8.10.106.R02 (GA) 8.10.102.R01 (GA) 8.9.130.R04 (MR) 8.9.94.R04 (GA)
<ul style="list-style-type: none"> <li>ISSU from 8.9.92.R04 is not supported on platforms: OS6360, OS6465, OS6560, OS6570M, OS9900 (due to SSH issue on build 8.9.92.R04)</li> </ul>	

### 8.10R3 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.

```
OS6860-> show system
System:
Description: Alcatel-Lucent OS6860-P24 8.9.94.R04 GA, March 28, 2024.,
Object ID: 1.3.6.1.4.1.6486.801.1.1.2.11.1.2,
Up Time: 88 days 2 hours 1 minutes and 44 seconds,
Contact: Alcatel-Lucent, https://www.al-enterprise.com,
Name: OS6860,
Location: Unknown,
Services: 78,
Date & Time: FRI OCT 11 2024 06:55:43 (PDT)
Flash Space:
Primary CMM:
Available (bytes): 1084694528,
Comments : None
```

2. Remove any old tech\_support.log files, tech\_support\_eng.tar files:

```
OS6860-> rm *.log
OS6860-> 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:

```
OS6860-> 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'**:

```
OS6860-> 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:

```
OS6860-> show tech-support  
OS6860-> show tech-support layer2  
OS6860-> 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.

```
OS6860-> 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 - 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.

```
OS6860-> 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.

```
OS6860-> show microcode
/flash/working
Package           Release           Size      Description
-----+-----+-----+-----
Uos.img           8.10.93.R03      239607692 Alcatel-Lucent OS

OS6860-> 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.

```
OS6860-> 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 - 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:

```
OS6860-> 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:

```
OS6860-> debug show virtual-chassis connection
```

Chas	MAC-Address	Address		Status
		Local IP	Remote IP	
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':

```
OS6860-> 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:

```
OS6860-> rm -r /flash/issu_dir
```

6. Log out of the Slave chassis:

```
OS6860-> exit
logout
Connection to 127.10.2.65 closed.
```

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

```
OS6860-> 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:

```
OS6860-> ls /flash/issu_dir
Uos.img      issu_version  vcboot.cfg   vcsetup.cfg
```

9. Upgrade the image files using ISSU:

```
OS6860-> 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)

```
OS6860-> show issu status
Issu pending
```

This indicates that the ISSU is completed

```
OS6860-> 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.

```
OS6860-> debug show virtual-chassis topology
Local Chassis: 1
Oper
Chas  Role      Status      Chas ID  Pri   Oper  MAC-Address      System
-----+-----+-----+-----+-----+-----+-----+-----
1      Master    Running      1        100   19    e8:e7:32:b9:19:0b  Yes
2      Slave     Running      2         99   19    e8:e7:32:b9:19:43  Yes
```

## 10. Verify the Software Upgrade

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

```
OS6860-> show microcode
/flash/working
Package      Release      Size      Description
-----+-----+-----+-----
Uos.img      8.10.93.R03  239607692 Alcatel-Lucent OS
```

## 11. Certify the Software Upgrade

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

```
OS6860-> write memory flash-synchro

OS6860-> 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
```

## 12. [Optional] Restore the *Running Configuration*

After completing the ISSU procedure the *Running Configuration* can be restored by setting it back to the directory used prior to the ISSU procedure. For example to change the *Running Configuration* back to the **working** directory enter the following:

