# Release Notes - Rev. A

## OmniSwitch 6465, 6560, 6860(E)/6865/6900

### Release 8.6R2

These release notes accompany release 8.6R2. These release notes provide important information on individual software features and hardware modules. Since much of the information in these release notes is not included in the hardware and software user manuals, it is important that you read all sections of this document before installing new hardware or loading new software.

**Note - The OS9900 is currently not supported in AOS Release 8.6R2.**
**(**The OS9900 is referenced in the 8.6R2 user guides and the release notes but is currently not a supported platform in AOS Release 8.6R2)

## Contents

## Related Documentation

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

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

## System Requirements

### Memory Requirements

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

| Platform | SDRAM | Flash |
|---|---|---|
| OS6465 | 1GB | 1GB |
| OS6560 | 2GB | 2GB |
| OS6560-24X4/P24X4 | 1GB | 1GB |
| OS6860(E) | 2GB | 2GB |
| OS6865 | 2GB | 2GB |
| OS6900-X Models | 2GB | 2GB |
| OS6900-T Models | 4GB | 2GB |
| OS6900-Q32 | 8GB | 2GB |
| OS6900-X72 | 8GB | 4GB |
| OS6900-V72/C32 | 16GB | 16GB |
| OS9900 | 16GB | 2GB |

### UBoot and FPGA Requirements

The software versions listed below are the MINIMUM required, except where otherwise noted. Switches running the minimum versions, as listed below, do not require any UBoot or FPGA upgrades. Use the '**show hardware-info**' command to determine the current versions.

Switches not running the minimum version required should upgrade to the latest UBoot 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 6465 – AOS Release 8.6.189.R02 (GA)

| Hardware | Minimum UBoot | Minimum FPGA |
|---|---|---|
| OS6465-P6 | 8.5.83.R01 | 0.10 |
| OS6465-P12 | 8.5.83.R01 | 0.10 |
| OS6465-P28 | 8.5.89.R02 | 0.7* |
| OS6465T-12 | 8.6.117.R01 | 0.4 |
| OS6465T-P12 | 8.6.117.R01 | 0.4 |
| **Note**: FPGA version 0.7 is optional to address issue CRAOS8X-12042. | | |

### OmniSwitch 6560 – AOS Release 8.6.189.R02 (GA)

| Hardware | Minimum Uboot | Minimum FPGA |
|---|---|---|
| OS6560-24Z24 | 8.5.22.R01 | 0.7 |
| OS6560-P24Z24 | 8.4.1.23.R02 | 0.6 (Minimum)<br>0.7 (Current)* |
| OS6560-24Z8 | 8.5.22.R01 | 0.7 |
| OS6560-P24Z8 | 8.4.1.23.R02 | 0.6 (Minimum)<br>0.7 (Current)* |
| OS6560-24X4 | 8.5.89.R02 | 0.4 |
| OS6560-P24X4 | 8.5.89.R02 | 0.4 |
| OS6560-P48Z16 (903954-90) | 8.4.1.23.R02 | 0.6 (Minimum)<br>0.7 (Current)* |
| OS6560-P48Z16 (904044-90) | 8.5.97.R04 | 0.3 |
| OS6560-48X4 | 8.5.97.R04 | 0.4 |
| OS6560-P48X4 | 8.5.97.R04 | 0.4 |
| OS6560-X10 | 8.5.97.R04 | 0.5 |
| **Note**: FPGA version 0.7 is only required to address issue CRAOS8X-7207. | | |

### OmniSwitch 6860(E) – AOS Release 8.6.189.R02 (GA)

| Hardware | Minimum Uboot | Minimum FPGA |
|---|---|---|
| OS6860/OS6860E (except U28) | 8.1.1.70.R01 | 0.9 |
| OS6860E-U28 | 8.1.1.70.R01 | 0.20 |
| OS6860E-P24Z8 | 8.4.1.17.R01 | 0.5 |

### OmniSwitch 6865 – AOS Release 8.6.189.R02 (GA)

| Hardware | Minimum Uboot | Minimum FPGA |
|---|---|---|
| OS6865-P16X | 8.3.1.125.R01 | 0.20 (minimum)<br>0.22 (current) |
| OS6865-U12X | 8.4.1.17.R01 | 0.23 |
| OS6865-U28X | 8.4.1.17.R01 | 0.11 (minimum)<br>0.12* |
| **Notes**:<br>FPGA version 0.12 is only required to address issue CRAOS8X-4150. | | |

**OmniSwitch 6900-X20/X40 – AOS Release 8.6.189.R02 (GA)**

| Hardware | Minimum UBoot | Minimum FPGA |
|---|---|---|
| CMM (if XNI-U12E support is not needed)<br>CMM (if XNI-U12E support is needed)<br>All Expansion Modules | 7.2.1.266.R02<br>7.2.1.266.R02<br>N/A | 1.3.0/1.2.0<br>1.3.0/2.2.0<br>N/A |

**OmniSwitch 6900-T20/T40 – AOS Release 8.6.189.R02 (GA)**

| Hardware | Minimum UBoot | Minimum FPGA |
|---|---|---|
| CMM (if XNI-U12E support is not needed)<br>CMM (if XNI-U12E support is needed)<br>All Expansion Modules | 7.3.2.134.R01<br>7.3.2.134.R01<br>N/A | 1.4.0/0.0.0<br>1.6.0/0.0.0<br>N/A |

**OmniSwitch 6900-Q32 – AOS Release 8.6.189.R02 (GA)**

| Hardware | Minimum UBoot | Minimum FPGA |
|---|---|---|
| CMM<br>All Expansion Modules | 7.3.4.277.R01<br>N/A | 0.1.8<br>N/A |

**OmniSwitch 6900-X72 – AOS Release 8.6.189.R02 (GA)**

| Hardware | Minimum Uboot | Minimum FPGA |
|---|---|---|
| CMM<br><br>All Expansion Modules | 7.3.4.31.R02<br><br>N/A | 0.1.10<br>N/A |

**OmniSwitch 6900-V72/C32 – AOS Release 8.6.189.R02 (GA)**

| Hardware | ONIE | CPLD |
|---|---|---|
| OS6900-V72 | 2017.08.00.01 | CPLD 1 – 0x5<br>CPLD 2 - 0x6<br>CPLD 3 – 0x8 |
| OS6900-C32 | 2016.08.00.03 | CPLD 1 – 0xA<br>CPLD 2 – 0xB<br>CPLD 3 – 0xB |
| **Note**: The OS6900-V72/C32 uses a different image file (Yos.img) than all other OS6900 models (Tos.img). Be sure to use the appropriate image file for the platform. | | |

### OmniSwitch 9900 – AOS Release 8.6.###.R02 (GA)

| Hardware | Coreboot-uboot | Control FPGA | Power FPGA |
|---|---|---|---|
| OS99-CMM | 8.3.1.103.R01 | 2.3.0 | 0.8 |
| OS9907-CFM | 8.3.1.103.R01 | - | - |
| OS99-GNI-48 | 8.3.1.103.R01 | 1.2.4 | 0.9 |
| OS99-GNI-P48 | 8.3.1.103.R01 | 1.2.4 | 0.9 |
| OS99-XNI-48 (903753-90)<br>OS99-XNI-48 (904049-90) | 8.3.1.103.R01<br>8.6.261.R01 | 1.3.0<br>1.4.0 | 0.6<br>0.7 |
| OS99-XNI-U48 (903723-90)<br>OS99-XNI-U48 (904047-90) | 8.3.1.103.R01<br>8.6.261.R01 | 2.9.0<br>2.10.0 | 0.8<br>0.8 |
| OS99-GNI-U48 | 8.4.1.166.R01 | 0.3.0 | 0.2 |
| OS99-CNI-U8 | 8.4.1.20.R03 | 1.7 | N/A |
| OS99-XNI-P48Z16 | 8.4.1.20.R03 | 1.4 | 0.6 |
| OS99-XNI-U24 | 8.5.76.R04 | 1.0 | 0.8 |
| OS99-XNI-P24Z8 | 8.5.76.R04 | 1.1 | 0.7 |
| OS99-XNI-U12Q | 8.6.117.R01 | 1.5.0 | N/A |
| OS99-XNI-UP24Q2 | 8.6.117.R01 | 1.5.0 | N/A |

## [IMPORTANT] *MUST READ*: AOS Release 8.6R2 Prerequisites and Deployment Information

### General Information

- The OS9900 is currently not supported in AOS Release 8.6R2. The OS9900 is referenced in the 8.6R2 user guides and the release notes but is currently not a supported platform in AOS Release 8.6R2.
- Early availability features are available in AOS and can be configured. However, they have not gone through the complete AOS validation cycle and are therefore not officially supported.
- Please refer to the Feature Matrix in Appendix A for detailed information on supported features for each platform.
- Prior to upgrading please refer to Appendix C for important best practices, prerequisites, and step-by-step instructions.
- Some switches that ship from the factory will default to VC mode (requiring a vcboot.cfg configuration file) and attempt to run the automatic VC, automatic remote configuration, and automatic fabric protocols. Please note that since the switches default to VC mode, automatic remote configuration does not support the downloading of a 'boot.cfg' file, only the 'vcboot.cfg' file is supported.
- Some switches may ship from the factory with a diag.img file. This file is for internal switch diagnostic purposes only and can be safely removed.

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

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

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

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

  **Note:** OS6560-P48Z16 (904044-90) - This is a new version of the OS6560-P48Z16 which does not have the link aggregation limitation mentioned above. The model number (OS6560-P48Z16) remains the same for both versions, only the part number can be used to differentiate between the versions.

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

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

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

- MACsec is now supported on ports 33-48 of the 6560-(P)48X4. CRAOS8X-7910 was resolved in 8.6R1.

- Deprecated Features / Functionality
  - EVB (8.5R4) - 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 (8.5R4) - 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

- DHCPv6 Guard (8.6R1) - Configuration via an IPv6 interface name is deprecated in 8.6.R1. Commands entered using the CLI must use the new '**ipv6 dhcp guard vlan** *vlan-id*' format of the command. The old format will still be accepted if present in a vcboot.cfg to preserve backwards compatibility.

- IP Helper (8.6R1) - The '**ip helpe**r' 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 - (8.6R1) - The vlan-priority and drop-eligible parameters have been deprecated from all SAA commands beginning in 8.6R1.

- Distributed ARP (8.6R2) - Beginning 8.6R2 distributed ARP is no longer supported.

- WRED (8.6R2) - Beginning in 8.6R2 WRED is no longer supported.

- QoS (8.6R2) - Beginning in 8.6R2 the 'qos dscp-table' command is no longer supported.

- NTP (8.6R2) - The **ntp** parameter for the '**ip service source-ip**' command was deprecated in 8.5R4. Support has been added back in 8.6R2.

