Release Notes - Rev. B

OmniSwitch 6900/6860(E)/6865

Release 8.3.1.R02

These release notes accompany release 8.3.1.R02. 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 and OS10K are not supported in this 8.3.1.R02 Release. Support will be added for these platforms in an upcoming 8.3.1.R02 Release.

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 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
OS6860(E)	2GB	2GB
OS6865	2GB	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.R02 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 8.3.1.160.R02(GA)

Hardware	Minimum UBoot	Minimum FPGA
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 8.3.1.160.R02(GA)

Hardware	Minimum UBoot	Minimum FPGA
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 8.3.1.160.R02(GA)

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

OmniSwitch 6900-X72 – AOS Release 8.3.1.160.R02(GA)

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

OmniSwitch 6860(E) – AOS Release 8.3.1.160.R02(GA)

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

OmniSwitch 6865 – AOS Release 8.3.1.160.R02(GA)

Hardware	Minimum Uboot	Minimum FPGA
OS6865-P16X	8.3.1.125.R01	0.14 (minimum) 0.22 (current)

[IMPORTANT] *MUST READ*: AOS Release 8.3.1.R02 Prerequisites and Deployment Information

General Information

- ***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.***
- 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.R02 please refer to Appendix B for important best practices, prerequisites, and step-by-step instructions.

Additional Information

- The Advanced license is included by default on the OS6865, OS6860E, and OS6900 platforms in 8.3.1.R02. It is not included on the OS6860-nonE models.
- All switches that ship from the factory with AOS Release 8.3.1.R02 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 OmniSwitch BPS (OS-BPS) is no longer supported beginning with AOS Release 8.3.1.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?			
	OS6900	OS6860(E)	OS6865	Notes
Data Center Features				
DCB (PFC,ETS,DCBx)	Yes	N/S	N/S	
EVB	Yes	N/S	N/S	
FIP Snooping	Yes	N/S	N/S	
FCoE VXLAN	Yes	N/S	N/S	
Advanced Features				
SPB	Yes	Yes	Yes	
Virtual Chassis	Yes	No	No	No license required for VC of 1
VxLAN Snooping	Yes	N/S	N/S	
IPSec	Yes	Yes	Yes	
OSPF v2/v3	Yes	Yes	Yes	
RIPng	Yes	Yes	Yes	
BGP	Yes	Yes	Yes	
IS-IS v4/v6	Yes	Yes	Yes	
Policy-Based Routing	Yes	Yes	Yes	
IPv6 static routing	Yes	No	No	
PIM-DM	Yes	Yes	Yes	
PIM-SM	Yes	Yes	Yes	
DVMRP	Yes	Yes	Yes	
VRRP/VRRPv3	Yes	No	No	
VRF	Yes	Yes	Yes	

- The Advanced license is included in this release and always active on the OS6865.
- The Advanced license is included in this release must be activated on the OS6860E and OS6900 with the command **license apply file *license.dat***.
    - There may be a default "license.dat" file included, if not, 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.

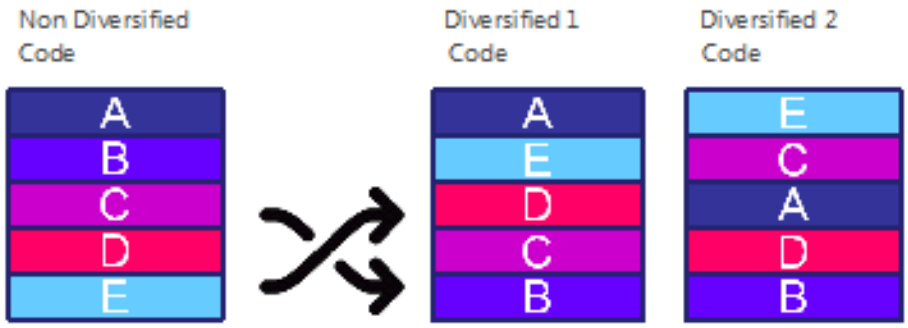
CodeGuardian

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.R02	AOS 8.3.1.RX2	AOS 8.3.1.LX2

- 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 / Updated Hardware Support

There is no new hardware in this release.

New Software Features and Enhancements

The following software features are being introduced with the 8.3.1.R02 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.R02 New Feature/Enhancements Summary

Feature	Platform	License
Secure Console for Admin Users	All	N/A

Secure Console for Admin User Only

This feature can be used to restrict all users from accessing the switch through a console session except for the 'admin' user account.