```
OS6860-> copy certified working make-running-directory
```

## 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	
	Description	Summary
CRAOS8X-12042	Description	Switch does not shutdown after crossing danger threshold temperature.
	FPGA Version	0.7
	Platforms	OS6465-P28
CRAOS8X-7207	Description	Chassis reboots twice to join a VC.
	FPGA Version	0.7
	Platforms	OS6560-P24Z24,P24Z8,P48Z16 (903954-90)
CRAOS8X-4150	Description	VC LED status behavior.
	U-boot Version	0.12
	Platforms	OS6865-U28X
8.7R1 Release		
CRAOS8X-16452	Description	Port remains UP when only SFP is connected.
	FPGA Version	- 0.6 (OS6560-P48Z16 (904044-90)) - 0.7 (OS6560-48X4, OS6560-P48X4) - 0.8 (OS6560-X10)
	Platforms	OS6560-P48Z16 (904044-90), OS6560-48X4, OS6560-P48X4, OS6560-X10
Fast/Perpetual PoE	Description	Fast and Perpetual PoE Support
	FPGA Version	0.7 (OS6860E-P24Z8) 0.10 0.14 (OS6865-U28X) 0.25 (OS6865-P16X/U12X)
	Platforms	OS6860/OS6865
8.7R2 Release		
CRAOS8X-4813/13440	Description	U-boot 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	U-boot unable to mount eUSB flash
	U-boot Version	8.7.2.R02
	Platforms	OS6560-24Z24/P24Z24/24Z8/P24Z8/P48Z16 (all PNs), 6865
CRAOS8X-22857	Description	OS6560-P24Z24 reloads continuously with pmds
	FPGA Version	0.8
	Platforms	OS6560-24Z24/P24Z24/24Z8/P24Z8/P48Z16 (903954-90)
1588v2 Support	Description	1588v2 Support
	FPGA Version	0.7 (OS6560-P48Z16 (904044-90)) 0.8 (OS6560-48X4/P48X4)
	Platforms	OS6560-48X4/P48X4/P48Z16(904044-90) 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 CRAOS8X-25033	Description	Required upgrade to enable 12V Power Fail Interrupt (CRAOS8X-26370). Required upgrade to address fan speed issue. (CRAOS8X-25033)
	FPGA Version	0.17
	Platforms	OS6360-24/P24/48/P48
CRAOS8X-24464	Description	U-boot update for CRAOS8X-24464, ability to disable / authenticate U-boot access.
	U-boot Version	8.7.30.R03
	Platforms	OS6360, 6465, 6560, 6860, 6865, 9900. (Not applicable for platforms that use ONIE)
8.8R1 Release		
Boot from USB	Description	U-boot update to allow switch to boot from USB.
	U-boot Version	8.8.33.R01
	Platforms	OS6465, OS6865
8.8R2 Release		
Future compatibility	Description	U-boot/FPGA update to allow future CMM2/OS9912 NI compatibility.
	U-boot/FPGA Versions	See <a href="#">OS9900 Table</a> for versions.
	Platforms	9907
8.9R1 Release		
N/A	There are no U-boot/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	U-boot fix for NAND flash bad file system block. Support of Gowin CPLD <sup>1</sup>
	U-boot	8.9.85.R02
	Platforms	OS6360 (All)
CPLD Support	Description	Support of Gowin CPLD <sup>1</sup>
	U-boot	8.9.92.R02
	Platforms	OS6570M-12/12D/U28
CRAOS8X_35470	Description	U-boot fix for NAND flash bad file system block
	U-boot/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 U-boot access.
	U-boot 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.
	U-boot Version	8.9.70.R04
	Platforms	OS6570M-12/12D/U28
8.10R1 Release		
CRAOS8X-43592	Description	1G/10G SFP not recognized.
	U-boot Version	XNI_U24 - 2.12.0 XNI_U48 - 2.12.0 GNI_U48 - 1.8.0 CNI_U8 - 1.10
	Platforms	OS9907/OS9912
8.10R2 Release		
CRAOS8X-44063	Description	Switches stuck in Marvel mode during bootup.
	U-boot Version	8.10.42.R02
	Platforms	6360, 6465, OS6560-24X4/P24X4/48X4/P48X4/X10
CRAOS8X-44607	Description	Switch stuck in Marvel mode after power cycle.
	U-boot Version	8.10.42.R02
	Platforms	6360, 6465, 6560, 6570M, 6860(E), 6865
CRAOS8X-46275	Description	Switch stuck in Marvel mode after power cycle.
	U-boot Version	8.10.42.R02
	Platforms	6360, 6465, OS6560-24Z8/P24Z8(E)/24Z24/P24Z24/P48Z16(E), 6570M, 6860(E), 6865
<b>Note:</b> The CRs above were also fixed with U-boot version 8.10.115.R01 in the 8.10R1 maintenance release. Switches running 8.10.115.R01 do not need to upgrade to 8.10.42.R02.		
8.10R3 Release		
There are no FPGA or U-boot upgrades required.		

**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\_9022
- u-boot.8.10.R02.114.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_9022
Parse /flash/fpga_kit_9022
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.8.10.R02.114.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		
<b>OS6860N-P48M/P48Z/P24M/P24Z</b>		
CRAOS8X-29731/30471	Description	OS6860N power supplies
	CPLD File	os6860n_p48m_p48z_u28_maincpu_20220318.updater os6860n_p24m_p24z_maincpld_22020309.updater
8.9R1 Release		
<b>OS6900-T48C6</b>		
CRAOS8X-30098	Description	Fixed I2C lockup issue on CPU board. (Please refer to CRAOS8X-30098 for additional details)
	CPLD File	denverton_cpucpld_v0b.02.0eh_20211124.jbc.updater
No CR	Description	Improved power down sequence when PSU shut down.
	CPLD File	os6900_t48c6_mainpld_v1.03.02.04.jbc.updater
<b>OS6900-X48C6</b>		
CRAOS8X-30098	Description	Fixed I2C lockup issue on CPU board. (Please refer to CRAOS8X-30098 for additional details)
	CPLD File	denverton_cpucpld_v0b.02.0eh_20211124.jbc.updater
No CR	Description	Improved power down sequence when PSU shut down.
	CPLD File	os6900_x48c6_mainpldall_bp_v1.03.02.02h.jbc.updater
<b>OS6900-X48C4E</b>		
CRAOS8X-30098	Description	Fixed I2C lockup issue on CPU board. (Please refer to CRAOS8X-30098 for additional details)
	CPLD File	OS6900_XC48C4E_MAIN_CPU_FAN_CPLD_2e3228_20220322.updater
8.9R4 Release		
<b>OS6900-X48C4E</b>		
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)
<b>Notes:</b> <ol style="list-style-type: none"> <li>Upgrading the CPLD on ONIE-based models using an updater kit is supported beginning with AOS Release 8.9.R03.</li> <li>The updater kit contains all the necessary individual updater files.</li> <li>CPLD versions are compatible with previous AOS releases. Downgrading to a previous AOS release is supported: <ol style="list-style-type: none"> <li>Backup the configuration files from previous release.</li> <li>Upgrade to AOS Release 8.9.R03.</li> <li>Upgrade the CPLD.</li> <li>Downgrade to previous release. (ISSU is not supported when downgrading AOS)</li> <li>Restore the configuration.</li> </ol> </li> </ol>		

**Note:** AOS must be upgraded to at least 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
<b>Case:</b> <b>00754006</b> CRAOS8X-45809	<b>Summary:</b> OS6900-V72: "IfOutErrors" are displayed for linkagg but not for the physical interfaces.  <b>Explanation:</b> Customer notices IfOutErrors counters incrementing for linkagg. However, the same counters are not displayed for physical interfaces.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00748568</b> CRAOS8X-47795	<b>Summary:</b> OS6860N: After successful authentication, all traffic on dynamic SAP port is dropped.  <b>Explanation:</b> OS6860N: Users connected on UNP SAP ports authenticate successfully. After successful authentication, all traffic is dropped.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00766139</b> CRAOS8X-48476	<b>Summary:</b> OS6570M-12D: Issue with throughput limitation.  <b>Explanation:</b> Issue with Throughput Limitation on OS6570M-12D Switches Running on AOS release 8.10.102.R02.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00782818</b> CRAOS8X-49242	<b>Summary:</b> OS6900X48C8: GRE Tunnel packets of size less than 76 bytes are dropped on VFL link.  <b>Explanation:</b> OS6900X48C8: Packets of size less than 64 bytes received via GRE Tunnel dropped on VFL link.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00793613</b> CRAOS8X-50217	<b>Summary:</b> Switch is not updating it's ARP table after a Gratuitous ARP is sent.  <b>Explanation:</b> After an upgrade from 8.9R04 to 8.10R01 it was noticed that the switch is not updating it's ARP table after a Gratuitous ARP is sent.   <a href="#">Click for Additional Information</a>