## Licensed Features

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

| | Data Center License Required |
|---|---|
| | OmniSwitch 6900 |
| Data Center Features | |
| DCB (PFC,ETS,DCBx) | Yes |
| FIP Snooping | Yes |
| FCoE VXLAN | Yes |
| **Note**: All other platforms, including the OS6900-V72/C32, do not support these Data Center features. | |

| | License Required | | | |
|---|---|---|---|---|
| | OS6465 | OS6560 | OS6860 | OS9900 |
| Licensed Features | | | | |
| MACsec (OS-SW-MACSEC) | Yes | Yes | Yes | Yes |
| 10G support (OS6560-SW-PERF) | No | Yes* | No | No |
| ***10G license is optional for ports 25/26 (OS6560-24X4/P24X4) and ports 49/50 (OS6560-48X4/P48X4). Ports support 1G by default. | | | | |

## ALE Secure Diversified Code

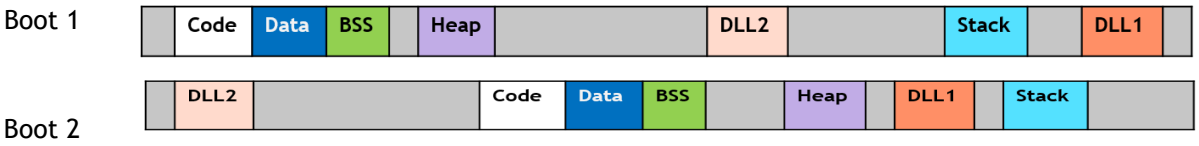
Alcatel-Lucent Enterprise provides network equipment that is hardened in conjunction with an independent 3rd party organization. ALE secure diversified code promotes security and assurance at the network device level using independent verification and validation of source code and software diversification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

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

**Software Diversification**

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

**ASLR**




Please contact customer support for additional information.

## New / Updated Hardware Support

The following new hardware is being introduced in this release.

**SFP-10G-LRM**
OmniSwitch 6560 support has been added for this transceiver beginning in 8.6R2. This transceiver is supported on the following models and ports:

- OS6560-48X4/P48X4
  - Ports 49-50 with OS6560-SW-PERF applied.
  - Ports 51/52.
- OS6560-P48Z16 (904044-90)
  - Ports 49-52.
- OS6560-X10
  - Ports 1-8.

**SFP-1G-T** - This transceiver is now supported on the OS6465T, OS6560, OS6860, OS6900, and OS9900 models.
**SFP-10G-T** - This transceiver is now supported on the OS6900-V72.

## New Software Features and Enhancements

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

### 8.6R2 New Feature/Enhancements Summary

| Feature | Platform |
|---|---|
| **Management / NMS Related Features** | |
| IoT Device Profiling -Iintegration with OV | 6465, 6560, 6860, 6865, 6900, 6900-V72/C32, 9900 |
| Webview 2.0 | 6465, 6560, 6860, 6865, 6900, 6900-V72/C32, 9900 |
| Webview Infrastructure for MQTT | 6465, 6560, 6860, 6865, 6900, 6900-V72/C32, 9900 |
| Webview in Chinese | 6465, 6560, 6860, 6865, 6900, 6900-V72/C32, 9900 |
| AOS Micro Services (AMS) - Broker Auto-assignment) | 6465, 6560, 6860, 6865, 6900, 6900-V72/C32, 9900 |
| Remote Configuration Download (RCL) | 6900-V72/C32 |
| Remote Chassis Detection (RCD) | 6860E |
| USB Adapter with Bluetooth Technology | 6465, 6560, 6865, 6900-V72/C32 |
| Swlog Clear Command | 6465, 6560, 6860, 6865, 6900, 6900-V72/C32, 9900 |
| Package Manager Support | 6465, 6560, 6860, 6865, 6900, 6900-V72/C32, 9900 |
| | |
| **Service / Access port / UNP Related Features** | |
| SPB L3VPN Inline Front-panel Loopback (two-pass) | 6900-V72/C32 |
| UNP VXLAN Support on OS6900-V72 | 6900-V72/C32 |
| SPB over VxLAN Support for Point-to-Point Connections | 6860, 6865, 6900, 6900-V72/C32, 9900 |
| SAA SPB Using 1-second Interval on 9900 | 9900 |
| | |
| **DHCP / UDP Related Features** | |
| DHCP Snooping (V4) | 6900-V72/C32 |
| DHCP Snooping (V6) | 6900-V72/C32 |
| IP Source Filtering (ISF) (V4) | 6900-V72/C32 |
| IP Source Filtering (ISF) (V6) | 6900-V72/C32 |
| | |
| **Layer 3 / Multicast Related Features** | |
| Anycast RP | 6860, 6865, 6900, 9900 |
| OSPF over Services: Display Service ID Instead of VLAN ID in Show Outputs | 6900-V72/C32, 9900 |
| Increase OSPF Interfaces to 8 on OS6560 | 6560 |
| BGP Peering (Class-E routes) | 6860, 6865, 6900, 6900-V72/C32, 9900 |
| | |
| **Security Related Features** | |
| Console Disable Command | 6465, 6560, 6860, 6865, 6900, 6900-V72/C32, 9900 |
| Kerberos / Windows Active Directory Logon Snooping | 6560, 6860, 6865, 6900, 6900-V72/C32, 9900 |
| AG L3 functionality (VLAN Domain) | 6900-V72/C32 |
| AG User Scalability Improvement) | 6465, 6560, 6860, 6865, 6900, 6900-V72/C32, 9900 |
| Support New Command to Install License | 6560 |
| | |
| **PoE Related Features** | |
| OS6560 802.3bt Type 3/4 Support | 6560 |
| | |

| Feature | Platform |
|---|---|
| **Virtual Chassis Related Features** | |
| Auto-VFL | 6900-V72/C32 |
| Auto-VC | 6900-V72/C32 |
| | |
| **Additional Features** | |
| LLDP Mixed Mode per Port | 6465, 6560, 6860, 6865, 6900, 6900-V72/C32, 9900 |
| Loopback Detection | 6900-V72/C32 |
| HAVLAN OS6900-V72/C32 | 6900-V72/C32 |
| Interface Details "new" | 6465, 6560, 6860, 6865, 6900 |
| DDM Information Not Displayed When Link is Down on Remote or Local | 6465, 6860, 6865 |
| LBD Difference Between Global and Per Port Configuration | 6465, 6560, 6860, 6865, 6900, 6900-V72/C32, 9900 |
| L2CP Statistics | 6465 |
| L2CP | 6860, 6865 |
| NTP Max Associations from 128 to 512 | 6465, 6560, 6860, 6865, 6900, 6900-V72/C32, 9900 |
| Validation of UNP and MVRP Compatibility | - |
| Determine Port Type Fiber/Copper | 6465, 6560, 6860, 6865, 6900, 6900-V72/C32, 9900 |
| | |
| **Early Availability / Internal Features** | |
| ISF support on X72, Q32 with splitter | 6900-X72/Q32 |
| Ethernet OAM OS6900-V72/C32 | 6900-V72/C32 |

## Management / NMS Related Features

### IoT Device Profiling - Integration with OV

In this enhancement for IoT Device Profiling, OmniVista runs the device profiler engine and the enforcement engine, which triggers a notification back to the switch with following information to be used for UNP enforcement.

- Mac-address [Index of the SNMP table]
- Device-Name
- Device-Type
- UNP-Profile

### Webview 2.0 and Chinese Translation

In 8.6R02, for continuity purposes, WebView 2.0 will be available for users to access, along with older WebView. The older WebView version will be deprecated in an upcoming release. WebView 2.0 is packaged into a Debian package that can be extracted and installed on the switch. This will allow upgraded versions of WebView to be installed on the switch without having to upgrade AOS software or reboot the switch. Support for simplified Chinese language is added in WebView 2.0. The Chinese language option can be selected from the language drop down box in WebView 2.0.

There is a single WebView 2.0 package for all platforms, the package can be downloaded from the Service & Support website. The package name will be "*package-webview-8.6.R02-*.deb*", where * stands for the build number.

To install the WebView 2.0 package, copy the package to the ***/flash/working/pkg*** directory and run the following command (this example uses build 168):

```
-> pkgmgr install package-webview-8.6.R02-168.deb
```

In some cases a memory threshold message may be displayed. The memory threshold can be increased using the 'health memory threshold' command, for example:

```
-> health memory threshold 85
```

Once verified that the new WebView 2.0 package is working properly, it can be commited making it available even after a system reboot.

```
-> pkgmgr commit
```

The following CLI commands are associated with this feature:

- pkgmgr install
- pkgmgr commit
- pkgmgr list

### AOS Micro Services (AMS) Enhancement - Broker Auto-assignment

As part of 8.6 R01, the AMS feature is launched manually with the broker IP/port specified in config-sync.cfg file. In 8.6R2 the broker IP/port can be automatically configured using the DHCP VSO option-43 and launch the required modules automatically. The following CLI commands are associated with this feature:

- appmgr start | stop | restart
- appmgr list
- appmgr commit

### Remote Configuration Download (RCL) OS6900-V72/C32

RCL is supported on the OS6900-V72/C32 beginning in 8.6R2.

**Remote Chassis Detection**

Remote Chassis Detection (RCD) is supported on the OS6860E models beginning in 8.6R2. In a mixed VC of OS6860 and OS6860E, RCD is not supported.

**USB Adapter with Bluetooth Technology**

Configuring an OmniSwitch using a USB Adapter with Bluetooth Technology is now supported on an OS6465, OS6560, OS6860 (previously supported), OS6865 and OS6900-V72/C32 beginning in 8.6R2. The following USB adapters with Bluetooth technology are supported:

- TRENDnet TBW-107UB - Network adapter - USB - Bluetooth 2.1 EDR - Class 2
- ZOOM 4314 USB Adapter - Network adapter - USB - Bluetooth 2.1 EDR - Class 1
- Belkin USB 4.0 Bluetooth Adapter - Network adapter - USB - Bluetooth 4.0
- IOGEAR Bluetooth 4.0 USB Micro Adapter Multi-Language Version - Network adapter - USB - Bluetooth 4.0 - Class 2
- SMK-Link Electronics Nano Bluetooth Dongle 4.0 LE + EDR - Network adapter - USB 2.0 – Bluetooth 4.0 EDR
- TRENDNET 4.0, IOGEAR 4.0 (100m range)
- ASUS USB-BT400 Bluetooth 4.0
- KINIVO BD-400 Bluetooth 4.0
- TARGUS Bluetooth 4.0
- DG40S Avantree Bluetooth 4.0
- SABRENT Bluetooth 4.0
- TP-LINK UB400  Bluetooth 4.0
- ROCKETEK Bluetooth 4.0

The following CLI commands are associated with this feature:

- bluetooth admin-state
- bluetooth transmit-power

**Swlog clear all**

The regular 'swlog clear' command only clears the contents of the switch logging file. To clear both the contents and event log of the switch logging files the 'all' option has been introduced. The following CLI command is associated with this feature:

- swlog clear all

**Package Manager Support**

The Package Manager framework provides a generic infrastructure to install the AOS or non-AOS/ Third party Debian packages. Package Manager framework is implemented in order to modularize AOS applications, thereby to install or remove Debian packages and also to start, stop and remove the applications present in the packages. The following CLI commands are associated with this feature:

- pkgmgr {install | remove | verify}
- pkgmgr list
- pkgmgr commit

## Service / Access port / UNP Related Features

### SPB L3VPN Two-pass Inline Routing Using Front Panel Loopback

In addition to the OmniSwitch 9900 support for L3 VPN inline routing, the following inline routing functionality is now supported on the OmniSwitch 6900-V72 and OmniSwitch 6900-C32:

- Two-pass inline routing using front-panel ports. An L3 VPN interface is defined through the configuration of a front-panel port to run in loopback mode.
- Bandwidth for the two-pass processing is taken from the front panel port.
- Multiple front-panel loopback ports can be combined into a static loopback link aggregate for redundancy and to increase bandwidth.

Unlike the external loopback option, two-pass inline routing with front-panel ports does not require a physical cable and only uses one front-panel port to provide the two-pass loopback function. The following CLI commands are associated with this feature:

- interfaces loopback
- show interfaces (“loopback mode” field added)
- linkagg static agg loopback
- show linkagg (command output modified for loopback interfaces)

### UNP VXLAN Support on OS6900-V72/C32

This enhancement adds for VXLAN UNP profile support for the OS6900-V72/C32 in head-end only mode.

