Release Notes - Rev. D

OmniSwitch
10K/9900/6900/6860(E)/6865

Release 8.3.1.R01

These release notes accompany release 8.3.1.R01. These release notes provide important information on individual software features and hardware modules. Since much of the information in these release notes is not included in the hardware and software user manuals, it is important that you read all sections of this document before installing new hardware or loading new software.

Contents

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. User guides can be downloaded at: http://enterprise.alcatel-lucent.com/?dept=UserGuides&page=Portal

- OmniSwitch 10K Hardware User Guide
- OmniSwitch 9900 Hardware User Guide
- OmniSwitch 6900 Hardware User Guide
- OmniSwitch 6860(E) Hardware User Guide
- OmniSwitch 6865 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
OS6900-X Models	2GB	2GB
OS6900-T Models	4GB	2GB
OS6900-Q32	8GB	2GB
OS6900-X72	8GB	4GB
OS10K	4GB	2GB
OS6860(E)	2GB	2GB
OS6865	2GB	2GB
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 the 8.3.1.R01 AOS 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 6900-X20/X40 – AOS Release 8.3.1.314.R01(GA)

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

OmniSwitch 6900-T20/T40 – AOS Release 8.3.1.314.R01(GA)

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

OmniSwitch 6900-Q32 – AOS Release 8.3.1.314.R01(GA)

Hardware	Minimum UBoot Release	Minimum FPGA Release
CMM All Expansion Modules	7.3.4.277.R01 N/A	0.1.8 N/A

OmniSwitch 6900-X72 – AOS Release 8.3.1.314.R01(GA)

Hardware	Uboot	FPGA
CMM All Expansion Modules	7.3.4.31.R02 N/A	0.1.10 N/A

OmniSwitch 10K – Release 8.3.1.314.R01(GA)

Module	Uboot	FPGA
CMM	7.2.1.266.R02	2.0
GNI-C48/U48	7.2.1.266.R02	0.7
GNI-U48 Daughter Card	7.2.1.266.R02	1.4
XNI-U32S	7.2.1.266.R02	2.12
XNI-U16L	7.3.1.325.R01	0.3
XNI-U16E	7.3.1.325.R01	0.3
XNI-U32E	7.3.1.325.R01	0.3
QNI-U4E	7.3.1.325.R01	0.3
QNI-U8E	7.3.1.325.R01	0.3

OmniSwitch 6860(E) – AOS Release 8.3.1.314.R01(GA)

Hardware	Uboot	FPGA
OS6860/OS6860E (except U28)	8.1.1.70.R01	Version 0.9
OS6860E-U28	8.1.1.70.R01	Version 0.14

OmniSwitch 6865 – AOS Release 8.3.1.314.R01(GA)

Hardware	Uboot	FPGA
OS6865-P16X	8.3.1.125.R01	0.14

OmniSwitch 9900 – AOS Release 8.3.1.314.R01(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	8.3.1.103.R01	1.3.0	0.6
OS99-XNI-U48	8.3.1.103.R01	2.9.0	0.8

[IMPORTANT] *MUST READ*: AOS Release 8.3.1.R01 Prerequisites and Deployment Information

General Information

- The OS9900 is being introduced in this release. AOS Release 8.3.1.R01 is a General Availability(GA) release for the OS9900. AOS Release 8.3.1.R01 has a combination of General Availability(GA) and Early Availability(EA) features for the OS9900.

  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.

- AOS Release 8.3.1 is a General Availability (GA) release for the OS6865 platforms. The OS6865 is being introduced in this release and supports a similar feature set as the OS6860(E).

- AOS Release 8.3.1.R01 is a General Availability(GA) release for the OS6900 and OS10K platforms. It supports the same features supported in 7.3.4.R02 as well as new features introduced in 8.3.1.R01.

- AOS Release 8.3.1 is a General Availability(GA) release for the 6860(E) platforms. It supports the same features supported in 8.2.1.R01 as well as new features introduced in 8.3.1.R01.

- Please refer to the Feature Matrix in Appendix A for detailed information on supported features for each platform.

- Prior to upgrading to AOS Release 8.3.1.R01 please refer to Appendix B for important best practices, prerequisites, and step-by-step instructions.

Additional Information

- The Advanced Routing license is included by default on the 6860E and 6865 platforms in 8.3.1.R01.

- All switches that ship from the factory with AOS Release 8.3.1 will default to VC mode 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.

- The OS9900 supports both the RJ-45 console connection and the micro-USB console connection. However, the micro-USB console cannot be used at the same time as the RJ-45 console connection.

- The OmniSwitch BPS (OS-BPS) is no longer supported beginning with AOS Release 8.3.1.R01.

- When upgrading from 7.3.3.R01 or earlier AOS builds to 8.3.1.R01, if the **'unp port'** command exists in the switch configuration file it will not get converted to the updated **'unp port port-type'** command (PR 212985).
    - If upgrading from 7.3.3.R01 all **'unp port'** commands without the **'port-type'** parameter should be reconfigured to **'unp port port-type'** prior to upgrading.
    - If upgrading from 7.3.2.R01 or earlier all **'unp port'** commands without the **'port-type'** parameter must be reconfigured to **'unp port port-type'** after upgrading since the parameter was not supported until 7.3.3.R01.

Demo License Operation

A 45-day Demo Advanced license is available. This license may or may not be automatically activated depending on the switch configuration. See the table below for an explanation of the switch behavior with the Demo Advanced license.