<b>Case:</b> <b>00788588</b> CRAOS8X-49791	<b>Summary:</b> Issue with CLI command display for proxy-ARP configuration in EVPN Nodes.  <b>Explanation:</b> Anomaly in the execution and display of CLI commands related to the proxy-arp flood-unknown-unicast-supression configuration in EVPN-enabled network devices.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00792251</b> CRAOS8X-50120	<b>Summary:</b> OS6900: For IPv6 BGP sessions, the BFD control packets are transmitted with a Hop Limit value of 64 for single-hop connections.  <b>Explanation:</b> For IPv6 BGP sessions, the BFD control packets are transmitted with a Hop Limit value of 64 for single-hop connections. This behavior is non-compliant with RFC 5881, which mandates that BFD control packets must use a TTL or Hop Limit of 255 in such scenarios.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00795501</b> CRAOS8X-50643	<b>Summary:</b> OS6360-P10A: When ipv6 ra-filter is applied, DHCPv6 server response packets are no longer forwarded to the client.  <b>Explanation:</b> When ipv6 ra-filter is applied, DHCPv6 server responses are no longer forwarded to the client. The client's DHCPv6 discovery messages reach the server, but server reply packets are dropped by the switch.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00801153</b> CRAOS8X-50856	<b>Summary:</b> OS6860N-P48Z: No connectivity after successful authentication on UNP SAP port.  <b>Explanation:</b> Connectivity issue is noticed on UNP SAP ports after toggling the ports. Authentication is successful, however, there is no connectivity after authentication. For example, the DHCP packets from the client are dropped.   <a href="#">Click for Additional Information</a>







<b>Case:</b> <b>00806249</b> CRAOS8X-51440	<b>Summary:</b> OS6860N: Connectivity issue on UNP ports after successful authentication.  <b>Explanation:</b> After SAP ports are successfully authenticated, all ingress traffic is dropped. The issue is observed only on ports that are toggled. Ports that remain stable continue to function normally as long as they are not flapped.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00806834</b> CRAOS8X-51633	<b>Summary:</b> OS6860E: Lifetime value for IPv6 RA-RDNSS and RA-DNSSL set to 0  <b>Explanation:</b> After SAP ports are successfully authenticated, all ingress traffic is dropped. The issue is observed only on ports that are toggled. Ports that remain stable continue to function normally as long as they are not flapped.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00783021</b> CRAOS8X-49335	<b>Summary:</b> In certain conditions, the following log was generated:  sftp-server[#] process_remove:1431 /flash/switch/dhcpClient.db  <b>Explanation:</b> This is a functional process log only. In AOS 8.10R03, its severity has been reduced, so it will not be flooded by default.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00800614</b> CRAOS8X-44940	<b>Summary:</b> Unable to download the port-monitoring file using SFTP/FTP from OS9900/OS9912.  <b>Explanation:</b> The port monitoring file was generated with incorrect file permissions. A workaround is available.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00777632</b> CRAOS8X-48478	<b>Summary:</b> OS6900 not handling SNMP requests sent by NMS.  <b>Explanation:</b> The aluSubagent which handles SNMP requests has its queue overloaded and congested and stops processing the incoming requests, resulting in SNMP timeout.   <a href="#">Click for Additional Information</a>









<b>Case:</b> <b>00784398</b> CRAOS8X-49464	<b>Summary:</b> On OS6900 with 2x PSU DC 400W, show powersupply displays 1x PSU in Unplugged state , even though the PSU front light (on the switch) and the PSU back light are all solid green.  <b>Explanation:</b> If the input voltage experiences fluctuations and is measured under a certain level ( $0 < V_{in} < 10$ ), the power supply state will be changed and stay to Unplugged status.  <b>Note:</b> the power supply still provides power to the switch, even though the display indicates Unplugged state. There is no risk for the switch to loose power.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00810994</b> CRAOS8X-47388	<b>Summary:</b> On OS6860 or 6865, running 89R04, show health memory is constantly displaying 10% .  <b>Explanation:</b> The health monitoring AOS process does not retrieve the proper memory usage values, to display it in show commands. Also the health monitoring memory threshold is not raised in the SNMP traps.  <b>Note:</b> it is a display issue, the memory is managed correctly in the switch.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00795505 /</b> <b>00798687</b> CRAOS8X-50411 / CRAOS8X-50624	<b>Summary:</b> ISSU from 89R04 to 810R02, with 6860N or 6900X48C6, using VFL DAC-100G-C5M fail with VC split.  <b>Explanation:</b> For these VFL DAC-100G-C5M, autoneg has been disabled in 810R02, whereas it was enabled in 89R04 and previous releases.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00784879</b> CRAOS8X-49517	<b>Summary:</b> Status of the RADIUS servers configured in the AOS switch flaps randomly.  <b>Explanation:</b> RADIUS server status is DOWN as per switch logs; however, there is no reachability issue between the switch and the server. A new approach is introduced to avoid these situation to get multiple socket binding to the same port.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00787553</b> CRAOS8X-49736	<b>Summary:</b> "Port-Monitoring" captures contain 802.1Q tag even when the Packets are captured from a source port with untagged VLAN.  <b>Explanation:</b> In AOS 8.x switches the ingress packets doesn't have the 802.1Q VLAN TAG; however, the egress packets are added with 802.1Q VLAN TAG. This behavior is a limitation, which is legacy and known. Egress packets captured using "port monitoring" contain a VLAN-header regardless the source port is tagged/untagged.




	 <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00790210</b> CRAOS8X-49923	<b>Summary:</b> In AOS 8.x switches, HTTPS is not enforced with HSTS (HTTP Strict Transport Security).  <b>Explanation:</b> During vulnerability scan in AOS 8.x switches, it is identified that HTTPS is not enforced with HSTS (HTTP Strict Transport Security).  If HTTPS is not enforced with HSTS, it could potentially allow a man-in-the-middle attack or downgrade HTTPS to plain text, enabling interception of the user's network traffic.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00791112</b> CRAOS8X-49971	<b>Summary:</b> AOS 8.x switches does not generate trap for RADIUS status change.  <b>Explanation:</b> AOS 8.x switches generate only the switch logs, if any of the configured RADIUS server is DOWN. New OIDs are added to generate traps during RADIUS server UP and DOWN scenario.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00782915</b> CRAOS8X-50488	<b>Summary:</b> During SNMP walk, the AOS switch incorrectly reports "ifHighSpeed" value as 0 for Link Aggregation.  <b>Explanation:</b> AOS switch set the value as Zero for "ifHighSpeed" in code by default; hence, the polled value is '0' during the snmpwalk. Issue seems to be specific to the linkagg ports and not the physical ports. This is a display issue and there is no functional impact.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00799177</b> CRAOS8X-50720	<b>Summary:</b> QOS QSI stats of a linkagg port is mirrored on other linkagg ports, even if the other linkagg ports are physically down.  <b>Explanation:</b> The loop in function "vfcmsShowStats" leads to a MIP OVERFLOW message, hence repeated entry of outputs were notices in QOS QSI stats. Issue is seen only when the linkagg agg number is clubbed in the CLI command.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00799588</b> CRAOS8X-50709 / CRAOS8X-49580	<b>Summary:</b> Resolving Throughput Issues on OS6560 10G to 1G Connections  <b>Explanation:</b> During periods of bursty traffic, egress traffic on 1 Gbps ports may exhaust buffers, significantly reducing throughput on the OS6560.