### SAA on 9900

SAA SPB support is extended to OmniSwitch 9900.

When SAA processes an iteration of a session, it will compare the results against the following criteria to see if an SNMP trap should be sent. A trap with the session name is sent if:

- At least one packet is lost.
- Warning: Average RTT/Jitter crosses 90% of threshold.
- Critical: Average RTT/Jitter at or above threshold.

The following CLI commands are associated with this feature:

- saa spb
- saa spb reset
- saa spb flush
- show saa spb

## DHCP / UDP Related Features

### DHCP Snooping (V4) OS6900-V72/C32

DHCPv4 snooping is supported on the OS6900-V72/C32 beginning in 8.6R2.

### DHCP Snooping (V6)

DHCPv6 snooping is supported on the OS6900-V72/C32 beginning in 8.6R2.

### ISF (V4) OS6900-V72/C32

IPv4 source filtering is supported on the OS6900-V72/C32 beginning in 8.6R2.

**ISF (V6) OS6900-V72/C32**

IPv6 source filtering is supported on the OS6900-V72/C32 beginning in 8.6R2.

## Layer 3 / Multicast Related Features

**Anycast RP**

Anycast RP provides load sharing and redundancy in Protocol Independent Multicast Sparse Mode (PIM-SM) networks. Anycast-RP is a mechanism that ISP-based backbones use to get fast convergence when a PIM rendezvous point (RP) router fails.

Anycast RP introduces the concept where the same IP address (RP Address) is configured on two or more routers serving as the RP. This address is advertised by the IGP. Other routers will select any of these routers based on the best path to the RP address. In case of a failure, the convergence is the same as the IGP. Both IPv4 and IPv6 addressing is supported.

Anycast will be supported with PIM-SM only. The following CLI commands are associated with this feature:

- ip pim anycast-rp
- show ip pim anycast-rp
- ipv6 pim anycast-rp
- show ipv6 pim anycast-rp

**OSPF Over Services: Display Service ID Instead of VLAN ID in Show Outputs**

When inline routing over the services was introduced, service information was not incorporated into some of the show commands of the routing protocols such as OSPF. Currently the show commands display the VLAN ID in all the relevant show commands. This enhancement incorporates the Domain Name and Domain ID into the show command outputs instead of just Vlan. The Domain Name can be VLAN, Service or Tunnel (IP Tunnels) and Domain ID can be VLAN ID or Service ID. The IP tunnels operate on the IP routing table and they don't have their own device like vlan or service, so the domain ID will be displayed as "N/A" for IP tunnels. The following CLI commands are associated with this feature ("Domain Name" and "Domain ID" fields added):

- show ip ospf interface
- show ip ospf neighbor
- show ip ospf routes
- show ip rip interface

**OS6560 OSPF Interfaces Increase**

The number of OSPF interfaces supported on an OS6560 is being increased from 2 to 8 in 8.6R2.

**BGP Peering (Class-E routes)**

BGP peering sessions are no longer torn down when receiving invalid class-E BGP prefixes.

## Security Related Features

**Console Disable Command**

Console session helps in security-sensitive networks and deployments. The option manages the access to the switch configuration shell through the console port.

The feature allows the following operations:

- Enable or disable the access to the switch configuration shell through the console port.
- Allows storing the configuration in the configuration file so that even after a reboot, the access to the switch remains through console port.

The following CLI commands are associated with the feature:

- aaa session console
- show aaa session console config

**Kerberos/Active Directory Logon Snooping**

Kerberos snooping will snoop the user information and can identify if a system has successfully logged on to a domain. Kerberos authentication is handled by external Kerberos server/KDC. Kerberos agent is placed between the client and the Kerberos server (or KDC). Upon receiving the Kerberos Request PDU, Kerberos agent relays and snoop the authentication frames between the user/client and the Kerberos server. Kerberos agent maintains the database of the clients i.e. the client info (client name, Source Mac, IP and domain name), authenticated state, port no, on which client is attached; qos-policy-list that needs to be applied after authentication process is over.

After receiving the response to the request packet from KDC, Kerberos agent snoop the reply packet from KDC and maintains the authentication state of the client (i.e. authentication pass/fail). Once the client has been authenticated then a qos-policy-list needs to be applied in hardware l2 table (if qos-policy-list configuration exists for Kerberos). The following CLI commands are associated with this feature:

- unp profile kerberos-authentication
- kerberos inactivity-timer
- kerberos ip-address ip_address port
- kerberos server-timeout
- kerberos authentication-pass policy-list-name
- kerberos authentication-pass domain policy-list-name
- clear kerberos statistics
- show kerberos configuration
- show kerberos users
- show kerberos statistics

**Access Guardian L3 Functionality (VLAN Domain)**

This enhancement adds support BYOD, user roles, Captive Portal and LTP (Location/Time policy) to all OS6900 models.

**Access Guardian User Scalability Improvements**

The following table documents the maximum number of UNP users per chassis and VC for each platform beginning in 8.6R2.

| Platform | Chassis Maximum | VC Maximum |
|---|---|---|
| OS6465 | 80 | 320 |
| OS6560 | 256 | 2K |
| OS6860 | 2K | 2K |
| OS6865 | 2K | 2K |
| OS6900-all models | 2K | 2K |

| | | |
|---|---|---|
| OS9900 | 1K | 2K |

**Support New Command to Install License**

A new parameter 'key' has been introduced in the license apply command which allows installation of the license onto the switch by entering the individual license key. The following CLI commands are associated with this feature:

- license apply key

**PoE Related Features**

**OS6560 802.3bt Type 3/4 Support**

IEEE 802.3bt support is being added to the OmniSwitch 6560. IEEE 802.3bt adds support for Type 3 and Type 4 PoE devices and an additional 4 classes (class 5 to class 8) with single detection and class 1D to 5D with dual detection, which can support up to 95 watts of power over 4-pairs of the ethernet cable. The following CLI commands are associated with this feature:

- lanpower slot 802.3bt

**Virtual Chassis Related Features**

**Auto-VFL and Auto-VC for OS6900-V72/C32**

This feature adds support for auto-VFL and auto-VC capability for a VC-of-2 OS6900-V72/C32 models. (Last 5 ports are default auto-VFL ports)

**Additional Features**

**LLDP mixed mode per port**

Provides an "inbound" option to specify a separate action for 802.1AB tagged and untagged traffic in a VLAN Stacking UNI L2 profile and a service manager L2 profile. The following CLI commands are associated with the feature:

Service Manager commands :
- service l2profile inbound 802.1ab
- show service l2profile ("802.1AB Both", "802.1AB Tagged", and "802.1AB Untagged" fields added)

VLAN Stacking commands:
- ethernet-service uni-profile inbound 802.1ab
- show ethernet-service uni-profile ("802.1AB Both", "802.1AB Tagged", and "802.1AB Untagged" fields added)

**Loopback Detection**

This enhancement adds support for Loopback Detection (LBD) on the OS6900-V72/C32 beginning in 8.6R2.

**HAVLAN OS6900-V72/C32**

This enhancement adds support for High Availability VLANs (HA VLAN) on the OS6900-V72/C32 beginning in 8.6R2.

**Interface Details "new"**

This enhancemen to the ‘show interfaces’ command displays the reason the operational status of a port is down by adding the 'Port-Down / Violation Reason' field to the output . This enhancement only displays the software reason that caused the operational status of the port to go to down such as due to LBD, LPS, or UDLD. If the port is down due to a physical fault, ‘None’ will be displayed. This enhancement is only for physical ports, for information on a link aggregate the 'show violation' command must be used. The following CLI commands are associated with the feature:

- show interfaces (Port-Down/Violation Reason) field added.

**DDM information not displayed when links is down on remote or local**

This enhancement allows for the DDM information to be displayed even when the local or remote end is down. Prior to the enhancement no DDM information would be displayed if either side was down. The following CLI commands are associated with the feature:

- show interfaces ddm

**LBD Difference between Global and Per Port Configuration**

In previous releases, when loopback detection was enabled globally and per port on both the devices (Device -1 and Device -2), which are connected back to back, the loop between two devices was not detected.

The LBD frame would carry a reserved multicast MAC address (0x01-20-DA-02-01-71) as the destination MAC address, and the source MAC address of the LBD packet was the MAC address of the port from which it is getting generated. The hardware rule would trap the packet whenever the destination MAC address of the packet was reserved multicast MAC address (0x01-20-DA-02-01-71).

In this case, when a LBD Frame is generated from Device -1 and reaches the Device -2 (LBD is enabled globally and for ports on both the devices) and the Destination MAC of the LBD Frame received at Device -2 is reserved multicast MAC, the packet will be trapped to the CPU. Then the packet will be processed and the Bridge ID will be verified. Since the bridge in the LBD frame does not matches the Device -2’s Bridge ID, the packet will be dropped. Since the packet is dropped at device -2 itself, it will not reach Device -1 and loop will not be etected.

After this enhancement, the source MAC address of the LBD packet will carry the Switch’s Base MAC instead of the MAC address of the port, and destination MAC address would be the reserved multicast MAC address (0x01-20-DA-02-01-71).

**L2CP Statistics**

This enhancment displays statistics of control protocol tunneling frames in the context of Ethernet Services UNI/NNI ports:

- RX frame statistics at UNI port level
- TX frame statistics at UNI port level
- RX frame statistics at NNI port level
- RX frame statistics at UNI profile level

The following CLI commands are associated with the feature:

- 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

**L2CP**

This enhancement adds OS6860 and OS6865 support for custom L2 protocols.

**NTP Max Associations**

Maximum number of associations increased from 128 to 512 beginning in 8.6R2. The following CLI commands are associated with the feature:

- ntp max-associations

**Determine Port Type Fiber/Copper**

A new row has been added to the 'show interface chassis/slot/port' command named 'interface type', possible values are copper, fiber, combo-copper or combo-fiber. If type is fiber or combo-fiber the SFP/XFP field will display the type of transceiver installed. The following CLI commands are associated with the feature:

- show interface

**EA: ISF support on X72/Q32 with splitter**

Currently until 86R1 the dhcp-snooping and ISF are limited to the 64 ports per NI for these platforms. But the 6900-X72/Q32 have more than 64 ports. Dhcp-snooping and ISF support has been extended to 128 ports per NI to support the X72/Q32 with splitter ports. The scalabilty numbers per NI are the same as OS6900 earlier.