	Standalone/VC-1	VC-2 or more	Comments
Demo Advanced License Installation	**Demo Advanced License** Automatically activated upon boot up if no Advanced license is already installed and no vcboot.cfg file exists in the Certified directory or the file size is zero bytes.	**Demo Advanced License** Automatically activated upon boot up if no Advanced license is already installed and no vcboot.cfg file exists in the Certified directory or the file size is zero bytes.	
Reboot Behavior After Demo License Expiration	If no Advanced features were ever enabled. – **Switch will not reboot.**	If no Advanced features were ever enabled. – **Switch will reboot.**	VC-1 or standalone does not require the Advanced license. VC-2 or more requires Advanced license.
	If Advanced features were enabled (even if the configurations were cleared or disabled before 45-day demo period). **- Switch will reboot.**	If Advanced features were enabled (even if the configurations were cleared/disabled before 45 days demo period). – **Switch will reboot**	
	If permanent license is installed before the expiration of demo license. – **Switch will not reboot.**	If permanent license is installed before the expiration of demo license. **- Switch will not reboot**	

Licensed Features

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

	License Required?					
	OS10K	OS9900	OS6900	OS6860(E)	OS6865	Notes
Data Center Features						
DCB (PFC,ETS,DCBx)	Yes	N/S	Yes	N/S	N/S	
EVB	Yes	N/S	Yes	N/S	N/S	
FIP Snooping	Yes	N/S	Yes	N/S	N/S	
FCoE VXLAN	N/S	N/S	Yes	N/S	N/S	
Advanced Features						
SPB	Yes	N/S	Yes	Yes	Yes	
Virtual Chassis	Yes	N/S	Yes	No	No	No license required for VC of 1
VxLAN Snooping	Yes	N/S	Yes	N/S	N/S	
IPSec	Yes	N/S	Yes	Yes	Yes	
OSPF v2/v3	No	No	Yes	Yes	Yes	
RIPng	No	N/S	Yes	Yes	Yes	
BGP	Yes	N/S	Yes	Yes	Yes	
IS-IS v4/v6	Yes	N/S	Yes	Yes	Yes	
Policy-Based Routing	No	N/S	Yes	Yes	Yes	
IPv6 static routing	No	N/S	Yes	No	No	
PIM-DM	No	No	Yes	Yes	Yes	
PIM-SM	No	N/S	Yes	Yes	Yes	
DVMRP	No	N/S	Yes	Yes	Yes	
VRRP/VRRPv3	No	N/S	Yes	No	No	
VRF	No	N/S	Yes	Yes	Yes	
U16L						
OS10K-XNI-U16	U16L	N/A	N/A	N/A	N/A	

- The Advanced license is included in this release and always active on the OS6865.
- The Advanced license is included in this release but must be activated on an OS6860E with the command **license apply file *license.dat.***
    - There is a default “license.dat” file included or one can be manually created. The file can be empty.
    - Upon successful installation the Advanced license is applied at runtime, no reboot required.
    - If part of a VC, the OS6860 non-E models must still have a valid license key.
    - If the Advanced demo license is activated it must be deactivated first.

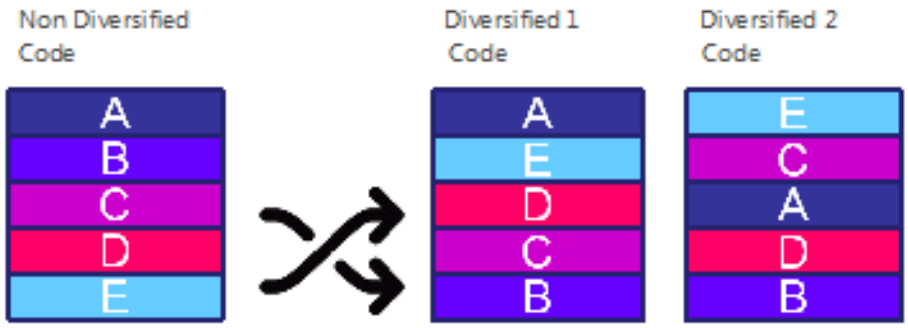
CodeGuardian

Alcatel-Lucent Enterprise and LGS Innovations have combined to provide the first network equipment to be hardened by an independent group. CodeGuardian promotes security and assurance at the network device level using independent verification and validation of source code, software diversification to prevent exploitation and secure delivery of software to customers.

CodeGuardian 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 randomizes the executable program so that various instances of the same software, while functionally identical, are arranged differently. The CodeGuardian solution rearranges internal software while maintaining the same functionality and performance and modifies the deliverable application to limit or prevent/impede software exploitation. There will be up to 5 different diversified versions per GA release of code.



CodeGuardian AOS Releases

Standard AOS Releases	AOS CodeGuardian Release	LGS AOS CodeGuardian Release
AOS 8.3.1.R01	AOS 8.3.1.RX1	AOS 8.3.1.LX1

- X=Diversified image 1-5
- ALE will have 5 different diversified images per AOS release (R11 through R51)
- Our partner LGS will have 5 different diversified images per AOS release (L11 through L51)

New Hardware Support

OmniSwitch 9900

The OmniSwitch 9900 (OS9900) Modular LAN chassis platform is a high-capacity, high-performance modular Ethernet LAN switch. The OmniSwitch 9900 series offers a broad range of modules supporting 1-GigE, 10-GigE and 40-GigE ports in an 11-RU chassis form factor.

OS9907 Chassis

- 7 Slots – Front-facing
- 2 Slots – Chassis management module (CMM)
- 6 Slots – Network interface (NI). Slot 2 is universal and can be used for a CMM or NI.
- 4 Slots – Rear-facing for chassis fabric modules (CFM)
- 3 Slots – Rear-facing for fan trays
- 4 Slots – Front facing for power supplies

OS9907-CMM
Chassis management module with USB port, RJ-45 EMP port, RJ-45/micro-USB console port, 2 QSFP+ ports.
Note: The QSFP+ ports are not supported in this release.

OS99-CFM
Chassis fabric module provides the switching fabric for the chassis.
Note: This release supports two CFMs only.

OS99-GNI-48
Provides 48 RJ-45 10/100/1000-BaseT ports.

OS99-GNI-P48
Provides 48 RJ-45 10/100/1000-BaseT PoE ports. Provided 8 ports of HPoE (75W) and 40 ports of 802.3at (30W).

OS99-XNI-48
Provides 48 RJ-45 1/10-GigE BaseT ports.

OS99-XNI-U48
Provides 48 1/10GigE SFP+ ports.