	<p>Starting with firmware version 8.10R03, a new debug command allows configuration of extended egress buffers with four settings: default, medium, high, and high2.</p> <p>debug qos port 1/1/11 packet-buffer [default   medium   high   high2]</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00788095</b> CRAOS8X-49796</p>	<p><b>Summary:</b> The network administrator observes high CPU usage (&gt;75%) on the core switch, with the Spanning Tree Protocol (STP) process as the top consumer.</p> <p><b>Explanation:</b> High CPU usage occurs when a switch boots with PVST+ compatibility enabled and a VLAN priority set to a value other than zero or a multiple of 4096. In such cases, the switch incorrectly uses the VLAN ID as the priority (e.g., VLAN 200 advertises a priority of 200), which violates the PVST+ standard. The PVST+ standard requires VLAN priorities to be zero or a multiple of 4096.</p> <p>Prior to AOS 8.10R03, the switch allowed booting with such misconfigurations, leading to non-standard behavior and increased CPU load. Additionally, once PVST+ compatibility is enabled, VLAN priorities cannot be set to non-compliant values.</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00771729</b> CRAOS8X-47973</p>	<p><b>Summary:</b> Switch will not be accessible via SSH or Telnet after configuring app-mon in the switch uplink.</p> <p><b>Explanation:</b> It appeared to have an issue with TCAM programming when APP-Mon is enabled on the network port. When appmon enabled on uplink ISIS network port, the switch was inaccessible via telnet or SSH from the adjacent switch.</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00788379</b> CRAOS8X-49795</p>	<p><b>Summary:</b> High memory in the Master unit, due to "agNI" process.</p> <p><b>Explanation:</b> For the arp packet, it creates a lookup table in the AGNI, and based on the packet tagging, the agni is finding the lookup and creating if we have miss in the finding.</p> <p>In the log, it is noticed that for every untagged ARP packet, Agni finds the lookup table for the default VLAN, and for the miss, it creates a new lookup for the native VLAN (unlearned).</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00794078</b> CRAOS8X-50181</p>	<p><b>Summary:</b> Sflow not working and breaking some other modules, like port monitoring and mirroring.</p> <p><b>Explanation:</b> While configuring Sflow on the non default VRF and followed by the port monitoring/mirroring configuration, it breaks the protocol.</p>

	 <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00779753</b> CRAOS8X-49343	<p><b>Summary:</b>  OS6560-P48Z16 running AOS 8.9.94.R04.or 8.10 R02 is facing a reboot while accessing learnedPortSecurityAgL2MacAddressTable and generated pmd.</p> <p><b>Explanation:</b>  Upon using snmp-getNext request for the table learnedPortSecurityAgL2MacAddressTable. The switch will convert the port index in to gport and fetch the port info struct and macvlancb for the corresponding gport.</p> <p>While accessing the getNext for the table with wrong index the macvlancb NULL value is returned and without further validation, switch is accessing the content inside a macvlancb pointer and getting in to the issue state.</p>  <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00781332</b> CRAOS8X-49384	<p><b>Summary:</b>  OmniSwitch 6860 Blocks wireless user traffic when AP mode is enabled in UNP</p> <p><b>Explanation:</b>  In a scenario where the AP has multiple SSIDs with tagged and untagged vlans, the switch changes the lportAP value from 1 to 0 when 1<sup>st</sup> client connects in tag and second in untagged SSID. When a 3<sup>rd</sup> client connects its blocked as lportAP=0.</p>  <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00777403</b> CRAOS8X-48612	<p><b>Summary:</b>  Routes not exchanged correctly to the other sites.</p> <p><b>Explanation:</b>  Few random routes from one SPB node not getting learned by the adjacent node via L3 IPVPN.</p>  <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00785068</b> CRAOS8X-49536	<p><b>Summary:</b>  Show IPVPN route table display issue</p> <p><b>Explanation:</b>  Show IPVPN route table display issue as the routes are not seen despite Exporting to the adjacent SPB node.</p>  <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00776399</b> CRAOS8X-49603	<p><b>Summary:</b>  OS6900: SPB LSP flood in the network.</p> <p><b>Explanation:</b>  The unit-2 (slave) of VC of OS6900-V72 was losing SPB adjacency to the nodes which are directly connected, at the same time the nodes connected to Unit-1 (Master) are stable.</p>  <a href="#">Click for Additional Information</a>





<b>Case:</b> <b>00779694</b> CRAOS8X-49422	<b>Summary:</b> OS6900-V48C8: Problem in getting IP address from DHCP server.  <b>Explanation:</b> The clients are not getting the IP address from the DHCP server connected to the OS6900-V72. The OS6900-V48 switch running in 8.10.R01GA acting as a DHCP relay was not forwarding DHCP offers to the clients.  🔒 <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00793735</b> CRAOS8X-50158	<b>Summary:</b> Circuit ID are not matching bewteen the show spb isis interface and show spb isis interface port x/x/x.  <b>Explanation:</b> A display issue where circuit ID are not matching bewteen the show spb isis interface and show spb isis interface port x/x/x.  🔒 <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00795214</b> CRAOS8X-50265	<b>Summary:</b> Switch as .1x supplicant "sw-supp-secure-mode" learnt as "trust-tag" if supplicant port is tagged.  <b>Explanation:</b> Switch A is the supplicant switch and switch B is the NAS, If Switch A is being tagged with a vlan that is used for dhcp-client ip interface, from Switch B the MAC of switch A is learnt as trust-tag and authentication is not triggered for switchA. This behavior is not normal and fixed in 8.10R03GA  🔒 <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00806143</b> CRAOS8X-51433	<b>Summary:</b> Swlog tls config is lost after reboot if the port used is not the default one.  <b>Explanation:</b> Configuring syslog over TLS to use port 6514, config saved and sync, if switch reboot then the config is no more available in the output show config snapshot system.  🔒 <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00790442</b> CRAOS8X-50043	<b>Summary:</b> VRRP Instances Lost When Deleting an IP Interface.  <b>Explanation:</b> Deleting an IP interface in a VLAN with multinetting removes all VRRP instances for that VLAN.  🔒 <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00798840</b> CRAOS8X-50971	<b>Summary:</b> Unexpected Reboot on USB Unmount with AOS 8.10.R02 on 6560-24X4 switches.




	<p><b>Explanation:</b> The issue was diagnosed as a software defect related to improper handling of USB storage unmounts.</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00732743</b> CRAOS8X-44001</p>	<p><b>Summary:</b> IP phones connected to OS6860E are entering into 802.1X authentication loop.</p> <p><b>Explanation:</b> 802.1X and MAC authentication are triggered by the IP phone, which causes 802.1X authentication failure. Once 802.1X auth failure is received the IP phone triggers reauthentication which starts the authentication loop.</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00766258</b> CRAOS8X-47562</p>	<p><b>Summary:</b> IP Phones failing to obtain an IP Address after moving to a different OS6860N.</p> <p><b>Explanation:</b> Both new and existing IP phones are unable to obtain an IP address as the DHCP DORA process remains incomplete.</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00776789</b> CRAOS8X-48614</p>	<p><b>Summary:</b> OS6360 Unable to remove device-profiling associated with unp configuration.</p> <p><b>Explanation:</b> Extended classification rules are automatically defined when Device Profiling is enabled for the switch, and these rules cannot be removed.</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00780757</b> CRAOS8X-48952</p>	<p><b>Summary:</b> Some devices never receive an IP address.</p> <p><b>Explanation:</b> In the relay switch, a mismatch between the primary interface and the relayed client interface is causing the issue.</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00789454</b> CRAOS8X-49851</p>	<p><b>Summary:</b> OS6560 thin client is not going for auto fabric when the switch is upgraded to 8.10R01MR.</p> <p><b>Explanation:</b> In 8.10.R1 onwards code changes are made that if there is an empty VCboot.cfg is present in the directory the auto-configuration will not trigger.</p> <p> <a href="#">Click for Additional Information</a></p>