## 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-8818 | Issue with using USB sticks for rescue. | To perform USB disaster recovery in OS6900-X models, switch should be loaded with factory default uboot version 7.2.1.266.R02. |
| CRAOS8X-10570 | Error messages are displayed on the console when a port is disabled on one side of a P2P connection. | Toggle the admin state of the enabled port. |
| CRAOS8X-10420 | "On an OS6860 and OS6865, traffic for a HAVLAN cluster is also forwarded to the non-HAVLAN cluster port. | There is no known workaround at this time. |
| CRAOS8X-11118 | On an OS6900-X72, the 1000BaseT SFP interface becomes "up" almost immediately after booting. | There is no known workaround at this time. |
| CRAOS8X-11263 | On a OS6465-P28 model, the mac aging value cannot be set larger than 414 seconds. | There is no known workaround at this time. |
| CRAOS8X-12735/14680 | On an OS6465 "fdbmgr1 hal ERR msgs" may be seen on the console during bootup due to a mismatch of MAC entries between hardware and software. | This issue does not appear to affect traffic flow. The error log shows which MAC may have been impacted, any issues can resolved with a flush of the MAC address. |
| CRAOS8X-14246 | Kerberos policy changes will not be reflected for MACs learned after MAC move. MAC learned on new port will be learned with same Kerberos policy as it was before policy change. | This is because Kerberos transaction was not seen on the new port. If user does kerberos transaction on new port MAC be learned with new kerberos policy. |
| CRAOS8X-14911 | UNP user learning fails when the radius unp-profile-precedence is set to tunnel-private-group-id. Sometimes when mac addresses are flushed they do not get removed from hardware and user learning fails. | Introduce a 2-3 seconds delay before sending user learning packets resolves the issue. |
| CRAOS8X-14920 | OS6560-X10: dynamic macsec port doesn't join linkagg after interface toggle. | Remove macsec configuration and reapply the macsec configuration on the port. For example:<br>- interfaces port 3/1/5 macsec admin-state disable<br>- no interfaces port 3/1/5 macsec<br>- interfaces port 3/1/5 macsec mode dynamic key-chain 1 server-priority 8 transmit-interval 3 encryption<br>- interfaces port 3/1/5 macsec admin-state enable |

| | | |
|---|---|---|
| CRAOS8X-15069 | On stackable platforms, the u-boot update is failing with "ni" option. | The "ni" option is not valid for non-chassis based platforms. Use the "cmm" option for stackable platforms." |

**QoS**

| PR | Description | Workaround |
|---|---|---|
| CRAOS8X-2081 | On an OS6560 10% of P7 traffic loss is seen when P0 traffic is oversubscribed with max Egress-bandwidth. | There is no known workaround at this time. |
| CRAOS8X-4424 | With color-only policy action configured, egress queues are not honoring the color marking and packet drop is observed and expected traffic rate is not achieved. | There is no known workaround at this time. |
| CRAOS8X-10498 | "qos port 1/1/3 maximum ingress-bandwidth 80M" doesn't work after vc-takeover and reload because it gets overwritten by default ingress-bandwidth of a port. | Configure ingress-bandwidth through "interfaces port c/s/p ingress-bandwidth mbps <num> burst <num>" instead of "qos port c/s/p maximum ingress-bandwidth <num>". |

**Service Related**

| PR | Description | Workaround |
|---|---|---|
| CRAOS8X-3941 | Sometimes SDP entry is not getting created for tagged traffic when the system-default service base is 512 and service-mod is 256. | There is no known workaround at this time. |
| CRAOS8X-4124 | Traffic is not tunneled over L2GRE service when sending traffic from edge to aggregate switch via another edge switch where SAP/loopback port on aggregate switch is configured as static linkagg. | There is no known workaround at this time. |
| CRAOS8X-7428 | IPMS Proxy is not supported on a service. | There is no known workaround at this time. |
| CRAOS8X-12513 | When 2048 IGMP groups were sent over SPB service, only 1025 IGMP groups were received with 1024 SAPs per service configured on the edge switch. Seen with large amount of SAPs (>1K) configured on same port. | Distribute the SAPs across different ports. |
| CRAOS8X-15386 | Unable to add lag to service access port if lag has been previously configured to be a network port | 1. Remove the Management IP interface on SPB Control Vlan. |

| | | |
|---|---|---|
| | | 2. Remove the SPB ISIS Interface on LinkAgg/Physical Port<br><br>3. Configure the Service Access port<br><br>4. Configure the Management IP interface on SPB Control Vlan. |
| CRAOS8X-15548 | After 2nd VC takeover the SAP port does not recover from shutdown violation when violation is cleared using clear violation command. | There is no known workaround at this time. |

**Virtual Chassis**

| PR | Description | Workaround |
|---|---|---|
| CRAOS8X-3877 | On 6900 and 6900-V72, untagged packets are mirrored as tagged traffic when when monitored port is across VC chassis. On standalone box, monitored egress traffic is tagged. | Use port mirroring. |
| CRAOS8X-15509 | RTT values may be incorrect when configuring SAA with ethoam loopback on a link aggregate that has member ports spread across different elements of a VC. | Ensure that the system time is synchronized across all elements of the VC when SAA ethoam loopback is configured. |

## Hot Swap/Redundancy Feature Guidelines

### Hot Swap Feature Guidelines

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

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

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

**OS6900 Hot Swap/Insertion Compatibility**

| Existing Slot | Hot-Swap/Hot-Insert compatibility |
|---|---|
| Empty | All modules can be inserted |
| OS99-CMM | OS99-CMM |
| OS9907-CFM | OS9907-CFM |
| OS99-GNI-48 | OS99-GNI-48 |
| OS99-GNI-P48 | OS99-GNI-P48 |
| OS99-XNI-48 | OS99-XNI-48 |
| OS99-XNI-U48 | OS99-XNI-U48 |
| OS99-XNI-P48Z16 | OS99-XNI-P48Z16 |

| | |
|---|---|
| OS99-CNI-U8 | OS99-CNI-U8 |
| OS99-GNI-U48 | OS99-GNI-U48 |
| OS99-XNI-U24 | OS99-XNI-U24 |
| OS99-XNI-P24Z8 | OS99-XNI-P24Z8 |
| OS99-XNI-U12Q | OS99-XNI-U12Q |
| OS99-XNI-UP24Q2 | OS99-XNI-UP24Q2 |

**OS9900 Hot Swap/Insertion Compatibility**

### Hot Swap Procedure

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

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

### VC Hot Swap / Removal Guidelines

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

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

## Technical Support

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

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

**Email:** ebg_global_supportcenter@al-enterprise.com

**Internet:** Customers with service agreements may open cases 24 hours a day via the support web page at: businessportal2.alcatel-lucent.com. Upon opening a case, customers will receive a case number and may review, update, or escalate support cases on-line. Please specify the severity level of the issue per the definitions below. For fastest resolution, please have hardware configuration, module types and version by slot, software version, and configuration file available for each switch.

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

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

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

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

## Third Party Licenses and Notices

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

## Appendix A: Feature Matrix

The following is a feature matrix for AOS Release 8.6R2.

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 | 6465 | 6560 | 6860(E) | 6865 | 6900 | 6900-V72/C32 | 9900 |
|---|---|---|---|---|---|---|---|
| **Management Features** | | | | | | | |
| Apple Netboot Support with DHCP Snooping or Relay | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 |
| AOS Micro Services (AMS) | 8.6R1 | 8.6R1 | 8.6R1 | 8.6R1 | 8.6R1 | 8.6R1 | 8.6R1 |
| Automatic Remote Configuration Download (RCL) | 8.5R1 | Y | Y | Y | Y | 8.6R2 | Y |
| Automatic/Intelligent Fabric | 8.5R1 | Y | Y | Y | Y | N | Y |
| Automatic VC | N | Y | Y | Y | Y | 8.6R2 | N |
| Bluetooth - USB Adapter with Bluetooth Technology | 8.6R2 | 8.6R2 | Y | 8.6R2 | N | 8.6R2 | N |
| Console Disable | 8.6R2 | 8.6R2 | 8.6R2 | 8.6R2 | 8.6R2 | 8.6R2 | 8.6R2 |
| Dying Gasp | Y | Y | Y | Y | N | N | N |
| Dying Gasp (EFM OAM / Link OAM) | 8.6R1 | 8.6R1 | 8.6R1 | 8.6R1 | N | N | N |
| EEE support | N | N | Y | Y | Y | N | N |
| Embedded Python Scripting / Event Manager | 8.5R1 | Y | Y | Y | Y | N | N |
| IP Managed Services | N | N | Y | Y | Y | 8.5R2 | Y |
| In-Band Management over SPB | N | N | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 |
| ISSU | N | N | Y | Y | Y | 8.5R2 | Y |
| NAPALM Support | 8.5R1 | 8.5R1 | 8.5R1 | 8.5R1 | 8.5R1 | N | N |
| NTP - Version 4.2.8.p11. | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 |
| OpenFlow | N | N | Y | N | Y | N | N |
| OV Cirrus – Zero touch provisioning | Y | Y | Y | Y | Y | N | N |
| OV Cirrus – Configurable NAS Address | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 |
| OV Cirrus – Default Admin Password Change | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 |
| OV Cirrus – OS6900-V72/C32 Managed | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 |
| Readable Event Log | 8.6R1 | 8.6R1 | 8.6R1 | 8.6R1 | 8.6R1 | 8.6R1 | 8.6R1 |
| Remote Chassis Detection (RCD) | N | N | 8.6R2 | N | Y | N | Y |
| SAA | 8.5R1 | N | Y | Y | Y | N | N |
| SAA SPB | N | N | Y | Y | Y | N | 8.6R2 |
| SAA UNP | Y | N | Y | Y | Y | N | N |
| SNMP v1/v2/v3 | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| UDLD | 8.5R1 | Y | Y | Y | Y | N | EA |
| USB Disaster Recovery | 8.5R1 | Y | Y | Y | Y | N | Y |
| USB Flash | 8.5R1 | Y | Y | Y | Y | N | N |
| USB as Backup and Restore | 8.5R1 | 8.5R1 | 8.5R1 | 8.5R1 | N | N | Y |
| USB – Encrypted | 8.5R2 | N | N | N | N | N | N |

| Feature | 6465 | 6560 | 6860(E) | 6865 | 6900 | 6900-V72/C32 | 9900 |
|---|---|---|---|---|---|---|---|
| Virtual Chassis (VC) | 8.5R2 | Y | Y | Y | Y | 8.5R2 (VC of 2) | Y |
| Virtual Chassis TCN | 8.5R2 | 8.5R2 | 8.5R2 | 8.5R2 | 8.5R2 | 8.5R2 | 8.5R2 |
| Virtual Chassis Split Protection (VCSP) | Y | Y | Y | Y | Y | 8.5R2 | Y |
| VRF | N | N | Y | Y | Y | 8.5R2 | Y |
| VRF – IPv6 | N | N | Y | Y | Y | 8.5R2 | Y |
| VRF – DHCP Client | N | N | Y | Y | Y | 8.5R2 | Y |
| Web Services & CLI Scripting | 8.5R1 | Y | Y | Y | Y | N | Y |
| | | | | | | | |
| Layer 3 Feature Support | | | | | | | |
| ARP | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| ARP - Distributed (deprecated in 8.6R2) | N | N | N | N | N | N | N |
| ARP - Proxy | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| BFD | N | N | Y | Y | Y | 8.5R2 | Y |
| BGP with graceful restart | N | N | Y | Y | Y | 8.5R2 | Y |
| BGP route reflector for IPv6 | N | N | Y | Y | Y | 8.5R2 | Y |
| BGP ASPATH Filtering for IPv6 routes on IPv6 peering | N | N | Y | Y | Y | 8.5R2 | Y |
| BGP support of MD5 password for IPv6 | N | N | Y | Y | Y | 8.5R2 | Y |
| BGP 4-Octet ASN Support | N | N | Y | Y | Y | 8.5R2 | Y |
| DHCP Client / Server | 8.6R1 | Y | Y | Y | Y | 8.5R4 | Y |
| DHCP Relay | 8.5R1 | Y | Y | Y | Y | 8.5R4 | Y |
| DHCPv6 Server | N | N | Y | Y | Y | EA | Y |
| DHCPv6 Relay | 8.5R1 | Y | Y | Y | Y | EA - 8.5R4 | Y |
| DHCP Snooping / IP Source Filtering | 8.5R4 | Y | Y | Y | Y | 8.6R2 | Y |
| ECMP | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| IGMP v1/v2/v3 | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| GRE | N | N | Y | Y | Y | 8.5R2 | 8.5R2 |
| IPv4/IPv6 Blackhole Route (Null) | 8.6R1 | 8.6R1 | 8.6R1 | 8.6R1 | 8.6R1 | 8.6R1 | 8.6R1 |
| IP-IP tunneling | N | N | Y | Y | Y | 8.5R2 | 8.5R2 |
| IP routed port | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| IPv6 | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| IPv6 - DHCPv6 Snooping | 8.6R1 | 8.6R1 | 8.5R3 | 8.5R4 | N | 8.6R2 | N |
| IPv6 - Source filtering | N | 8.6R1 | 8.5R3 | 8.5R4 | N | 8.6R2 | N |
| IPv6 - DHCP Guard | EA | EA | EA | EA | N | N | N |
| IPv6 - DHCP Client Guard | EA | EA | EA | EA | N | N | N |
| IPv6 - RA Guard (RA filter) | N | 8.5R2 | Y | Y | Y | N | N |
| IPv6 - DHCP relay and Neighbor discovery proxy | 8.5R1 | Y | Y | Y | Y | N | Y |
| IP Multinetting | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| IPSec (IPv6) | N | N | Y | Y | Y | N | EA |