OS99-PS-A
AC power supply auto-ranging from 110VAC to 240VAC providing 1200W at 110VAC and 3000W at 240VAC.

OS99-PS-D
DC power supply providing up to 2500W of power with 40VDC to 72VDC.

OS9907-FAN-TRAY
Modular fan tray with 3 fans.

Note: Mixing of AC and DC power supplies is not supported. Mixing of Hi (240VAC) and Low (110VAC) input is not supported.

OmniSwitch 6865-P16X

The OmniSwitch 6865 is a 1-GigE and 10-GigE platform designed for demanding electrical & severe temperature environments. Fixed-configuration, hardened, fan-less chassis in a 2U form factor.

- Twelve (12) RJ-45 10/100/1000-BaseT PoE ports. Supports 4 ports of HPoE (75W) and 8 ports of 802.3at (30W)
- Two (2)1000 Base-X SFP ports
- Two (2) SFP+ (1G/10G) ports
- USB port
- RJ-45 console port
- Two (2) power supply connectors for external power supplies
- Operates at a wider temperature range from -40°C to 65°C. (74°C with airflow)
- **OS6865-BP -** AC power supply providing 180W of system and PoE power
    - One power supply provides up to 140W of PoE power
    - Two power supplies provide up to 150W of PoE power

Note: The maximum supported PoE power is 150W even with two power supplies installed.

Transceivers

OmniSwitch 6865	OmniSwitch 9900
iSFP-GIG-SX	SFP-GIG-SX
iSFP-GIG-LX	SFP-GIG-LX
iSFP-GIG-LH40	SFP-GIG-LH40
iSFP-GIG-LH70	SFP-GIG-LH70
iSFP-GIG-BX-D	SFP-GIG-T
iSFP-GIG-BX-U	SFP-GIG-EXTND
iSFP-GIG-T	SFP-GIG-BX-D
iSFP-10G-SR	SFP-GIG-BX-U
iSFP-10G-LR	SFP-10G-SR
iSFP-10G-ER	SFP-10G-LR
iSFP-10G-C*	SFP-10G-ER
	SFP-10G-LRM
	SFP-10G-ZR
	SFP-10G-C*
	SFP-10G-24DWD80
	SFP-10G-GIG-SR
	SFP-10G-GIG-LR

* Check for availability of lengths.

New Software Features and Enhancements

The following software features are being introduced with the 8.3.1.R01 release, subject to the feature exceptions and problem reports described later in these release notes. Features listed as 'Base' are included as part of the base software and do not require any license installation. Features listed as 'Advanced' or "Data Center" require the installation of a license.

8.3.1.R01 New Feature/Enhancements Summary

Feature	Platform	License
Access Guardian CLI Changes	OS10K/6900/6860/6865	N/A
Private VLANs	OS10K/9900(EA)/6900/6860/6865	N/A
Support for Port Groups having LAG members in ACL	OS6900/6860/6865	N/A
Support for QSP Profile Configuration on VFL Ports	OS6860/6865	N/A
Transparent bridging on NNI port	OS6860/6865	N/A
L2 Control protocol tunneling	OS6860/6865	N/A
FIPS	All	N/A
Common Criteria	All	N/A
NIS Requirements	All	N/A
CodeGuardian	OS10K/9900/6900/6860E/6865	N/A

Access Guardian CLI Changes

The 8.3.1 release unifies the CLI syntax from the 7.x and 8.x releases to provide a new, streamlined CLI syntax for Access Guardian commands. Previous commands were tightly coupled with the underlying technology that is used to create access side VLAN-port associations (VPAs) or virtual ports (VPs) for services. This caused a lot of duplication whenever new underlying technology was introduced (for example, additional types of UNP ports and profiles were added for different types of services).

The new CLI syntax is agnostic to the underlying technology information. This greatly simplifies the addition of new technologies and movement of users on the access side of the network.

The 8.3.1 implementation of the new Access Guardian CLI syntax provides the following streamlined functionality:

- Two Universal Network Profile (UNP) port types: bridge and access.
- Port templates that are used to apply a pre-defined UNP port configuration to UNP bridge and access ports.
- One type of UNP profile with configurable attributes. This also simplifies the CLI syntax used to configure additional Access Guardian functionality that requires a profile name (such as configuring UNP classification rules).

- Two types of profile mapping: VLAN or service. The independent mapping of a VLAN or service to a profile determines if the profile attributes are applied to traffic received on UNP bridge ports (VLAN-mapped profiles) or UNP access ports (service-mapped profiles).

Private VLANs

Private VLAN is a concept to bring layer two data isolation between devices on the same VLAN. The isolation improves the security and simplifies system configuration.

The private VLAN allows the creation of secondary VLANs within the primary VLAN. Usually, a regular VLAN represents a single broadcast domain, the PVLAN divides a VLAN (Primary) into sub-VLANs (Secondary), the single broadcast domain is partitioned into smaller broadcast sub domains while keeping the existing Layer 3 configuration. When you configure a PVLAN, the regular VLAN is called the primary VLAN and the sub-VLANs are called secondary VLANs.

Note: IP multicast is currently not supported with PVLANs. PVLAN is only supported in STP Flat mode and the MSTP protocol.

Support for Port Groups having LAG members in ACL
QoS port groups being used in ACLs can now contain link aggregation members.

Support for QSP Profile Configuration on VFL Ports

QSP profiles can now be configured on VFL ports.

Transparent Bridging on NNI port
The transparent bridging enhancement associates NNI ports with all VLANs (1 - 4094) even if they are not created in the switch. Currently AOS can support this by creating all possible VLANs (1 – 4094) and associating them to NNI ports. The transparent bridging enhancement has an advantage over the conventional configuration approach by reducing the administrative effort of configuring VLANs from 1 to 4094 and associated VPAs. Transparent bridging associates all VLANs from 1 to 4094 to the specified NNI port and spanning tree group 1. This feature is typically limited to a “ring” topology where there are only 2 NNI ports/LAGs per switch.