<b>Case:</b> <b>00790650</b> CRAOS8X-49951	<b>Summary:</b> On the OS6360 switch, during reboot, the fan may enter a failure state and remain non-operational.  <b>Explanation:</b> Upon boot-up, the switch checks the fan status register to determine the fan's condition. If the register contains valid data, the fan is marked as operational. If the data is invalid or unavailable, the fan is marked as faulty.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00805042</b> CRAOS8X-51289	<b>Summary:</b> Need to know if CVE-2025-26466 and CVE-2025-26465 are vulnerable to AOS 8.X switches.  <b>Explanation:</b> The OpenSSH client and server are vulnerable to a pre-authentication DoS attack that causes memory and CPU consumption.  CVE-2025-26466 and CVE-2025-26465 is fixed in AOS 8.10R03 GA.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00801483</b> CRAOS8X-47308	<b>Summary:</b> Noticed the slowness in loading the Notification Page or saving configurations to switches in the OVC.  <b>Explanation:</b> The issue is due to the continuous increase in the number of out of order SNMP traps from AOS 8X switches while older traps with smaller sequence IDs are being deleted. This repeated deletion and creation of new traps with smaller SEQ IDs is wasting OVC resources and causing the high CPU and OVC slowness. SNMP out-of-order traps issue is fixed in AOS 8.10R03 GA.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00786254</b> CRAOS8X-49830	<b>Summary:</b> The OS6360 switch lost connectivity when applied QoS from OV2500 LDAP.  <b>Explanation:</b> Policies pushed from OV have the source set as QOS_SOURCE_LDAP. After a reboot, when the switch loads policies from the vcboot.cfg, there is a mismatch in the QoS policy source. The network group policy, originally sourced from LDAP, is re-initialized with the source QOS_SOURCE_CLI, leading to a mismatch. As a result, the entry moves to the PENDING_PRIME state, updates the source to CLI, and removes all TLVs, so the network group configuration is not applied. Without the network group, the drop rule blocks all traffic, causing the switch and OV to become unreachable.  The issue is fixed on 8.10.R03 GA.




	<a href="#">🔒 Click for Additional Information</a>
<b>Case:</b> <b>00810673</b> CRAOS8X-52074	<p><b>Summary:</b> CLI interprets ! (Exclamation mark) as a command, not a comment in AOS 8.X switches.</p> <p><b>Explanation:</b> Due to recent updates in bash compiling tools, the code handling this feature wasn't loaded correctly. This issue is fixed in AOS 8.10R03 GA.</p> <p>🔒 <a href="#">Click for Additional Information</a></p>
<b>Case:</b> <b>00805068,</b> <b>00807964,</b> <b>00796677</b> CRAOS8X-50683	<p><b>Summary:</b> Upgrading the OS6900 to version 8.10R02 resulted in the loss of the Advanced PERM license.</p> <p><b>Explanation:</b> In version 8.10R02, the Advanced License incorrectly switches to DEMO mode instead of remaining PERMANET license mode, unlike in other AOS 8.X versions. A fix to auto-install the license if a permanent one isn't found is included in AOS 8.10R03 GA.</p> <p>🔒 <a href="#">Click for Additional Information</a></p>
<b>Case:</b> <b>00789710</b> CRAOS8X-49955	<p><b>Summary:</b> When supplicant switch is initiating VLAN traffic on more than one VLAN, supplicant switch which is connected to NAS switch on the UNP port, faces an authentication times out and fails.</p> <p>Workaround: Authentication works again if tagged traffic is stopped and supplicant switch or UNP port is admin DOWN to UP for re-authentication.</p> <p><b>Explanation:</b> The issue is seen since the supplicant switch is connected to NAS before enabling the UNP on the NAS port, and the device type was not updated in the LLDP shared memory as expected. This issue is fixed in AOS 8.10R03 GA.</p> <p>🔒 <a href="#">Click for Additional Information</a></p>
<b>Case:</b> <b>00796771</b> CRAOS8X-50442	<p><b>Summary:</b> Trust-tag UNP (or) LLDP-MED classification is applied for supplicant switch device traffic on UNP port before performing RADIUS authentication on the NAS switch.</p> <p><b>Explanation:</b> The issue is seen for the NAS switch port type bridge since the classification is done based on the tagged packets, before the switch supplicant authentication completes. Even though the supplicant authentication is not completed, the Mac is already learnt as switch supplicant Mac, based on the config and the lldp packets. Hence tagged packets trust-tag-based classification is done and Mac is learnt. The onex authentication for switch supplicant MAC ends up in AAA timeout in this case, and the same mac learnt to block with timeout error.</p>













	<p>Fix available in AOS 8.10R03 GA.</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00807152</b> CRAOS8X-51717</p>	<p><b>Summary:</b> PortMgrNi error detected in OS6860 and OS6865 switch.</p> <p>portMgrNi main ERR: : [pmnHALLinkStatusCallback:230] Error geting port state for gport 16908289  portMgrNi main ERR: : [pmnHALLinkStatusCallback:513] Cannot get state of port int: 2/1/0/1 (gport 0x1020001)  portMgrNi main ERR: : [pmShmDbSetPPEEntry:653] PM PP Entry - gport 16908289 Entry Not found (nil)  portMgrNi main ERR: : [pmProcessLinkStatus:159] Unable to Set PM PP Entry gport 0x1020001</p> <p><b>Explanation:</b> The fix for this error log is provided in AOS 8.10R03 GA.</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00794879</b> CRAOS8X-50998</p>	<p><b>Summary:</b> 802.1X reauthentication fails on UNP port after manual flushing done using “unp user flush port &lt;port id&gt;” command.</p> <p><b>Explanation:</b> After using UNP user flush port on a UNP-enabled port, 802.1X reauthentication fails and falls back to MAC authentication.</p> <p>Fix available in AOS 8.10R03 GA.</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00801813</b> CRAOS8X-51042</p>	<p><b>Summary:</b> UNP port range command is not saved after configuration. Example: unp port 1/1/1-6 profile vlan &lt;id&gt;  Attempt for reconfiguration printed the following error:  "ERROR: Profile with duplicate service parameter"</p> <p><b>Explanation:</b> 'show config snapshot da-unp' output missed to print the UNP port profile config for the first or first range of ports. Configuration is applied but not seen during the config snapshot, which will lead to missing the config permanently if reload is done.</p> <p>Fix available in AOS 8.10R03 GA.</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00798570</b> CRAOS8X-50618</p>	<p><b>Summary:</b> A few CLI commands throw an error as follows for virtual chassis manager application.</p> <p>swlogd MIP_GATEWAY mipgwd WARN: ERROR response for MIP_GET(1) 67/0-&gt;153 (APPID_CLI-&gt;APPID_VIRTUAL_CHASSIS_MANAGER) 4955:</p>