| Feature | 6465 | 6560 | 6860(E) | 6865 | 6900 | 6900-V72/C32 | 9900 |
|---|---|---|---|---|---|---|---|
| ISIS IPv4/IPv6 | N | N | Y | Y | Y | 8.5R2 | 8.5R2 |
| M-ISIS | N | N | Y | Y | Y | 8.5R2 | 8.5R2 |
| OSPFv2 | N | 8.5R2[1] | Y | Y | Y | 8.5R2 | Y |
| OSPFv3 | N | N | Y | Y | Y | 8.5R2 | Y |
| RIP v1/v2 | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| RIPng | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| UDP Relay (IPv4) | 8.5R4 | 8.5R4 | Y | Y | Y | 8.5R4 | 8.5R4 |
| UDP Relay (IPv6) | 8.6R1 | 8.6R1 | 8.6R1 | 8.6R | 8.6R1 | 8.6R1 | 8.6R1 |
| VRRP v2 | 8.5R2 | Y | Y | Y | Y | 8.5R2 | Y |
| VRRP v3 | 8.5R2 | Y | Y | Y | Y | 8.5R2 | Y |
| Server Load Balancing (SLB) | N | N | Y | Y | Y | N | N |
| Static routing | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| | | | | | | | |
| Multicast Features | | | | | | | |
| DVMRP | N | N | Y | Y | Y | 8.5R2 | N |
| IPv4 Multicast Switching | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| Multicast *,G | Y | 8.5R2 | 8.5R2 | Y | Y | 8.5R2 | Y |
| IPv6 Multicast Switching | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| PIM-DM | N | N | Y | Y | Y | 8.5R2 | Y |
| PIM-SM | N | N | Y | Y | Y | 8.5R2 | Y |
| PIM-SSM | N | N | Y | Y | Y | 8.5R2 | Y |
| PIM-SSM Static Map | N | N | N | N | N | N | N |
| PIM-BiDir | N | N | Y | Y | Y | 8.5R2 | Y |
| PIM Message Packing | N | N | 8.6R1 | N | 8.6R1 | 8.6R1 | N |
| PIM - Anycast RP | N | N | 8.6R2 | 8.6R2 | 8.6R2 | 8.6R2 | 8.6R2 |
| | | | | | | | |
| Monitoring/Troubleshooting Features | | | | | | | |
| Ping and traceroute | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| Policy based mirroring | N | N | Y | Y | Y | EA | 8.5R4 |
| Port mirroring | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| Port monitoring | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| Port mirroring - remote | 8.5R1 | Y | Y | Y | Y | EA | EA |
| Port mirroring – remote over linkagg | N | N | Y | Y | Y | N | N |
| RMON | 8.5R1 | Y | Y | Y | Y | N | N |
| SFlow | 8.5R1 | Y | Y | Y | Y | EA | Y |
| Switch logging / Syslog | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| TDR | N | N | Y | N | N | N | N |
| | | | | | | | |
| Layer 2 Feature Support | | | | | | | |
| 802.1q | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |

| Feature | 6465 | 6560 | 6860(E) | 6865 | 6900 | 6900-V72/C32 | 9900 |
|---|---|---|---|---|---|---|---|
| DHL | 8.5R1 | Y | Y | Y | N | N | N |
| ERP v2 | 8.5R1 | 8.5R2 | Y | Y | Y | N | 8.5R3 |
| HAVLAN | EA | N | Y | Y | Y | 8.6R2 | EA |
| Link Aggregation (static and LACP) | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| LLDP (802.1ab) | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| Loopback detection – Edge (Bridge) | 8.5R1 | Y | Y | Y | N | 8.6R2 | Y |
| Loopback detection – SAP (Access) | N | N | Y | Y | Y | 8.6R2 | EA |
| MAC Forced Forwarding | N | N | 8.6R1 | 8.6R1 | N | N | N |
| Port mapping | Y | Y | Y | Y | Y | 8.5R2 | Y |
| Private VLANs | N | N | Y | Y | Y | N | N |
| SIP Snooping | N | N | Y | N | N | N | N |
| Spanning Tree (1X1, RSTP, MSTP) | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| Spanning Tree (PVST+, Loop Guard) | N | N | Y | Y | Y | N | EA |
| STP - TCN Dampening/Duplicate Handling | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 |
| MVRP | 8.5R1 | Y | Y | Y | Y | 8.5R4 | Y |
| SPB[2] | N | N | Y | Y | Y | 8.5R2 | Y |
| SPB – HW-based LSP flooding | N | N | N | N | N | N | 8.5R4 |
| QoS Feature Support | | | | | | | |
| 802.1p / DSCP priority mapping | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| IPv4 | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| IPv6 | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| Auto-Qos prioritization of NMS/IP Phone Traffic | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| Auto-Qos – New MAC range | 8.5R2 | 8.5R2 | 8.5R2 | 8.5R2 | 8.5R2 | 8.5R2 | 8.5R2 |
| Groups - Port | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| Groups - MAC | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| Groups - Network | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| Groups - Service | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| Groups - Map | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| Groups - Switch | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| Ingress/Egress bandwidth limit | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| Per port rate limiting | N | N | Y | Y | Y | 8.5R2 | N |
| Policy Lists | 8.5R1 | Y | Y | Y | Y | N | Y |
| Policy Lists - Egress | N | N | Y | Y | Y | N | N |
| Policy based routing | N | N | Y | Y | Y | 8.6R2 | EA |
| Tri-color marking | N | N | Y | Y | Y | N | N |
| QSP Profiles 1 | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| QSP Profiles 2/3/4 | N | N | Y | Y | Y | N | N |
| QSP Profiles 5 | 8.5R1 | Y | N | N | N | N | Y |
| | | | | | | | |

| Feature | 6465 | 6560 | 6860(E) | 6865 | 6900 | 6900-V72/C32 | 9900 |
|---|---|---|---|---|---|---|---|
| Metro Ethernet Features | | | | | | | |
| CPE Test Head | 8.6R1 | N | N | N | N | N | N |
| Ethernet Loopback Test | N | N | 8.6R1 | 8.6R1 | N | N | N |
| Ethernet Services (VLAN Stacking) | 8.5R1 | N | Y | Y | Y | 8.5R4 | N |
| Ethernet OAM (ITU Y1731 and 802.1ag) | 8.5R1 | N | Y | Y | Y | N | EA |
| EFM OAM / Link OAM (802.3ah) | 8.6R1 | 8.6R1 | 8.5R4 | 8.5R4 | N | N | N |
| PPPoE Intermediate Agent | 8.6R1 | N | N | 8.6R1 | N | N | N |
| 1588v2 End-to-End Transparent Clock | 8.5R1 | N | Y | Y | Y (X72/Q32) | N | N |
| 1588v2 Peer-to-Peer Transparent Clock | 8.6R1 | N | N | N | N | N | N |
| 1588v2 Across VC | N | N | N | N | 8.5R2 (X72) | N | N |
| Access Guardian / Security Features | | | | | | | |
| 802.1x fail to MAC Authentication | 8.5R2 | Y | Y | Y | Y | N | Y |
| Access Guardian – Bridge | 8.5R1 | Y | Y | Y | Y | 8.6R1 | Y |
| Access Guardian - Access | N | N | Y | Y | Y | 8.5R4 | Y |
| Application Fingerprinting | N | N | N | N | Y | N | N |
| Application Monitoring and Enforcement (Appmon) | N | N | Y | N | N | N | N |
| ARP Poisoning Protection | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| BYOD - COA Extension support for RADIUS | Y | Y | Y | Y | 8.62 | 8.6R2 | Y |
| BYOD - mDNS Snooping/Relay | Y | Y | Y | Y | 8.62 | 8.6R2 | Y |
| BYOD - UPNP/DLNA Relay | Y | Y | Y | Y | 8.62 | 8.6R2 | Y |
| BYOD - Switch Port location information pass-through in RADIUS requests | Y | Y | Y | Y | 8.62 | 8.6R2 | Y |
| Captive Portal | 8.5R4 | Y | Y | Y | 8.62 | 8.6R2 | Y |
| Critical Voice VLAN | EA | N | N | N | N | N | N |
| IoT Device Profiling | 8.5R2 | 8.5R2 | 8.5R2 | 8.5R2 | 8.5R2 | 8.6R1 | 8.5R2 |
| Directed Broadcasts – Control | 8.5R2 | 8.5R2 | 8.5R2 | 8.5R2 | 8.5R2 | N | N |
| Interface Violation Recovery | 8.5R1 | Y | Y | Y | Y | EA | Y |
| Kerberos Snooping | N | 8.6R2 | 8.6R2 | 8.6R2 | 8.6R2 | 8.6R2 | 8.6R2 |
| L2 GRE Tunnel Access (Edge) (bridge ports) | N | Y | Y | Y | 8.6R1[3] | N | Y |
| L2 GRE Tunnel Access (Edge) (access ports) | N | N | 8.6R1 | 8.6R1 | 8.6R1[3] | N | 8.6R1 |
| L2 GRE Tunnel Aggregation | N | N | Y | Y | Y[3] | N | Y |
| Learned Port Security (LPS) | 8.5R1 | Y | Y | Y | Y | 8.5R4 | Y |
| LPS – Multiple MAC Range | 8.6R1 | 8.6R1 | 8.6R1 | 8.6R1 | 8.5R3 | 8.6R1 | 8.6R1 |
| LLDP | 8.5R1 | Y | Y | Y | Y | 8.5R2 | Y |
| MACsec[4] | 8.5R1 | 8.5R4 | Y | N | N | N | 8.5R2 |
| MACsec MKA Support[4] | 8.5R2 | 8.5R4 | 8.5R2 | N | N | N | 8.5R2 |

| Feature | 6465 | 6560 | 6860(E) | 6865 | 6900 | 6900-V72/C32 | 9900 |
|---|---|---|---|---|---|---|---|
| Quarantine Manager | N | N | Y | Y | N | N | N |
| RADIUS test tool | 8.5R1 | Y | Y | Y | Y | N | Y |
| RADIUS - RFC-2868 Support | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 |
| Role-based Authentication for Routed Domains | N | N | 8.5R4 | 8.5R4 | 8.5R4 | 8.6R1 | 8.5R4 |
| Storm Control | N | N | Y | Y | Y | N | N |
| TACACS+ Client | 8.5R1 | Y | Y | Y | Y | 8.6R1 | Y |
| TACACS+ command based authorization | N | N | Y | Y | Y | N | N |
| UNP Access Mode (SPB/VXLAN) for Silent Devices | N | N | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 | 8.5R4 |
| PoE Features | | | | | | | |
| 802.3af and 802.3at | 8.5R1 | Y | Y | Y | N | N | Y |
| 802.3bt | N | 8.6R2 | N | N | N | N | N |
| Auto Negotiation of PoE Class-power upper limit | 8.5R1 | Y | Y | Y | N | N | Y |
| Display of detected power class | 8.5R1 | Y | Y | Y | N | N | Y |
| LLDP/802.3at power management TLV | 8.5R1 | Y | Y | Y | N | N | Y |
| HPOE support | 8.5R1 (60W) | Y (95W) | Y (60W) | Y (75W) | N | N | Y (75W) |
| Time Of Day Support | 8.5R1 | Y | Y | Y | N | N | Y |
| Data Center Features (License May Be Required) | | | | | | | |
| CEE DCBX Version 1.01 | N | N | N | N | Y | N | N |
| Data Center Bridging (DCBX/ETS/PFC) | N | N | N | N | Y | N | N |
| EVB | N | N | N | N | N | N | N |
| FCoE / FC Gateway | N | N | N | N | Y | N | N |
| VXLAN[5] | N | N | N | N | Q32/X72/ V72/C32 | 8.5R3 | N |
| VM/VXLAN Snooping | N | N | N | N | Y | N | N |
| FIP Snooping | N | N | N | N | Y | N | N |

**Notes:**
1. OS6560 supports stub area only.
2. See protocol support table in Appendix B.
3. Supported on OS6900-Q32/X72 models.
4. Site license required beginning in 8.6R1.
5. L2 head-end only on V72/C32.