Note: Transparent bridging is only supported in STP Flat mode and the RSTP protocol.

L2 Control protocol tunneling
The new L2TP control prototocl tunneling has new behavior.

FIPS Encryption

Federal Information Processing Standards (FIPS) is a mode of operation that satisfies security requirements for cryptographic modules. When FIPS mode is enabled on OmniSwitch, FIPS 140-2 compliant encryption is used by the OmniSwitch devices in the various management interfaces such as SFTP, SSH and SSL.
As per the National Institute of Standards and Technology (NIST), FIPS 140-2 standard, strong cryptographic algorithms has to be supported to achieve FIPS compliance. These strong cryptographic algorithms ensure secure communication with the device to provide interoperable, high quality, cryptographically-based security for IP networks through the use of appropriate security protocols, cryptographic algorithms, and keys and prevent any form of hijacking/ hacking or attack on the device through the secure mode of communication.
FIPS mode functionalities:

- FIPS operates in OpenSSL mode allowing only highly secure and strong cryptographic algorithms.
- Switch management protocols such as SFTP, SSH, and SSL use the FIPS 140-2 compliant encryption algorithms.

- OpenSSH and Web Server which use the OpenSSL as the underlying layer for secure communications also works in the FIPS mode.
- The FIPS mode is enabled/disabled only with a reboot of the switch.

Common Criteria

The Common Criteria for Information Technology Security Evaluation (CC), and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Arrangement (CCRA), which ensures that:

- Products can be evaluated by competent and independent licensed laboratories so as to determine the fulfillment of particular security properties, to a certain extent or assurance
- Supporting documents, are used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying specific technologies.
- The certification of the security properties of an evaluated product can be issued by a number of Certificate Authorizing Schemes, with this certification being based on the result of their evaluation;

These certificates are recognized by all the signatories of the CCRA. The CC is the driving force for the widest available mutual recognition of secure IT products.

NIS Requirements

ASA Enhanced mode allows configuration of enhanced security restrictions to the OmniSwitch. This enhanced switch access mode adds new features for switch authentication. This feature provides the following functionality:

- Improved password policies and lockout setting for the users.
- Restricts access to the switch only for certain IP addresses (configured as management station), bans those IP addresses permanently from further access on invalid authentication attempts reaching threshold limit.
- Provides option to configure privileges for all access types, align IP services dynamically with AAA authentication configuration.
- Restricts only one session per user.
- Option for password obscuring to prohibit disclosure while entering the password.
- Option to configure user passwords with SHA-224/256 (SHA-2) or SHA-2+AES encryption.
- SSH/SSL Pub Key hashed with SHA2.
- Separate user password for SNMPv3 frame authentication/encryption.
- Supports both DSA 1024 and RSA 2048 public key algorithms for SSH private and SSH public keys.
- Provides option to verify the integrity of the images in a given directory is matching with the SHA-2 (SHA256 or 512 key) shared along with the image file.
- Process Self-Test functional commands to view the major hardware and software process status.
- Support of TLS 1.2 version for TLS connections.
- Valid ASA credentials need to be provided to access SWLOG content.

IP Multicast Changes
The OmniSwitch 9900 multicast functionality works differently than on other OmniSwitch platforms supported in AOS Release 8.3.1.R01. The OS9900 contains separate bridge and routing engines and the multicast software has to maintain the state in both of them to ensure proper multicast functionality.

Due to the architectural differences of the OS9900 the **show ip multicast source** and **show ip multicast forward** commands behave differently. These commands are only valid when multicast routing is enabled. You will be able to see sources on all interfaces that are enabled for multicast routing, but you will only see the forward state for the RPF interface as determined by multicast routing.

- **show ip multicast forward** –Will display the forwarding state for the RPF interface as determined by multicast routing.
- **show ip multicast source** – Will display the sources on all interfaces that are enabled for multicast routing.

To provide similar capability as other platforms the **show ip multicast bridge** and **show ip multicast bridge-forward** commands have been introduced in 8.3.1.R01 for the OS9900. These commands can be used to display the forwarding database on an OS9900.

Additionally, AOS Release 8.3.1.R01 introduces a new **ip multicast forward-mode** command for all platforms which can be used to select how traffic is classified in the forwarding database. The options are:

- **asm** - Sets the IPMS forwarding mode to ASM (the bridge lookup is based on the packet group destination IP address).
- **ssm** -Sets the IPMS forwarding mode to SSM (the bridge lookup is based on the packet source IP as well as the group destination IP).
- **mac** - Sets the IPMS forwarding mode to MAC address (the bridge lookup is based on the MAC destination address). This parameter option is supported only on the OmniSwitch 9900.
- **auto** - Automatically determines the IPMS forwarding mode based on the current IGMP protocol version and the existing protocol state (default).

See the examples below based on IGMPv2.

```
-> show ip multicast bridge vlan 130
Total 1 Bridge Entries
Interface    Type         Group Address    Host Address    UpTime   Action
-----------+------------+----------------+---------------+--------+---------
vlan 130     asm          225.0.0.1                       8576     forwarding


-> show ip multicast bridge-forward vlan 130
Total 1 Bridge Forwarding Entries
Interface    Type         Group Address     Host Address      Next Interface   UpTime
-----------+------------+-----------------+-----------------+----------------+--------
vlan 130     asm          225.0.0.1                           1/3/25           8589


-> ip multicast vlan 130 forward-mode mac

-> show ip multicast bridge-forward vlan 130
Total 1 Bridge Forwarding Entries
Interface    Type         Group Address     Host Address      Next Interface   UpTime
-----------+------------+-----------------+-----------------+----------------+--------
vlan 130     mac          01-00-5e-00-00-01                   1/3/25           2
```

Open Problem Reports and Feature Exceptions

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

System

PR	Description	Workaround
218555	Due to increased memory usage on an OS6860 the default memory threshold has been changed to 85% in 8.3.1.R01.	There is no known workaround at this time.
218846	Openflow destination MAC-based Table 2 flows may not be useable after specific configuration steps due to PVLAN being enabled by default.	Table 0/ 1 flows in Openflow can be levereged in Openflow 1.3.1, for destination mac based flows.
218895	When using FTP via the front panel ports performance will vary depending on the FTP client settings.	Use the EMP port or increase the TCP connect timeout of the FTP client.