	<p>swlogd MIP_GATEWAY mipgwd WARN: ERROR code: 33/13(specified application not loaded)</p> <p>The other applications loading error as given below are already addressed from AOS 8.9.94R04 and later builds.</p> <p>APPID_AAA APPID_CONFIGMANAGER APPID_VLAN_MGR APPID_SRCLEARNING</p> <p><b>Explanation:</b> The socket between the MIP gateway and some of the applications seems disconnected, and hence those applications are not responding to the respective CLI commands. So, a reconnection mechanism to the MIP gateway has been implemented to establish the connection again with the disconnected applications. The fix is available in AOS release 8.10R03.</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00795478</b> CRAOS8X-50418</p>	<p><b>Summary:</b> Vulnerability check of CVE-2024-13176 for AOS 8X switches.</p> <p><b>Explanation:</b> The fix for CVE-2024-13176 is included in the AOS release 8.10R03.</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00776491</b> CRAOS8X-48406</p>	<p><b>Summary:</b> Need to change the length of the attribute "EAP-Key-Name" from 2 bytes to a minimum of 3 bytes when the switch sends the "EAP-Key-Name" empty in the Access-Request to request this attribute to make it compatible with ClearPass Policy Manager as RADIUS server.</p> <p><b>Explanation:</b> Basically, when a host MACsec is detected, the switch adds an attribute "EAP-Key-Name" in the RADIUS Access-Request. The "EAP-Key-Name" will be added in the Access-Accept from the RADIUS server (ClearPass) only if the Access-Request includes an empty EAP-Key-Name attribute with a length of &gt;=3 bytes. The fix is available in AOS release 8.10R03.</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00789703</b> CRAOS8X-49922</p>	<p><b>Summary:</b> Unable to export CSR (certificate signing request) from the switch and upload a custom CA certificate in the "ca.d" directory.</p> <p><b>Explanation:</b> The private key generated from the switch has no option to select RSA key size; by default, it chooses 2048. Now, the key sizes up to 4096 (2048, 3072, 4096) are supported. The fix is available on AOS release 8.10R03.</p>






	<a href="#">🔒 Click for Additional Information</a>
<b>Case:</b> <b>00796991</b> CRAOS8X-50514	<p><b>Summary:</b> The switch is rebooting daily due to failure of the "udpRelayCmmd" task, and PMD is getting generated.</p> <p><b>Explanation:</b> The DHCP payload packet length is 1518, and the actual buffer payload length (Bplen) is 2020. The mismatch in length of the DHCP data packet and DHCP server payload leads to generating the PMD every time the client sends the request packet to the server. The fix is available on AOS release 8.10R03.</p> <p><a href="#">🔒 Click for Additional Information</a></p>
<b>Case:</b> <b>00780279</b> CRAOS8X-49238	<p><b>Summary:</b> Swlog error message "Interface is not fiber channel" though fiber channel is not configured "intfCmm Mgr ERR: cmmEsmDrv_alcfcStatsTableGet:5745 Interface &lt;101049&gt; is not fibre channel"</p> <p><b>Explanation:</b> Code change done to move the "cmmEsmDrv_alcfcStatsTableGet" error log to debug2 level</p> <p><a href="#">🔒 Click for Additional Information</a></p>
<b>Case:</b> <b>00789410</b> CRAOS8X-49908	<p><b>Summary:</b> Unable to assign ip name-server with the IP address ending with ".127".</p> <p>-&gt; ip name-server 192.168.10.127 ERROR: Test of IP name server address failed: c0a80a7f.</p> <p><b>Explanation:</b> Code changes done to fix this issue.</p> <p><a href="#">🔒 Click for Additional Information</a></p>
<b>Case:</b> <b>00786908</b> CRAOS8X-49997	<p><b>Summary:</b> Vlan-xlation enable was missing after rebooting the switch. The following error was noticed in switch log.</p> <p>Configuration done: service access port 1/1/7</p> <p>Added VLAN tag configuration to the SAP port configured with hybrid enabled.</p> <p>Configuration noticed: service access port 1/1/7 vlan-xlation enable</p>

	<p>svcCmm mPORT ERR message: smgrPmSetPortProperty@1326 Port=1007 state=0 property=0x80 cur_state=2(TAGGED) cur_prop=0x3000001(Multiple Conflicting Properties!) gport=6 res=11</p> <p><b>Explanation:</b> The properties of PM_SFLOW_SAMPLER_PORT and PM_SFLOW_POLLER_PORT are not enabled for the port property PM_SERVICE_ACCESS_PORT.</p> <p>This issue is fixed in AOS 8.10R03.</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00802116</b> CRAOS8X-51414</p>	<p><b>Summary:</b> ISFP-10G-C1M is showing the link Down after a reboot on hybrid combo ports. 10G DAC connected port was down which is connected on 1G port.</p> <p><b>Explanation:</b> Previous changes done to update PHY type of 10G copper port as SFP_PLUS_COPPER on 1G port were not applied to the hybrid combo ports of OS6360-48/P48, which is the root cause of the issue. This issue is fixed in AOS 8.10R03.</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00782292</b> CRAOS8X-49666</p>	<p><b>Summary:</b> NULL gateway IP in static route configuration is not removed from VRF, when issued “show configuration snapshot   grep vrf”.</p> <p>Vrf create test test::-&gt; ip static-route 192.168.100.0/24 gateway 0.0.0.0</p> <p><b>Explanation:</b> In iprmSRDeleteStaticList() , for default gateway, the gwaddr is assigned with loopback address (127.0.0.0) and same is passed in iprmSRFindInStaticList() instead of 0.0.0.0 (NULL gateway IP). When configuration was verified, it will scan the IPv4 static route list looking for a match. As it could not find static route with loopback as gateway, NULL is returned and SkipListDelete is not called. Hence the entry is not deleted.</p> <p>This issue is fixed in AOS 8.10R03.</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00791641</b> CRAOS8X-50061</p>	<p><b>Summary:</b> Duplicated traps were found in OV notification. When slave unit in a VC is rebooted</p> <p><b>Explanation:</b> slave switch sends an unexpected sequence ID when it goes for a reload, the repolled traps are treated as new traps, resulting in duplicate traps being displayed. The reception of unexpected lower and higher sequence IDs causes OV to clear the existing</p>






	<p>traps and repoll all traps as new ones; however, the root cause (RCA) for this behavior is because the slave unit has its own trap sequence ID.</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00799356</b> CRAOS8X-51326</p>	<p><b>Summary:</b> While configuring SPB with inline routing on an OS6900-C32E, it was observed that the QoS policy did not drop traffic as expected, even though it was intended to be dropped.</p> <p><b>Explanation:</b> The QoS policy does not work as intended because service packets are not classified by the software. When service-tagged packets reach the QoS module, they are simply forwarded without any checks or classification</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00800621</b> CRAOS8X-50817</p>	<p><b>Summary:</b> OS6870 when configuring "no forwarding" for an IP interface, unable to ping the IP interface configured within the same subnet.</p> <p><b>Explanation:</b> This issue is due to packet drop at the hardware level in OS6870 switches.</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00782330</b> CRAOS8X-49161</p>	<p><b>Summary:</b> AOS 8.X switches is not connecting to OVC after upgrading to 8.10.R01 when using Remote Configuration Download (RCL) for initial provisioning</p> <p><b>Explanation:</b> RCL will be enabled automatically if there is no vcboot.cfg is present or vcboot.cfg with 0 size present for the builds before 8.10.R01. From 8.10.R01, RCL will only start if there is no vcboot.cfg is present. RCL will not start even if the vcboot.cfg with size 0</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00767263</b> CRAOS8X-47121</p>	<p><b>Summary:</b> The clients in L2GRE profile on a OS6560-P48Z16 do not get an IP address.</p> <p><b>Explanation:</b> When the end device is connected to a port between 25 and 48, which falls on ASIC-1, the UNP profile L2GRE is assigned to an L2GRE service, which is incorrectly programmed in the hardware. This is the reason L2GRE packets are not even sent out of the switch.</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00755303</b> CRAOS8X-48391 / CRAOS8X-49803</p>	<p><b>Summary:</b> L2GRE GTTS tunnel is not stable when multiple routes are available to reach far-end IP.</p> <p><b>Explanation:</b></p>