## Appendix B: SPB L3 VPN-Lite Service-based (Inline Routing) and External Loopback Support

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

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

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

## Appendix C: General Upgrade Requirements and Best Practices

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

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

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

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

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

## Supported Upgrade Paths and Procedures

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

| Platform | AOS Releases Supporting ISSU to 8.6R2 (GA) |
|---|---|
| OS6465 | 8.5.255.R02 (GA)<br>8.5.54.R03 (GA)<br>8.5.196.R04 (GA)<br>8.6.289.R01 (GA)<br>8.6.299.R01 (MR) |
| OS6560 | 8.5.196.R04 (GA)<br>8.6.289.R01 (GA)<br>8.6.299.R01 (MR) |
| OS6860(E) | 8.5.255.R02 (GA)<br>8.5.54.R03 (GA)<br>8.5.196.R04 (GA)<br>8.6.289.R01 (GA)<br>8.6.299.R01 (MR) |
| OS6865 | 8.5.255.R02 (GA)<br>8.5.196.R04 (GA)<br>8.6.289.R01 (GA)<br>8.6.299.R01 (MR) |
| OS6900 | 8.5.255.R02 (GA)<br>8.5.54.R03 (GA)<br>8.5.196.R04 (GA)<br>8.6.289.R01 (GA)<br>8.6.299.R01 (MR) |
| OS6900-V72/C32 | 8.5.255.R02 (GA)<br>8.5.54.R03 (GA)<br>8.5.196.R04 (GA)<br>8.6.289.R01 (GA)<br>8.6.299.R01 (MR)<br><br>See Appendix G when upgrading an OS6900-V72/C32. |
| OS9900 | N/A |

**8.6R2 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 UBoot and FPGA. If they meet the minimum requirements, (i.e. they were already upgraded during a previous AOS upgrade) then only an upgrade of the AOS images is required.
- Depending on whether a standalone chassis or VC is being upgraded, upgrading can take from 5 to 20 minutes. Additional time will be needed for the network to re-converge.

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

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

### Switch Maintenance

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

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

```
6900-> show system
System:
Description:  Alcatel-Lucent OS6900-X20 8.6.289.R01 GA, July 14, 2019.,
Object ID:    1.3.6.1.4.1.6486.801.1.1.2.1.10.1.1,
```

```
   Up Time:       0 days 0 hours 1 minutes and 44 seconds,
   Contact:       Alcatel-Lucent, http://alcatel-lucent.com/wps/portal/enterprise,
   Name:          6900,
   Location:      Unknown,
   Services:      78,
   Date & Time:   MON AUG 12 2019 06:55:43 (UTC)
   Flash Space:
   Primary CMM:
   Available (bytes):  1111470080,
 Comments         :  None
```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1. Download the Upgrade Files

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

- OS6465 – Nos.img (**Note**: If upgrading an OS6465-P28, upgrading the FPGA to version 0.7 may be required to address CRAOS8x-12042. AOS must be upgraded prior to upgrading the FPGA. See Appendix F.)
- OS6560 – Nos.img (**Note**: If upgrading an OS6560-P24Z24/P48Z16 (903954-90)/P24Z8, upgrading the FPGA to version 0.7 may be required to address CRAOS8x-7207. AOS must be upgraded prior to upgrading the FPGA. See Appendix F.)
- OS6860 – Uos.img
- OS6865 – Uos.img (**Note**: If upgrading an OS6865-U28X, upgrading the FPGA to version 0.12 may be required to address CRAOS8X-4150. AOS must be upgraded prior to upgrading the FPGA. See Appendix F.)
- OS6900 **-** Tos.img
- OS6900-V72/C32 – Yos.img. See Appendix G.
- OS9900 – Mos.img, Mhost.img, Meni.img
- imgsha256sum (not required) –This file is only required when running in Common Criteria mode. Please refer to the Common Criteria Operational Guidance Document for additional information.

2. FTP the Upgrade Files to the Switch

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

3. Upgrade the image file

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

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

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

4. Verify the Software Upgrade

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

```
OS6900-> show microcode
/flash/working
Package           Release                 Size     Description
------------------+-----------------------+--------+-----------------------------------
Tos.img           8.6.189.R02             210697424 Alcatel-Lucent OS


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

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

5. Certify the Software Upgrade

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

```
OS6900-> copy running certified

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

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

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

1. Download the Upgrade Files

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

- OS6465 – Nos.img (**Note**: If upgrading an OS6465-U28, upgrading the FPGA to version 0.7 may be required to address CRAOS8x-12042. AOS must be upgraded prior to upgrading the FPGA. See Appendix F.)
- OS6560 – Nos.img (**Note**: If upgrading an OS6560-P24Z24/P48Z16 (903954-90)/P24Z8, upgrading the FPGA to version 0.7 may be required to address CRAOS8x-7207. AOS must be upgraded prior to upgrading the FPGA. See Appendix F.)
- OS6860 – Uos.img
- OS6865 – Uos.img (**Note**: If upgrading an OS6865-U28X, upgrading the FPGA to version 0.12 may be required to address CRAOS8X-4150. AOS must be upgraded prior to upgrading the FPGA. See Appendix F.)
- OS6900 **-** Tos.img
- OS6900-V72/C32 – Yos.img. See Appendix G.

  **Note:** When performing an ISSU upgrade on an OS6900-V72/C32 from the 8.5R2 GA Release the following error is displayed on the console. This is a display issue only, the upgrade will be completed successfully. For example:

```
6900-V72-VC-2-> issu from issu
Are you sure you want an In Service System Upgrade? (Y/N) : y
md5sum: can't open '/flash/issu/Tos.img': No such file or directory
sh: 9260: unknown operand
sh: 9260: unknown operand
```

- OS9900 – Mos.img, Mhost.img, Meni.img
- ISSU Version File – issu_version
- imgsha256sum (not required) –This file is only required when running in Common Criteria mode. Please refer to the Common Criteria Operational Guidance Document for additional information.

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

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

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

3. Clean up existing ISSU directories

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

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

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

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

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

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

6. Log out of the Slave chassis:

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

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

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

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

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

9. Upgrade the image files using ISSU:

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

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

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

This indicates that the ISSU is completed

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

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

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

10. Verify the Software Upgrade

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

```
OS6900-> show microcode
/flash/working
Package           Release                 Size     Description
-----------------+-----------------------+--------+-----------------------------------
Tos.img           8.6.189.R02
```

11. Certify the Software Upgrade

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

```
OS6900-> copy running certified

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

## Appendix F: FPGA Upgrade Procedure

The following CRs can be addressed by performing an FPGA/CPLD upgrade on the respective models.

| CR | Summary |
|---|---|
| CRAOS8X-12042 | OS6465-P28 - Switch does not shutdown after crossing danger threshold temperature. |
| CRAOS8X-7207 | OS6560-P24Z24,P24Z8,P48Z16 (903954-90) - Chassis reboots twice to join a VC. |
| CRAOS8X-4150 | OS6865-U28X - OS6865-U28X VC LED status behavior. |

**Note: AOS must be upgraded to 8.6R2 prior to performing an FPGA upgrade.**

1. Download and extract the upgrade archive from the Service & Support website. In addition to the AOS images, the archive will also contain the following FPGA upgrade kit.

- CPLD File - fpga_kit_nnnn

2. FTP (Binary) the FPGA upgrade kit listed above 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.