Layer 2 / Multicast

PR	Description	Workaround
216750	If DHL session is administratively disabled retaining the linka and linkb port/linkagg STP will be disabled on these ports and traffic could continuously loop if these ports are part of a loop.	If the links belonging to a DHL admin disabled sessions are part of a loop, bring down one of the links to avoid the loop or delete the session through configuration.
219094	IPMS displays forwarding entries back to the same source vlan/port.	There is no known workaround at this time. This has no functional impact.
212367	The loop guard error state is cleared afteran NI reload.	There is no known workaround at this time. State will be updated upon receipt of BPDU.

QoS

PR	Description	Workaround
219729	The 'show qos config' command does not display the 'pending changes' field on an OS9900.	There is no known workaround at this time.
218282	On an OS9900 the log function for a policy rule is not supported. It causes the 'show qos log' command to timeout.	Command not supported at this time. There is no workaround at this time.

ISSU/Takeover/Reload

PR	Description	Workaround
210385	On an OS6860 during a VC takover, reload, or ISSU one of the VFL member ports may be detected as unassigned.	Administratively disable/enable the port.
218194	ISSU may not complete successfully on an OS6860 if the Master chassis is not the chassis with the lowest ID.	ISSU is supported on an OS6860 only when the lowest chassis ID is the Master (i.e. Chassis ID 1). If a chassis other than the lowest chassis ID is the Master, use the takeover command to make the lowest chassis ID the Master prior to performing an ISSU upgrade.
220605	During ISSU upgrade RFP over ethoam enabled ports may shutdown after a large number of port flaps.	The CCM interval should be configured to 10 seconds.
220385	On a standalone, non-VC OS-10K upon CMM takeover after ISSU, all NIs are reporting "ipni udprelay warning unknown msg 0x160019: ipni main alarm unknwn ip msg 66 (0xf400a)" messages.	This is a display issue only. Messages will stop once ISSU completes.
220420	After a slot reload on an OS9900 errors similar to "lldpNi Agent error niLldpProcessEvent" may be seen for ports that do not exist in the system.	There is no known workaround at this time. This is a display issue only. Messages will stop once the NI finishes resetting.
212985	When upgrading from 7.3.3.R01 or earlier to 8.3.1.R01 if the 'unp port' command exists in the switch configuration file it will not get converted to the new 'unp port port-type' command.	The 'unp port' commands should be reconfigured to 'unp port port-type' prior to upgrading (7.3.3.R01) or after upgrading (7.3.2.R01 and earlier).
220652	During ISSU on 6860, duplicate master condition gets triggered if 10G VFL is configured in the ring.	ISSU is not supported with a 10G VFL. Use standard upgrade.

Access Guardian

PR	Description	Workaround
220934	Recovery of users (mix of supplicant and non-supplicant) in the auth-serv-down-state happens at the rate of one user per auth-server-down-timeout duration (default: 60 seconds) instead of all the users recovering at the same time. The issue is not seen when only non-supplicant users are present.	Flush the user under the auth-serv-down profile using 'unp user flush profile <name>' or change the auth-server-down-timeout value.

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 module extractions must have a 30 second interval before initiating another hot swap activity.
- All module insertions must have a 5 minute interval AND the OK2 LED blinking green before initiating another hot swap activity.

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
OS10K-GNI-C48E	OS10K-GNI-C48E
OS10K-GNI-U48E	OS10K-GNI-U48E
OS10K-XNI-U32S	OS10K-XNI-U32S
OS10K-XNI-U16L	OS10K-XNI-U16L
OS10K-XNI-U16E	OS10K-XNI-U16E
OS10K-XNI-U32E	OS10K-XNI-U32E
OS10K-QNI-U4E	OS10K-QNI-U4E

OS10K-QNI-U8E	OS10K-QNI-U8E

OS10K 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

OS9900 Hot Swap/Insertion Compatibility

Hot Swap Procedure

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

Technical Support

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

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

Email: ebg_global_supportcenter@al-enterprise.com

Internet: Customers with service agreements may open cases 24 hours a day via the support web page at: support.esd.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 revision by slot, software revision, 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 8.3.1.R01.

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	OS10K	OS9900	OS6900	OS6860	OS6865	Notes
Management Features						
USB Console Support	N	Y	N	Y	N	
SNMP v1/v2/v3	Y	Y	Y	Y	Y	
NTP	Y	Y	Y	Y	Y	
PING and TRACEROUTE as a Read-Only user	Y	Y	Y	Y	Y	
USB Disaster Recovery	Y	EA	Y	Y	Y	
Automatic Remote Configuration / Zero touch provisioning	Y	EA	Y	Y	Y	
IP Managed Services	Y	EA	Y	Y	Y	
SSH for read-only users	Y	EA	Y	Y	Y	
VRF	Y	EA	Y	Y	Y	
VRF – DHCP Client	Y	EA	Y	Y	Y	
Automatic/Intelligent Fabric	Y	N	Y	Y	Y	
Automatic VC	Y	N	Y	Y	Y	
Bluetooth for Console Access	N	N	N	Y	N	
EEE support	N	N	Y	Y	Y	
Embedded Python Scripting / Event Manager	Y	N	Y	Y	Y	
ISSU	Y	N	Y	Y	Y	
OpenFlow	Y	N	Y	Y	N	
SAA	Y	N	Y	Y	Y	
SNMPv3 FIPS Certified Cryptographic Algorithms	N	N	N	N	N	
UDLD	Y	N	Y	Y	Y	
USB Flash	Y	N	Y	Y	Y	
Virtual Chassis (VC)	Y	N	Y	Y	Y	
VC Split Protection (VCSP)	Y	N	Y	Y	Y	
Web Services & CLI Scripting	Y	N	Y	Y	Y	
Layer 3 Feature Support						
ARP	Y	Y	Y	Y	Y	
OSPFv2	Y	Y	Y	Y	Y	
Static routing to an IP interface name	Y	Y	Y	Y	Y	
ECMP	Y	Y	Y	Y	Y	
IGMP v1/v2/v3	Y	Y	Y	Y	Y	