	<p>The IPRM is updating the Service Manager with two routes, i.e., the default route and the /24 route. This is not expected, as only the best route should be updated to the SVCMMGR. This makes svc mgr toggle the next hop between the default route and specific route every 3 minutes as the arp is refreshed.</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00789099</b> CRAOS8X-49846</p>	<p><b>Summary:</b> The L2GRE traffic from Wireless client is dropped on OS6900 switches after the loopback0 was reconfigured</p> <p><b>Explanation:</b> When the IP interface Loopback0 was reconfigured, the global variable for Loopback0 was set to 0 instead of the address of the loopback0.</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00792729</b> CRAOS8X-50106</p>	<p><b>Summary:</b> A new L2GRE service has been created to terminate the tunnel from a new site. However, the clients connected to this service are not getting their IP addresses. The existing services are working fine, and the clients in those services are working.</p> <p><b>Explanation:</b> The VPs that are being allocated to the new SAPs are causing the issue. When one of the used VPs is assigned to a new SAP, the L3 bitmap is not getting programmed; this affects the traffic getting terminated on the service using that SAP and the VP.</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00805095</b> CRAOS8X-51302</p>	<p><b>Summary:</b> When the ports are configured as LAG and port mirroring is enabled, the UDLD cannot be configured on those ports. It throws an error.</p> <p><b>Explanation:</b> The LACP+PMM+UDLD is a valid combination. This issue is seen in AOS 8.10 R02, which adds a check for the LACP ports when UDLD is being configured. The releases prior to 8.10 R02 are not impacted by this issue.</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00775052</b> CRAOS8X-48419</p>	<p><b>Summary:</b> The Axis Cameras are not powered up on OS6465-P12</p> <p><b>Explanation:</b> The Axis cameras are powered up with ALT-B pairs, and by default, the switch provides power on ALT-A. A command is introduced in 8.10 R03 to enable the Alt-B.</p> <p> <a href="#">Click for Additional Information</a></p>



<b>Case:</b> <b>00784656</b> CRAOS8X-49591	<b>Summary:</b> After an upgrade from 8.9R04 GA to 8.10R01 GA it was noticed that even after a gratuitous ARP was sent the switch did not updated its ARP table.  <b>Explanation:</b> When the new EVPN (Ethernet Private Virtual Network) feature was introduced, it broke gratuitous ARP.  A fix has been checked into 8.10.116.R01 MR for this issue.  🔒 <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00772941</b> CRAOS8X-48758	<b>Summary:</b> Noticed high memory in the VC of OS6360 switches running in version 8.9.94.R04. Due to this, the clients were getting disconnected from the switch.  <b>Explanation:</b> The issue was due to the reception of ARP flood to the switch. For the ARP packet, the switch creates a lookup table in the AGNI and does not get erased, making the memory spike gradually.
<b>Case:</b> <b>00772311</b> CRAOS8X-47797	<b>Summary:</b> Memory usage increases by approximately 1% every 2-3 days. The issue persists even after upgrading to version 8.9.94.R04 on a different Virtual Chassis (VC). Investigation revealed high memory consumption by the mrvld and lpNi tasks.  <b>Explanation:</b> The root cause is linked to a memory leak associated with sshd, and a permanent fix is included in AOS version 8.10.R03.  🔒 <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00784371</b> CRAOS8X-49998	<b>Summary:</b> OS6900-Traffic interruption while performing the ISSU upgrade.  <b>Explanation:</b> If the packet has to traverse from Master unit-1 when slave is in bootup process no issue will be seen, however when the traffic has to switch back from Master to (New Master unit-2) the ping or any traffic was getting failed and the issue will be seen only if the linkagg is configured as SDP ports. The traffic would resume once the unit-1 joins back to as slave to the VC.  🔒 <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00769578</b> CRAOS8X-47611	<b>Summary:</b> OS6560: CRC errors on copper port running in 10mbyte half-duplex.  <b>Explanation:</b> The DCS systems connected to these switches, which operate at 10 Mbps and half-duplex are reporting CRC errors on the connected ports.  🔒 <a href="#">Click for Additional Information</a>



<b>Case:</b> <b>00773563</b> CRAOS8X-48931	<b>Summary:</b> Server traffic is disrupting while trying to upgrade a VC via ISSU.  <b>Explanation:</b> The upgrading of the switches in the virtual chassis by ISSU upgrade procedure from 8.9.107.R02 to 8.10.102.R01 and the servers are connected to the switches, losing communication.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00783407</b> CRAOS8X-49481	<b>Summary:</b> OS6860E reporting below error: ERROR: no answer received (timeout)-18 (CLI-mip_msg_nowait_response)  <b>Explanation:</b> The errors are seen when tried to issue show commands and also during flash synchronization via commands.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00790671</b> CRAOS8X-49921	<b>Summary:</b> OS6900-X24C2: Flapping the missing route makes the existing route disappear.  <b>Explanation:</b> Routes are missing between SPB adjacent nodes that were supposed to be learned via L3-VPN, and to recover the situation, deleting and forcing the missed route to relearn is replacing the existing route.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00792136</b> CRAOS8X-50093	<b>Summary:</b> OS6860E, upon upgrading either to the release 8.9 R04 or higher version AOS 8.10 R01, a new service is being created dynamically on the switch.  <b>Explanation:</b> Transit service ISID created by the switch is affecting the UNP user who needs to use the same service.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00805949</b> CRAOS8X-51722	<b>Summary:</b> When out-of-box switch boot it uses RCD, the DHCP Offer is never received.  <b>Explanation:</b> The out-of-box switch was sending DHCP Discovery including a Trailer that was not added on purpose as the packet was not undersized frame. This unwanted trailer was causing the DHCP packet drop by the uplink on AOS switch.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00794969</b> CRAOS8X-50482	<b>Summary:</b> OS6560-P48X4: VC partial split scenario.



	<p><b>Explanation:</b> OS6560-P48X4: Partial VC spilt scenario observed as Master unit identifying the slave units however no interface ports from slaves units are seen.</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00799231</b> CRAOS8X-50685</p>	<p><b>Summary:</b> OS6900: 'fec fc' commands does exist upon reboot however not operational.</p> <p><b>Explanation:</b> A VC of 2 OS6900-X48C8 have been upgraded via ISSU from AOS 8.9 R03 to AOS 8.10 R01, however upon VC bootup, the uplink ports which are configured with FEC mode as FC does exist in the configuration however, the port wasn't coming up until this command is removed and readded.</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00810109</b> CRAOS8X-51998</p>	<p><b>Summary:</b> OS6900-V72: LSP flooding and SPB adjacency loss for 300 seconds.</p> <p><b>Explanation:</b> Unexpected LSP flooding, followed by SPB adjacency loss, is observed on the virtual chassis. The SPB adjacency remains DOWN for around 300 seconds.</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00809736</b> CRAOS8X-52105</p>	<p><b>Summary:</b> When client ARP packets are transmitted over EVPN tunnel, the destination mac address is set to all zeros.</p> <p><b>Explanation:</b> As ARP suppression is disabled, the ARP packets are transmitted over the EVPN tunnel. However, while transmitting the ARP packet, the destination MAC address is set to all zeros. Notice the following output. EVPN-Node-1 received an ARP packet from Client1 with the destination MAC address set to broadcast (ff:ff:ff:ff:ff:ff). However, when the ARP packet is forwarded over the EVPN tunnel, the destination mac-address is changed to all zeros (00:00:00:00:00:00).</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00807566</b> CRAOS8X-51655</p>	<p><b>Summary:</b> After upgrading the OS6860N-P48M switch to 8.10.115.R01, the UNP worked for some time and then stopped working. The APs are working fine, but the clients connected to the AP don't get an IP address. When the "show unp user" command is executed on the switch, only the output "Please wait ...".</p> <p><b>Explanation:</b> The issue is seen due to a deadlock causing the UNP engine to hang and thus blocking the DHCP and packets and user authentications.</p> <p> <a href="#">Click for Additional Information</a></p>