```
-> update fpga-cpld cmm all file fpga_kit_6285
Parse /flash/fpga_kit_6285
Please wait...
fpga file: fpga_6560_v07.vme
update chassis 1
Starting CMM ALL FPGA Upgrade
CMM 1/1
Successfully updated
Reload required to activate new firmware.
```

Once complete, a reboot is required.

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

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

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

- Standard Upgrade
  - If upgrading from AOS Release 8.5R02, 8.5R03, or 8.5R04 - Script file will perform flash cleanup.
  - If upgrading from AOS Release 8.6R01 - Script file not needed.
- ISSU Upgrade
  - If upgrading from AOS Release 8.5R02, 8.5R03, or 8.5R04 - Script file will perform flash cleanup and FEC disable.
  - If upgrading from AOS Release 8.6R01 - Script file will perform FEC disable.
- Script file name: ***pre_update_script.sh*** (Available from service & support website)

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

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

## Appendix H: Fixed Problem Reports

The following problem reports were closed in this AOS Release.

| CR | Description |
|---|---|
| **Case:**<br>**00359834**<br>*CRAOS6X-2070* | **Summary**:<br>LPS moves the UNP users to filtering state.<br><br>**Explanation**:<br>Port-security of maximum one bridged MAC is configured on the LPS port, if authentication gets failed, the UNP user port moved to default block profile (as per non-supplicant policy).<br>This results in increasing the LPS filter count to 1 and blocks as the allowed maximum bridged count is configured as 1.<br><br>Click for Additional Information |
| **Case:**<br>**00368479**<br>*CRAOS8X-10880* | **Summary:**<br>link between 6900V72 and 9907 CNIU8 (using FINISAR AOC cable) doesn't come up.<br><br>**Explanation**:<br>On some ports, the signal received on the OS99-CNI-U8 port was too weak to allow the link to come up. It is seen only with one Vendor FINISAR, and on very rare occasions.<br><br>Click for Additional Information |
| **Case:**<br>**00377275**<br>*CRAOS8X-9129* | **Summary**:<br>OS680 users are not getting IP address from the DHCP server.<br><br>**Explanation**:<br>OS6860 acts as an IP-helper.<br>The relay-agent is not changing the source ip address of the discover packet. The relay-agent is sending the packet with the source ip address 0.0.0.0 which is from dhcp-client interface configuration on the switch.<br><br>Click for Additional Information |
| **Case:**<br>**00381458**<br>*CRAOS8X-9939* | **Summary:**<br>QOS condition with "Established" Parameter does not work.<br><br>**Explanation**:<br>QoS rule with established parameter is not added in the software due to which packets ingressing the software are dropped as the rule is not present. This issue is seen only with OS9900 switches.<br><br>Click for Additional Information |
| **Case:**<br>**00389102**<br>*CRAOS8X-10757* | **Summary**:<br>OS6860 switch issue with UNP classification for defaultWLANProfile.<br><br>**Explanation**:<br>AP-1231 is getting classified into "default-profile" instead of "defaultWLANProfile " after the reboot.<br><br>Click for Additional Information |
| **Case:**<br>**00394825**<br>*CRAOS8X-11555* | **Summary**:<br>OS6560: Authentication error and the user cannot access the network.<br><br>**Explanation**:<br>The switch was not updating the IP information because it didn't receive ARP packet from the client during the authentication, instead receiving ARP probe packets which would be dropped by switch and move the device to default profile.<br><br>Click for Additional Information |
| **Case:**<br>**00396606** | **Summary**:<br>OS6860E SVLAN's UNI cannot learning Core Router MAC Address. |

| | |
|---|---|
| *CRAOS8X-11867* | **Explanation:**<br>There are same ethernet-service SVLAN mapped to two different SAP UNI Linkagg ports. When removing the ethernet-service for one SAP using "no ethernet-service sap", it leads to flushing the MAC-addresses learnt on the other SAP UNI Linkagg port. This behavior is seen only when these two SAP UNI ports are Linkagg ports.<br><br>Click for Additional Information |
| **Case:**<br>**00397029**<br>*CRAOS8X-11563* | **Summary:**<br>swlogd lpCmm LanCmmUtl INFO: lpCmmUtilChassisIdSlotFound 99 lpVcCmmInfo (1c64ec8) Messages are seen on OS6860 switch.<br><br>**Explanation:**<br>The above log message are generated when an SNMP getnext action is being performed from SNMP server (like OV2500, OVCirrus etc). The message provides the information that snmp getnext operation is being performed. The messages are generated as per the design. If there is any issue related to lanpower.<br><br>Click for Additional Information |
| **Case:**<br>**00399087**<br>*CRAOS8X-11870* | **Summary:**<br>AP-514/515 boots UP with restricted power mode in the HPoE ports of Alcatel switch.<br><br>**Explanation:**<br>Alcatel AP-514/515 boot UP with restricted power mode, when connected directly to the HPoE (Above 60W) ports of Alcatel switch. The same APs connected to the PoE+ (Max 30W) ports would work properly.<br>AP's "System Status" LED would be either Amber-Solid, Amber-Flashing or RED, if it works with restricted power mode.<br><br>Click for Additional Information |
| **Case:**<br>**00400220**<br>*CRAOS8X-11743* | **Summary:**<br>CVE-2019-11478 and CVE-2019-11479 vulnerabilities.<br><br>**Explanation:**<br>These two vulnerabilities are related to SACK and MSS which will result in excess resource utilization and Denial of Service.<br><br>Click for Additional Information |
| **Case:**<br>**00400745**<br>*CRAOS8X-11779* | **Summary:**<br>OS9907 spontaneous CMM takeover occured with a pmd confd generated on the CMM that restarted<br><br>**Explanation:**<br>The confd task crashed because 2x connections to the confd happened simultaneously, on the CMM and triggered a CMM reboot.<br><br>Click for Additional Information |
| **Case:**<br>**00401416**<br>*CRAOS8X-12048* | **Summary:**<br>Vulnerabilities related to CVE-2014-3566, CVE-2008-1483, CVE-2008-1657 which is vulnerable to TLS Version 1.0.<br><br>**Explanation:**<br>Vulnerabilities detected on the security scan on the OS6860 switch on 8.5.R04.196.<br>CVE-2014-3566<br>CVE-2008-1483<br>CVE-2008-1657<br><br>Click for Additional Information |
| **Case:**<br>**00402083**<br>*CRAOS8X-11890* | **Summary:**<br>OS6860: inserting an "Out of the Box" chassis in a VC in production, running SPB, caused a network flooding.<br><br>**Explanation:** |

| | |
|---|---|
| | The new chassis (out of the box) introduced had a temporary chassis-id 1 confused the chassis 2, thinking he was now the master even though the chassis 1 was still master. This leads to have linkagg ports programmed as primary on both chassis 1 and 2 and caused network flooding.<br><br>Click for Additional Information |
| **Case:**<br>**00403751**<br>*CRAOS8X-13040* | **Summary:**<br>MAC-Range UNP Classification not working for ALE IP Phones.<br><br>**Explanation:**<br>Configured MAC-Range UNP classification on port 1/1/1 of OS6560-P24Z8 to move the IP Phone automatically to Vlan 132 (untagged).<br><br>When the Phones restarts, the error message "no tftp response" is displayed on the IP Phone.<br><br>Click for Additional Information |
| **Case:**<br>**00404051**<br>*CRAOS8X-12040* | **Summary:**<br>PoE is not stopped after 70°C temperature in OS6465 as per hardware guide specification.<br><br>**Explanation:**<br>PoE budget will be reduced to 130W when the board temperature goes above 70 deg C, it stays the same even when the temperature crosses more than 100 deg C.Once the temperature goes below 70 deg C, PoE budget will be retained to 150W.<br><br>Click for Additional Information |
| **Case:**<br>**00404075**<br>*CRAOS8X-12042* | **Summary:**<br>OS6465 switches do not shutdown after crossing danger threshold temperature.<br><br>**Explanation:**<br>According to hardware specification, the switch should shutdown whenever the switch board temperature reaches the danger threshold. However, OS6465 switches continue to operate even after crossing the danger threshold temperature.<br><br>Click for Additional Information |
| **Case:**<br>**00404236**<br>**00385767**<br>*CRAOS8X-10319* | **Summary:**<br>OS9907 XNIU48 ports don't pass traffic and mac addresses not getting learnt for a range of ports on the same ASIC<br><br>**Explanation:**<br>This is one of the 6x ASIC that got his interruption handling frozen, caused by ports flapping at a very fast rate. A work-around consists in power off/on the NI to have it recovered. (doing no power slot 1/X; power slot 1/X, X being the NI slot) . Flapping ports should be monitored closely and avoided as they can trigger this issue again.<br><br>Click for Additional Information |
| **Case:**<br>**00404626**<br>*CRAOS8X-12092* | **Summary:**<br>PMD file and switch reboot when upgrading from 8.5.R04 to 8.6.R01<br><br>**Explanation:**<br>Crash is related to ip6ni_dhcp6_guard, the removal of ipv6 interface is suggested as workaround<br><br>Click for Additional Information |
| **Case:**<br>**00404686**<br>*CRAOS8X-12188* | **Summary:**<br>OS6560 LBD with remote-origin issue.<br><br>**Explanation:**<br>Enable the LBD with the remote origin.<br>The remote origin entry is not shown in show configuration snapshot.<br><br>Click for Additional Information |

| | |
|---|---|
| **Case:**<br>**00404764**<br>*CRAOS8X-12109* | **Summary:**<br>OS9900_DDM display issue.<br><br>**Explanation:**<br>The CLI command "show interface DDM" only displays some of the transceivers' value. For the rest of the transceivers "Calibration :1" is only displayed.<br><br>Click for Additional Information |
| **Case:**<br>**00405938**<br>*CRAOS8X-12393* | **Summary:**<br>Aruba AP-555 and AP-535 are not recovering after OS6860 switch reboot.<br><br>**Explanation:**<br>Aruba AP-555 plugged into 6860-P24Z8 HPOE port 1/1/18, seeing "denied" in the status column of "show lanpower slot 1/1" When 4pair is disabled on the port the AP will come up. Performing a write memory preserves the 4pair disable in the running config.<br><br>If switch is rebooted the AP again shows "denied" in the status column of "show lanpower slot 1/1". To resolve, must enable 4pair and then disable again to AP to come up.<br><br>Click for Additional Information |
| **Case:**<br>**00406315**<br>*CRAOS8X-12222* | **Summary:**<br>Issue in disabling LAN power for Multi-Gigabit port of OS6860 switch<br><br>**Explanation:**<br>In OS6860 switch the Multi-Gigabit port continuous to provide power to PD, even after disabling the PoE. This issue would be only seen with the AP-514/515, AP-534/535 and AP-555, which supports Multi-Gigabit port.<br><br>Click for Additional Information |
| **Case:**<br>**00407382**<br>*CRAOS8X-12206* | **Summary:**<br>BGP connection is closed when an update message containing a class D or class E prefix is received.<br><br>**Explanation:**<br>When OS6900 receives a BGP update message which contains a class D or class E prefix (route entry), the BGP connection is closed. This results in connectivity issues as all BGP routes are flushed.<br><br>Click for Additional Information |
| **Case:**<br>**00408657**<br>*CRAOS8X-12519* | **Summary:**<br>OS6860 - OSPF Auth-type mismatch error.<br><br>**Explanation:**<br>Auth-type mismatch error message seen due to which switch fails to form adjacency in OSPF.<br><br>Click for Additional Information |
| **Case:**<br>**00408973**<br>*CRAOS8X-12837* | **Summary:**<br>OS6900 virtual-chassis crash with "capmanc" task.<br><br>**Explanation:**<br>Virtual chassis of OS6900 switch is crashed due to the "capmanc" task for Capability manger, It was seen while accessing a NULL pointer when the task was trying to print a swlog message. The Crash happened while accessing a null pointer.<br><br>Click for Additional Information |
| **Case:**<br>**00412113**<br>**00418277**<br>*CRAOS8X-12907* | **Summary:**<br>OS6900 VC units rebooted consecutively with PMD.<br><br>**Explanation:**<br>The Master unit in a VC of two OS6900 units rebooted with PMD. After a while, slave unit (converted to master) rebooted with PMD. This Virtual Chassis acts as an IP helper. |

| | |
|---|---|
| | Click for Additional Information |
| **Case:**<br>**00412476**<br>**00429250**<br>*CRAOS8X-13008* | **Summary:**<br>OS6900 - High memory above threshold due to "qoscmm" task.<br><br>**Explanation:**<br>When the "QoS apply" command is continuously applied every 3 to 5 seconds by a script or by an external control device. This will accumulate the memory cache and lead to high memory.<br><br>Click for Additional Information |
| **Case:**<br>**00412499**<br>**00423026**<br>*CRAOS8X-13301* | **Summary:**<br>Show system and show interface output shows different timestamps.<br><br>**Explanation:**<br>Show system and swlog timestamp show the timezone which has been configured on the switch. Whereas the field "Last Time Link Changed" under "show interfaces chassis/slot/port" output shows time in the UTC timezone.<br><br>Click for Additional Information |