Feature	OS10K	OS9900	OS6900	OS6860	OS6865	Notes
PIM-DM	Y	Y	Y	Y	Y	
IPv4 Multicast Switching	Y	Y	Y	Y	Y	
Add tags to static-route command to enable easier redistribution	Y	EA	Y	Y	Y	
BGP with graceful restart	Y	EA	Y	Y	Y	
BGP route reflector for IPv6	Y	EA	Y	Y	Y	
BGP ASPATH Filtering for IPv6 routes on IPv6 peering	Y	EA	Y	Y	Y	
BGP support of MD5 password for IPv6	Y	EA	Y	Y	Y	
BGP 4-Octet ASN Support	Y	EA	Y	Y	Y	
GRE	Y	EA	Y	Y	Y	
IP-IP tunneling	Y	EA	Y	Y	Y	
IP routed port	Y	EA	Y	Y	Y	
IPv6	Y	EA	Y	Y	Y	
IPv6 DHCP relay and Neighbor discovery proxy	Y	EA	Y	Y	Y	
ISIS IPv4/IPv6	Y	EA	Y	Y	Y	
M-ISIS	Y	EA	Y	Y	Y	
OSPFv3	Y	EA	Y	Y	Y	
RIP v1/v2/NG	Y	EA	Y	Y	Y	
DHCP Server (v4, v6 with integrated support of QIP remote management)	Y	EA	Y	Y	Y	
VRRP v2/v3	Y	EA	Y	Y	Y	
ARP - Proxy	Y	N	Y	Y	Y	
ARP - Distributed	N	N	Y	N	N	
BFD	Y	N	Y	Y	Y	
DHCP Snooping	Y	N	Y	Y	Y	
DHCPv6 Relay	Y	N	Y	Y	Y	
IP Multinetting	Y	N	Y	Y	Y	
IPSec	Y	N	Y	Y	Y	
Server Load Balancing (SLB)	Y	N	Y	Y	Y	
Multicast Features						
IGMP v1/v2/v3	Y	Y	Y	Y	Y	
IPv4 Multicast Switching	Y	Y	Y	Y	Y	
PIM-DM	Y	Y	Y	Y	Y	
DVMRP	Y	N	Y	Y	Y	
IPv6 Multicast Switching (MLD v1/v2)	Y	N	Y	Y	Y	
IPv6 Scoped Multicast Addresses	Y	N	Y	Y	Y	

Feature	OS10K	OS9900	OS6900	OS6860	OS6865	Notes
PIM-SM/ PIM-SSM	Y	N	Y	Y	Y	
PIM-BiDir	Y	N	Y	Y	Y	
Monitoring/Troubleshooting Features						
Extended ping and traceroute	Y	Y	Y	Y	Y	
Port mirroring	Y	Y	Y	Y	Y	
Port monitoring	Y	Y	Y	Y	Y	
Switch logging / Syslog	Y	Y	Y	Y	Y	
RMON	Y	EA	Y	Y	Y	
SFlow	Y	EA	Y	Y	Y	
Policy based mirroring	Y	EA	Y	Y	Y	
Port mirroring - remote	Y	N	Y	Y	Y	
TDR	N	N	N	Y	N	
Layer 2 Feature Support						
802.1q	Y	Y	Y	Y	Y	
Spanning Tree (802.1ad, 802.1w, MSTP, PVST+, Root Guard)	Y	Y	Y	Y	Y	
LLDP	Y	Y	Y	Y	Y	
Link Aggregation (static and LACP)	Y	Y	Y	Y	Y	
STP Loop Guard	Y	EA	Y	Y	Y	
DHL	N	N	N	Y	Y	
ERP v1/v2	Y	N	Y	Y	Y	
HAVLAN	Y	N	Y	Y	Y	
Loopback detection – Edge (Bridge)	N	N	N	Y	Y	
Loopback detection – SAP (Access)	Y	N	Y	N	N	
MVRP	Y	N	Y	Y	Y	
Source Learning – Distributed Mode	N	N	N	N	N	
SIP Snooping	N	N	N	Y	N	
QoS Feature Support						
QSP Profiles	Y	Y	Y	Y	Y	OS9900 – QSP 1 only.
Network Groups	Y	Y	Y	Y	Y	
Per port rate limiting	Y	Y	Y	Y	Y	
802.1p / DSCP priority mapping	Y	Y	Y	Y	Y	
Auto-Qos prioritization of NMS/IP Phone Traffic	Y	Y	Y	Y	Y	

Feature	OS10K	OS9900	OS6900	OS6860	OS6865	Notes
ACL – IPv4	Y	Y[1]	Y	Y	Y	
ACL – IPv6	Y	N	Y	Y	Y	
Map Groups	Y	N	Y	Y	Y	
Policy based routing	Y	N	Y	Y	Y	
Policy Lists	Y	N	Y	Y	Y	
Port Groups	Y	N	Y	Y	Y	
Ingress bandwidth shaping	Y	N	Y	Y	Y	
Egress bandwidth shaping	N	N	N	N	N	
Switch Groups	Y	N	Y	Y	Y	
Tri-color marking	Y	N	Y	Y	Y	
Metro Ethernet Features						
Ethernet Services	Y	EA	Y	Y	Y	
Ethernet OAM (ITU Y1731 and 802.1ag)	Y	EA	Y	Y	Y	
Security Features						
Access Guardian – UNP	Y	N	Y	Y	Y	
Interface Violation Recovery	Y	EA	Y	Y	Y	
Learned Port Security (LPS)	Y	EA	Y	Y	Y	
LLDP Rogue Detection	Y	EA	Y	Y	Y	
TACACS+ Client	Y	EA	Y	Y	Y	
TACACS+ command based authorization	Y	EA	Y	Y	Y	
Accounting	Y	N	Y	Y	Y	
Application Monitoring and Enforcement (Appmon)	N	N	N	Y	N	
ARP Poisoning Protection	Y	N	Y	Y	Y	
Application Fingerprinting	Y	N	Y	N	N	
Access Guardian - BYOD	N	N	N	Y	Y	
COA Extension support for RADIUS (BYOD)	N	N	N	Y	Y	
mDNS Snooping/Relay (BYOD)	N	N	N	Y	Y	
UPNP/DLNA Relay (BYOD)	N	N	N	Y	Y	
Switch Port location information pass-through in RADIUS requests (BYOD)	N	N	N	Y	Y	
Captive Portal	N	N	N	Y	Y	
Quarantine Manager	N	N	N	Y	Y	
Radius test tool	Y	N	Y	Y	Y	
Storm Control	Y	N	Y	Y	Y	