<b>Case:</b> <b>00812860</b> CRAOS8X-52463	<b>Summary:</b> SNMP OID dot1qTpFdbPort does not show the ports of slave chassis.  <b>Explanation:</b> In a Virtual Chassis (VC) setup of OS6860N-P48Z switches, MAC addresses learned on untagged VLANs through slave chassis ports are not reflected in the SNMP OID dot1qTpFdbPort, even though they are correctly learned and visible via CLI.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00774343</b> CRAOS8X-47974	<b>Summary:</b> Unlike IPv4, the OS6900 switches do not support an equivalent command for IPv6 BGP route aggregation (such as the ip bgp aggregate-address used in IPv4 configurations).  <b>Explanation:</b> A new CLI command is introduced to support IPv6 BGP route aggregation.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00777895</b> CRAOS8X-48480	<b>Summary:</b> Encountering the error "not supported by PortMacro TSC" when using the "configuration apply ..." command.  <b>Explanation:</b> During the initial configuration of 25G ports 51-54 on OS6900 switches, an error may appear when Auto-Negotiation (AN) is enabled without any SFPs inserted. For port 51, AN can be disabled without triggering any errors, but for ports 52-54, an error is logged during the first configuration after reboot. This behavior is observed only when there is no transceiver connected at the time of configuration. The error has no impact on port functionality and does not recur once the ports are configured successfully. It is specific to ports 51-54 and does not affect other ports. A fix to suppress these non-impacting error messages is planned for AOS 8.10.R03.   <a href="#">Click for Additional Information</a>
<b>Case:</b> <b>00794750</b> CRAOS8X-50391	<b>Summary:</b> After a migration, the switch began logging recurring TLS-related errors on port 10161, including messages such as "Accepted TLS connection," "Failed SSL_accept," and associated OpenSSL system errors. These logs raised concerns during post-migration monitoring.  <b>Explanation:</b> The errors occur when the switch receives invalid or incomplete TLS connection attempts on port 10161, which remains open when SNMP TLS security is enabled by default. These attempts fail during the handshake process, resulting in SSL-related log messages. The errors are harmless and do not impact switch functionality. Disabling SNMP TLS with the command snmp security tls disable filters traffic on this port and stops the error logs.   <a href="#">Click for Additional Information</a>

<p><b>Case:</b> <b>00794989</b> CRAOS8X-50420</p>	<p><b>Summary:</b> The edge router is receiving repeated unauthorized SSH attempts, resembling a DoS attack. Although deny policies are applied, some traffic still reaches the router because the command “show policy network group Switch is showing as "modified" and does not include all active switch IP interfaces.</p> <p>Following TCAM errors will be seen when doing a qos apply:</p> <p>swlogd tcamni main ERR: : [tnComparatorPairReserve:13837] : Source is not valid for Rule</p> <p>swlogd tcamni main ERR: : [tnPopulateBcmFieldQualifiers:7602] : Comparator NOT found in Db TCAM_RET_NOT_FOUND 0 0 ipProto 17 state COMM SRC</p> <p><b>Explanation:</b> The issue occurs because the current policy uses the Switch network group in combination with TCP/UDP port ranges (e.g., udp-port 1812-1813). This combination requires more specific matching logic, which fails if the Switch group does not include all active IP interfaces. As a result, the deny rule does not apply consistently, allowing unwanted traffic through. To address this, it's recommended to create a dedicated network group that includes all relevant switch IPs and avoid combining the Switch group with port ranges.</p> <p>Code change is done to ensure consistent policy enforcement in such scenarios.</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00798867</b> CRAOS8X-50667</p>	<p><b>Summary:</b> Statseeker monitoring tool no longer displays MAC address or VLAN name information for AOS switches. Specifically, the VLAN Name column is missing, and the OID dot1qVlanStaticName is not returning any data.</p> <p><b>Explanation:</b> Statseeker relies on the SNMP OID dot1qVlanStaticName (from the Q-BRIDGE-MIB) to map VLAN IDs to VLAN names. In previous AOS versions, this OID returned the expected output, allowing Statseeker to associate MAC addresses with VLAN names and switch ports. However, after upgrading to AOS 8.10.105.R02, running an SNMP walk on this OID results in a “No Such Instance currently exists” message. This indicates that the OID is missing or not implemented in the new software version.</p> <p> <a href="#">Click for Additional Information</a></p>
<p><b>Case:</b> <b>00804050</b> CRAOS8X-51183</p>	<p><b>Summary:</b> Following a wireless controller upgrade, several devices—including access points, VoIP phones, and wired clients—were unable to obtain IP addresses via DHCP. Clients sent DHCP Discover messages and the DHCP server responded with Offers, but the Offers did not reach the clients. Static IPs worked, and firmware rollback did not resolve the issue. The problem was isolated to a CORE switch (OS6900V48C8) acting as the DHCP relay.</p> <p><b>Explanation:</b> The DHCP relay was receiving Offer packets from the server but not forwarding them to clients, causing the DHCP process to fail. This behavior is linked to the use of a blocking socket by the relay, which sends packets to multiple DHCP servers. If one of the servers</p>

	<p>is unreachable and does not respond to ARP, the socket blocks while waiting for ARP resolution, delaying the relay process. Additionally, the Send-Q socket buffer size was set to 212480 bytes, which is smaller than the receive buffer, limiting the relay's capacity to handle multiple DHCP replies efficiently. These conditions together contributed to the failure in forwarding DHCP Offers to clients.</p> <p> <a href="#">Click for Additional Information</a></p>
<b>Case:</b> <b>00806211</b> CRAOS8X-51451	<p><b>Summary:</b>          A null static route (x.x.x.x/24 via 0.0.0.0) remains in the configuration even after an attempt to remove it using the CLI. The system reports that the route does not exist, yet it continues to appear in the configuration snapshot.</p> <p><b>Explanation:</b>          When the static route is deleted through the CLI, the system responds with an error indicating that the route does not exist in the running configuration. However, a snapshot of the configuration still lists the route, showing a discrepancy between the running state and the stored configuration. This issue has been reproduced in a lab environment and confirmed as a software defect.</p> <p> <a href="#">Click for Additional Information</a></p>

## 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
uos-mrp-v1.deb nos-mrp-v1.deb	MRP Application
*-ams-v#.deb *-ams-apps-v#.deb	AOS Micro Services Application
uosn-mpls-v5.deb uosn-sitemgr-v3.deb uosn-siteend-v2.deb yos-mpls-v5.deb yos-sitemgr-v3.deb yos-siteend-v2.deb	MPLS Application and Licensing
yos-nutanix-v3.deb	Nutanix Prism Plug-in Package
ovng-agent-v.1.10.deb	OmniVista Cirrus 10
kaos-sitemgr-v3.deb kaos-siteend-v2.deb	Licensing for SW-PERF for 6870
nos-pnet-v1.deb	Profinet Application
<ul style="list-style-type: none"> <li>- If a package is not committed it can result in image validation errors when trying to reload the switch.</li> <li>- Some packages are included as part of the AOS release and do not have to be installed separately.</li> <li>- Applications should be stopped prior to upgrading a package.</li> </ul>	

### 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
default	installed	default	
ams-apps	default	installed	default
mrp	8.7.R03-xxx	installed	/flash/working/pkg/mrp/install.sh

ams

## 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	CVE	CVSS
CRAOS8X-47683	CVE-2024-45490, CVE-2024-45491, CVE-2024-45492	CVSS 9.8
CRAOS8X-50688	CVE-2025-26465, CVE-2025-26466	CVSS 7.5