| **Case:**<br>**00412983**<br>*CRAOS8X-11889* | **Summary:**<br>OS6465-P12 switch shows the lanpower status as Powered OFF, even though the service is enabled in the configuration.<br><br>**Explanation:**<br>Error logs in the switch logs stating that the Dragonite controller has failed to initialize. This issue is caused due to some error when the PoE register is accessed from kernel.<br><br>Click for Additional Information |
| **Case:**<br>**00413188**<br>*CRAOS8X-13115* | **Summary:**<br>Configuration of NTP IP service on any IP managed interface.<br><br>**Explanation:**<br>Feature is deprecated from AOS 8.5.R04. The feature will be reintroduced on AOS 8.6R02.<br><br>Click for Additional Information |
| **Case:**<br>**00413506**<br>*CRAOS8X-13124* | **Summary:**<br>OS6860E-P24 - Hash-control mode changes itself after switch reboot.<br><br>**Explanation:**<br>A user has configured "hash-control" mode from "Extended" to "Brief". Following the changes, the user did "write memory flash-synchro". However, upon rebooting "reload from working no rollback-timeout" the chassis, the hash-control mode has changed to "Extended" again.<br><br>Click for Additional Information |
| **Case:**<br>**00413988**<br>*CRAOS8X-13102* | **Summary:**<br>“show interfaces macsec statistics” output command Bytes Xmitted/Received is stuck to value "4294967295" on OS6465 when link is secured with dynamic macsec<br><br>**Explanation:**<br>Hardware counter was 32 bits on OS6465, it stops incrementing after reaching the maximum value 0xffffffff = 429496729<br><br>Click for Additional Information |
| **Case:**<br>**00415788**<br>*CRAOS8X-13418* | **Summary:**<br>Unable to do the internal SSH/SCP/Telnet to the Slave virtual chassis units from Master virtual chassis unit using 6900-X20 VC.<br><br>**Explanation:**<br>Internal SSH/SCP/Telnet session (127.10.2.65) timed out from Master CLI. Atleast one VLAN IP interface should be UP in Master to do the CLI sessions to SSH/SCP/Telnet to the Slave unit |

| | |
|---|---|
| | As long as the "source-ip" is set to any VLAN IP interface, the internal sessions are not allowed from Master CLI as per the code behavior.<br>This behavior has been fixed in 8.6.89.R02.<br><br>Click for Additional Information |
| **Case:**<br>**00415789**<br>*CRAOS8X-13597* | **Summary:**<br>Primary port of static linkagg is not forwarding traffic when the backup link is down.<br><br>**Explanation:**<br>While unplugging the backup linkagg member link slowly the traffic is disturbed and not getting forwarded in primary link member of the linkagg .<br><br>Click for Additional Information |
| **Case:**<br>**00417821**<br>*CRAOS8X-13699* | **Summary:**<br>Getting the error: AGCMM AG-General INFO message: +++ Cannot configure Access port as port_property is set to PM_NETWORK_PORT, when the UNP Access port is part of IP interface enabled VLAN (NETWORK port).<br><br>**Explanation:**<br>The ports that are being assigned as SPB Access/VXLAN expects it not to be member of IP interface vlan. It is being tried to remove from vlan 1, the port property(NETWORK) is cleared and modified to default port property.<br><br>Click for Additional Information |
| **Case:**<br>**00418628**<br>*CRAOS8X-13851* | **Summary:**<br>OS6900: After takeover, VRRP TCAM rule is always enabled, even if it is disabled in the configuration.<br><br>**Explanation:**<br>By default, when a VRRP packet is received on an SPB service access port, the customer VLAN tag is removed. However, the default behavior can be changed by executing the command ‘service local-vrrp disable’. Even when this command is present in the configuration, the VLAN tag is removed after takeover/reload.<br><br>Click for Additional Information |
| **Case:**<br>**00418649**<br>*CRAOS8X-13852* | **Summary:**<br>No DHCP Relay Interfaces After Reboot.<br><br>**Explanation:**<br>Issue while creating a DHCP relay interface with numeric value and this interface will disappear after reload of switch even though the configuration is saved.<br><br>Click for Additional Information |
| **Case:**<br>**00419241**<br>*CRAOS8X-13842* | **Summary:**<br>OS6465-P12 and P6 Power Supply Output Power mismatch.<br><br>**Explanation:**<br>Power supply used is OS6465-BPN-H AC (SDR-240-55) on OS6465-P12/P6 switches. The PS is of 180W as per HW guide however, is showing 240w on the SW.<br><br>Click for Additional Information |
| **Case:**<br>**00419781**<br>*CRAOS8X-13856* | **Summary:**<br>DHCP relay interface with numeric value is missing out after reboot of switch, even though configuration has been saved.<br><br>**Explanation:**<br>While creating DHCP relay interface with numeric value as below, for example<br>->ip dhcp relay interface "120" destination 192.168.1.3. The relay interface will not be available after reboot of the switch, even though the configuration is saved. However it does not have any issue with Alphanumeric string.<br><br>Click for Additional Information |
| **Case:** | **Summary:** |

| | |
|---|---|
| **00420086**<br>*CRAOS8X-14053* | The OS9900 (OS99-XNI-U48 ) and OS6465 switches are connected in the linkagg by using two links. If one port is disabled from the linkagg members, it would shut down both the member ports of the linkagg.<br><br>**Explanation:**<br>This issue is because of the XNI module in OS9900 along with the CLI command "disable" used to shutdown the member port of linkagg. When one port was powered off and due to the power off of the PHY interface, it toggled the other member port in the linkagg. Code changes has been done to reset the interface instead of power off when the command "disable" used to shut down the interface port of the linkagg.<br><br>Click for Additional Information |
| **Case:**<br>**00420103**<br>*CRAOS8X-13913* | **Summary:**<br>OS6900 - Interface port details are missing in lldp remote-system output.<br><br>**Explanation:**<br>In VC, after a slave chassis reboot and joins back, checking show lldp remote-system output from Master chassis would miss the interface port detail for 1/1/1 who is a primary link of the linkagg - 1. To recover this behavior, the entire VC (Chassis-1 & 2) has to be reloaded again.<br><br>Click for Additional Information |
| **Case:**<br>**00420433**<br>*CRAOS8X-13902* | **Summary:**<br>"Not OK" status on "Checking Layer3/Switching" for the Command "show aaa switch-access process-self-test".<br><br>**Explanation:**<br>The OS6560-P48/24Z16 switch displays "Checking Layer3/Switching" is "Not OK" for the command "show aaa switch-access process-self-test".<br><br>Click for Additional Information |
| **Case:**<br>**00420722**<br>*CRAOS8X-14461* | **Summary:**<br>OS9900 - LED link indicator on the OS99-CNI-U8 NI module remains Solid Green despite the traffic flow instead of Blinking Green.<br><br>**Explanation:**<br>According to the hardware guide of OS9900, LED behavior of NI modules will be Blinking Green while there is traffic. However, the port LEDs of the NI module (OS99-CNI-U8) in OS9900 indicating Solid GREEN despite the traffic flow.<br><br>Microcode optimization has been done to copy the traffic behavior to the LEDs for NI (OS99-CNI-U8). Fix is available in AOS 8.6R02.<br><br>Click for Additional Information |
| **Case:**<br>**00421775**<br>*CRAOS8X-14104* | **Summary:**<br>OS6860 - Incorrect display of power availability.<br><br>**Explanation:**<br>OS6860E is installed with Dual power supply units (PS-1 & PS-2). Now, out of 2 power supply units, removed the power supply cord for one unit. Now displaying the output of "show powersupply" is supposed to indicate the remaining power after the removal of a PS unit. However, the switch still shows or not updating the actual value of the remaining power. Instead, it still shows a power value as if both the power supply units were installed.<br><br>Click for Additional Information |
| **Case:**<br>**00422353**<br>**00429192**<br>*CRAOS8X-14713* | **Summary:**<br>OS9900_CMM-B is Down<br><br>**Explanation:**<br>After CMM-A rebooted due to the Kernel Crash, CMM-A did not failover to CMM-B, and CMM-B stayed DOWN.<br><br>Click for Additional Information |

| | |
|---|---|
| **Case:**<br>**00423355**<br>*CRAOS8X-14322* | **Summary:**<br>OS9900 - "show module chassis-id X long" command does not show some NI modules installed.<br><br>**Explanation:**<br>When executing the "show module or show module long" command, it shows the details of all NI slots installed, however, executing the CLI command "show module chassis-id <Chassis ID#> long" did not show some of the NI modules installed. This behavior happens randomly with NI's installed.<br><br>Click for Additional Information |
| **Case:**<br>**00422393**<br>*CRAOS8X-11208* | **Summary:**<br>Wrong time is displayed for the 'Last Enabled' & 'Last SPF' fields of show spb isis info command.<br><br>**Explanation:**<br>We can see the date/time displayed for these 2 fields is different and several years ahead of the time displayed under show system.<br><br>Click for Additional Information |
| **Case:**<br>**00422417**<br>*CRAOS8X-14203* | **Summary:**<br>NTP Interface loopback zero workaround not working in 86.R01<br><br>**Explanation:**<br>Since the CLI command < Ip service source-ip Loopback0 ntp> has been deprecated from 85.R04 and 86.R01, tried to apply the NTP loopback Zero workaround on OS6860 running 86.R01 with no success.<br><br>Click for Additional Information |
| **Case:**<br>**00422733**<br>*CRAOS8X-142556* | **Summary:**<br>NTP Client Server- list never get erased.<br><br>**Explanation:**<br>The show command-> show ntp server client-list displays the list of NTP clients in the NTP server switch, however this list is never flushed, even if, NTP client is disabled on the client side for a long time, still the client interface IP is seen under NTP server client list.<br><br>Click for Additional Information |
| **Case:**<br>**00422749**<br>*CRAOS8X-14310* | **Summary:**<br>OS9907 switch seen as STP rootBridge by remote devices and one link to a remote switch got STP blocked even though spantree cist was disabled on it.<br><br>**Explanation:**<br>The issue is that once a port has its vlan per default changed to a vlan different from vlan 1, removing this port from this default vlan will reenable accidentally the STP on this port. To recover from this state, spantree cist must be enabled/disabled again on the port.<br><br>Click for Additional Information |
| **Case:**<br>**00423179**<br>*CRAOS8X-14378* | **Summary:**<br>9907 Core switch Failure Notification Delay of 9 minutes in NMS trap.<br><br>**Explanation:**<br>OS9900 VC of 2. When one of the units powered off, NMS was not receiving switch down trap immediately and is taking around 9-10 min to send the trap. Issue has been fixed and NMS able to receive traps from OS900 VC within 30 sec after Mater unit powers off.<br><br>Click for Additional Information |
| **Case:**<br>**00424131**<br>*CRAOS8X-14473* | **Summary:**<br>OS6860 Configured MTU size in a rtr-port is getting reset to 1500 after the reboot.<br><br>**Explanation:** |

| | |
|---|---|
| | Router VLAN MTU is not seen in the configuration snapshot and that causes the reset in MTU post the reload.<br><br>Click for Additional Information |
| **Case:**<br>**00424709**<br>*CRAOS8X-14879* | **Summary:**<br>OS6860: dhcp-snooping configuration on vfl link made the VC-2 OS6860 unstable and contributed to non-stop ARP overwritten swlog messages seen on adjacent CORE OS6900.<br><br>**Explanation:**<br>The communication issues in the VC-2 6860 were caused by an erroneous dhcp-snooping configuration on the VFL links.<br><br>Click for Additional Information |
| **Case:**<br>**00428852**<br>**00426538**<br>**00411045**<br>**00424903**<br>*CRAOS8X-12998* | **Summary:**<br>SSH session disconnection issue with OS6860 & OS6560<br><br>**Explanation:**<br>The parameter 'Session CLI Timeout' is wrongly implemented for "inactivity timer" but instead, it terminates the session after it expires the value set in 'Session CLI Timeout'. The issue is due to an upgraded version of OpenSSH in AOS8.6R01, which is not sending TTY information to the session manager.<br><br>Click for Additional Information |
| **Case:**<br>**00430970**<br>*CRAOS8X-13135* | **Summary:**<br>OS9900: The traffic of same TCP stream flow was load balanced between ports of a linkagg.<br><br>**Explanation:**<br>With default hash-control mode "extended", the traffic of same TCP stream flow was load balanced by all ports of a linkagg. It cause disorder of the packets received on the Receiver, TCP session has dropped down the bandwidth.<br><br>Click for Additional Information |
| **Case:**<br>**00436466**<br>*CRAOS8X-15896* | **Summary:**<br>Deleting a BVLAN causes SPB ISIS adjacency to toggle.<br><br>**Explanation:**<br>After adding ISID on any node of SPB Backbone (Ex: BVLAN 4002) and removing it right away, if the respective BVLAN (Ex: 4002) is removed on any of the nodes, the SPB ISIS protocol starts to toggle.<br><br>Click for Additional Information |