Feature	OS10K	OS9900	OS6900	OS6860	OS6865	Notes
PoE Features						
802.1af and 802.3at	N	Y	N	Y	Y	
Auto Negotiation of PoE Class-power upper limit	N	Y	N	Y	Y	
Display of detected power class	N	Y	N	Y	Y	
LLDP/802.3at power management TLV	N	Y	N	Y	Y	
HPOE support (60W/75W)	N	Y (75W)	N	Y (60W)	Y (75W)	
POE Time Of Day Support	N	Y	N	Y	Y	
Data Center Features						
CEE DCBX Version 1.01	N	N	Y	N	N	
Data Center Bridging (DCBX/ETS/PFC)	Y	N	Y	N	N	
EVB	Y	N	Y	N	N	
FCoE / FC Gateway	N	N	Y	N	N	
FIP Snooping	Y	N	Y	N	N	
IPv4 over SPB	Y	N	Y	Y	Y	
RFP on SPB UNI port	Y	N	Y	N	N	
SPB	Y	N	Y	Y	Y	
VXLAN	N	N	Q32/X72	N	N	
VM/VXLAN Snooping	Y	N	Y	N	N	
Other Features						
Dying Gasp	N	N	N	Y	Y	
Update MAC Range for IP Phones	Y	N	Y	Y	Y	
Auto LLDP Vlan assignment for IP touch phones	N	N	N	Y	Y	

1. On the OS9900 the following ACL types are supported, all others are EA only:
   Condition: Source/destination IP, source/destination network group, source/destination tcp/udp port
   Action: disposition accept/deny, dscp

Appendix B: 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

	Upgrading from 7.3.4.270.R02 Maintenance Release or higher	**Upgrading from any other 7.X Release**
OS6900 – VC	ISSU – Supported Standard Upgrade - Supported	ISSU – Not Supported Standard Upgrade - Supported
OS6900 – Standalone	ISSU – N/A Standard Upgrade - Supported	ISSU – N/A Standard Upgrade - Supported
OS10K – VC	ISSU – Supported Standard Upgrade - Supported	ISSU – Not Supported Standard Upgrade - Supported
OS10K – Standalone (Dual-CMM)	ISSU – Supported Standard Upgrade - Supported	ISSU – Not Supported Standard Upgrade - Supported
OS10K – Standalone (Single-CMM)	ISSU – N/A Standard Upgrade - Supported	ISSU – N/A Standard Upgrade - Supported

AOS Release 7 Upgrade Paths

	Upgrading from 8.2.1.353.R01 Maintenance Release or higher	**Upgrading from any other 8.X**
OS6860-VC	ISSU – Supported Standard Upgrade - Supported	ISSU – Not Supported Standard Upgrade - Supported
OS6860-Standalone	ISSU – N/A Standard Upgrade - Supported	ISSU – N/A Standard Upgrade - Supported
Note: ISSU is supported on an OS6860 only when the lowest chassis ID is the Master (i.e. Chassis ID 1). If a chassis other than the lowest chassis ID is the Master, use the **takeover** command to make the lowest chassis ID the Master prior to performing an ISSU upgrade. (PR 218194). **Note**: ISSU is not supported with a 10G VFL. Use standard upgrade. (PR 220652)		

AOS Release 8 Upgrade Paths

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 7.3.2.568.R01 Service Release, September 05, 2014.,
  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:  FRI OCT 31 2014 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 Alcatel-Lucent 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
```

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 C for specific steps to follow.
- If upgrading a VC using ISSU please refer to Appendix D for specific steps to follow.

Appendix C: 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:

- OS10K – Ros.img, Reni.img
- OS9900 – Mos.img, Mhost.img, Meni.img
- OS6900 **-** Tos.img
- OS6860 – Uos.img
- OS6865 – Uos.img

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          8.3.1.314.R01          210697424 Alcatel-Lucent OS
```

```
-> 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
Please wait……..

-> 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 D: 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:

- OS10K – Ros.img, Reni.img
- OS9900 – Mos.img, Mhost.img, Meni.img
- OS6900 **-** Tos.img
- OS6860 – Uos.img
- OS6865 – Uos.img
- ISSU Version File – issu_version

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 affect 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.

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          8.3.1.314.R01           210697424 Alcatel-Lucent OS
```

```
OS6900-> copy running certified
Please wait.....

-> 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  : CERTIFY NEEDED
SYNCHRONIZATION STATUS
  Flash Between CMMs      : SYNCHRONIZED
  Running Configuration   : SYNCHRONIZED
```

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
Please wait.....

-> 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 E: Fixed Problem Reports

The following problem reports were closed or are in verification in AOS Release 8.3.1.R01.

187240	OS6900: Nov 3 01:46:27 AdminDC-L5-120 swlogd: portMgrNi main error(2) : [pmVcPeerRxCB:1045] Unknown
194405	VC Stabilzation - ISSU Prevalidation and 8x async sock changes
197855	[TYPE1]Pmd-EtherCmm generated in OS6900 VC-setup(master) , while testing L2mcast module . While En
200885	10K VC :: traffic stopped when Master is rebooted and joined VC as Slave
202982	While converting VC to standalone below error thrown in (OS6900 ?T20):
203406	rtr-port configured on OS6900 switch participating in spantree when running on flat mode
203474	[10k-VC]Slave Chassis not taking over after removing both CMMs on primary unit
204531	ARP Poison not working in OS 10K
205935	UNP Users are not learned after NIs reload
206331	CERT-IST/AV-2015.0452 Logjam vulnerability in Diffie-Hellman CVE-2015-4000
206664	While reloading in VC of 6 ?bootmgr error message ?seen.
206955	After reloading in virtual chassis DUT ?VcmCmm? info messages are seen & these messages are seen
208808	During ISSU of the OS6900VC, the device got isolated from network for 10mins
209960	CERT-IST/AV-2015.0788 Vulnerabilities in PHP CVE-2015-6834 CVE-2015-6835 CVE-2015-6836 CVE-2015-6837
210209	[TYPE1]dhcpv6 server: switch crashing with dhcpv6srv task failed when it switch receives dhcp discov
210354	6860E classifying client MAC under UNP MAC rule when UNP IP rule exists.
210386	OS6900: TACACS server missing from configuration
211072	Queries on command show lanpower slot 1/1 update-from
211284	Need for new CLI (unp force-l3-learning enable/disable) command enabled.
211558	LBD not working with DHL setup
212427	ICMP traffic is block due to DHCP snooping feature enabled.
213122	If the authentication server is reachable via front panel ports it is authenticated locally, but sti
213167	chassis 3,4 and 5 drop out of a VC of 8

213712	OS6900 VC takeover after adding IP interfaces and saving the changes
213754	[TYPE2]Correct DHCP options 66 & 67 sent from DHCP server seen by the switch as "NULL"
214103	OS6860 link-fault-propagation error after reboot on 8.2.1 code.
214368	OS6860 switch port going shutdown state when LLDP packet is received
214476	OS6860 Unable to ssh to the switchn using "ssh -l" command
214780	?show interface status? command in Master Split-Topology Switch displays that the interfaces are ad
215388	OS6860: Incorrect spelling for violation messages by LBD seen on swlogs
215401	Both Master and Master Split Topology holds the VC EMP Address
215699	SPB- If VLAN 1 has an IP interface, Service Port configuration is not loaded after reboot.
215709	show linkagg command output has incorrect Attached Vs Selected ports.
215717	OS6860 unable to create port monitoring in tag port
215806	Query regarding memory status in a 2XOS6900-X20 VC.
215849	mac-ping dst-mac doesnt work on bvlan
215923	NTP source interface not used even after configuration
216065	When a Master VC loss its power and rejoin the VC of 8, it rebooted 2 times before joining the VC su
216161	2 minute convergence time for 500 streams pim dense mode
216492	Need to check CVE-2016-2108 CVE-2016-2107 CVE-2016-2105 CVE-2016-2106 CVE-2016-2109 CVE-2016-2176
216509	Need to know meaning of message "VlanMgrCmm main error(2)"
216689	VC Chassis isolated after upgrade from 7.3.3.505.R01 to 7.3.4.236.R02.
216710	OSPF route flap issue
216721	Radius CLI task suspension multiple times in the PRI units of 6860.
217053	OS6860-24: No rebooting reason logged in switch logs.
217319	storm control: port is shutdown immediately once there is ONE broadcast packet.
217488	Security advisory CERT-IST/AV-2016.0374 Vulnerabilities in PHP CVE-2016-3074, CVE-2016-3078
217509	Security advisory CERT-IST/AV-2016.0451 Vulnerabilities in the "libxml2" library on Linux/Unix CVE-2

217605	?aaa test-radius-server? command selects incorrect source and NAS-IP-address IP address.
217606	Switch picks incorrect NAS-IP-address during client authentication.
217641	Script file is not taking effect in the OS_7.3.4.248.R02
217760	Unit 2 and Unit 3 in a VC of 3 OS6900 crashed due to Spin lock issue
217804	802.1x authentication failed in OS6860.
217903	SES AAA error(2) Error 3: Operation canceled [in catchAllAndLog()]
218046	ERROR: Service (11) does not exist
218055	OS10K: Unexpected BGP crash
218147	Do not forward IPv6 Network Discovery packets with hop limit not equal to 255
218231	Cannot enable sFlow Sampler on LACP port
218298	OS 6860 UNP user status shows Active with no MAC learnt
218395	OS10K is not using managed interface for TACACS request after upgrade to 734.248R02 from 732.689R01
218556	Different OID's for AlcatelIND1Base.mib
218896	IBGP in idle state due to community receivied from the ISP router
219159	clarification on dhcp relay when the dhcp reply interface is disabled
219200	OS6900 STP topology age display issue
219265	5 minutes outage on layer 3 traffic while performing issu from 734.248 - 734.273
219392	When enable accounting , for example "aaa accounting session "FR"". all accounting packet type sen
219631	OS6900 switch is not forwarding DHCP packets to server.
219642	ipmsNi ipms warning error on OS10K in a VC and Crash of the XNI-U32S NI upon forming VC
219725	Noel: unexpected reload / takeover in an OS-6860 VC
219751	swlog: ?stpCmm library(plApi) error(2) pllsGportValid@11686: Invalid port type 2? is seen in the sw
219774	2XOS6900- VM Mac-address are not learned in SPB network; multicast stale entries on takeover during
219789	OS6900 swlog error "svcCmm mMIP error" RCA
219932	2xOS10K VC the SFP "JDSU" is not working after the upgrade of VC to 7.3.4.273.R02

220107	No communication with QinQ TPID 88a8 over SPB network.
220209	Need to Check Vulnerability for the CVE-2016-5696 for 7x and 8x switches
220345	OS6900: Client not receiving IP from DHCP server over GRE