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
222310	Flash file system not visible after reload from working. Flash files are only visible from 'su' mode.	Console: 1. From 'su' (superuser), type 'ls' to verify that the flash/working and flash/certified directories and the contents (images, vcboot.cfg, vcsetup.cfg) are still available. 2. Power cycle the switch. Remote: 1. Issue 'reload from working no rollback-timeout' 2. As soon as the switch is up start holding any key to get the u-boot prompt (=>). 3. Issue the 'boot' command to reboot.
216267	Slave NI ports do not always go into violation after reaching high-threshold for unknown-unicast traffic.	There is no known workaround at this time.
222080	Dynamic unicast SDP entry is not showing up under service domain when unknown unicast traffic is sent from SAP to SAP.	There is no known workaround at this time.

Layer 2 / Multicast

PR	Description	Workaround
216750	If DHL session is administratively disabled while 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 session 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.
221870	On OS6860, dot1qVlanCurrentEgressPorts SNMP Object will show an incorrect value for Egress Port Bitmap corresponding to the VLAN.	There is no known workaround at this time.
222153	During a takeover in a VC, the chassis that was rebooted may respond to requests	Flush the MACs on the switches connected to server-cluster ports connected to the chassis

	before being fully operational causing unknown destination MACs to be flooded to edge switches which may cause server-cluster traffic connected to those edge switches to be dropped.	that did not go down during takeover or wait for MACs to age out.

QoS

PR	Description	Workaround
222853	Openflow agent (VC of 2 OS6900 X72/Q32) is sending wrong OFP_port number to controller in OFP.	There is no known workaround at this time.
222968	The traffic is not forwarded for all 224K MAC entries learned in hardware as openflow L2-dest flows. Traffic forwarding is happening only for approximately 213K flows.	There is no known workaround at this time.

ISSU/Takeover/Reload

PR	Description	Workaround
220683	After an ISSU upgrade seeing traffic loss for one or more VLANs on UNP ports.	Performing a MAC flush or port toggle helps to recover.

Virtual Chassis

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.
222554	Expansion slot extraction leads to node reload in Auto-VC setup of vc-of-6.	Remove the VFL configuration before performing hot-swap of the expansion slot.
222609	Dynamic SAP ports were not created as a part of auto-fabric process if both are AOS switches and one of them is configured as a plain L2 switch.	Enable auto-fabric globally and disable SPB protocol individually on the ports on which UNP is expected to be auto-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 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

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.R02.

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

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

Feature	OS6900	OS6860(E)	OS6865	Notes
IPv6 Multicast Switching (MLD v1/v2)	Y	Y	Y	
IPv6 Scoped Multicast Addresses	Y	Y	Y	
PIM-SM	Y	Y	Y	
PIM-SSM	Y	Y	Y	
PIM-SSM Static Map	Y	Y	Y	
PIM-BiDir	Y	Y	Y	
Monitoring/Troubleshooting Features				
Extended ping and traceroute	Y	Y	Y	
Port mirroring	Y	Y	Y	
Port monitoring	Y	Y	Y	
Switch logging / Syslog	Y	Y	Y	
RMON	Y	Y	Y	
SFlow	Y	Y	Y	
Policy based mirroring	Y	Y	Y	
Port mirroring - remote	Y	Y	Y	
TDR	N	Y	N	
Layer 2 Feature Support				
802.1q	Y	Y	Y	
Spanning Tree (802.1ad, 802.1w, MSTP, PVST+, Root Guard)	Y	Y	Y	
LLDP (802.1ab)	Y	Y	Y	
Link Aggregation (static and LACP)	Y	Y	Y	
STP Loop Guard	Y	Y	Y	
DHL	N	Y	Y	
ERP v1/v2	Y	Y	Y	
HAVLAN	Y	Y	Y	
Loopback detection – Edge (Bridge)	N	Y	Y	
Loopback detection – SAP (Access)	Y	Y	Y	
MVRP	Y	Y	Y	
Private VLANs	Y	Y	Y	
Source Learning – Distributed Mode	N	N	N	
SIP Snooping	N	Y	N	
QoS Feature Support				
QSP Profiles	Y	Y	Y	

Feature	OS6900	OS6860(E)	OS6865	Notes
Per port rate limiting	Y	Y	Y	
802.1p / DSCP priority mapping	Y	Y	Y	
Auto-Qos prioritization of NMS/IP Phone Traffic	Y	Y	Y	
ACL – IPv4	Y	Y	Y	
ACL – IPv6	Y	Y	Y	
MAC Groups	Y	Y	Y	
Network Groups	Y	Y	Y	
Port Groups	Y	Y	Y	
Service Groups	Y	Y	Y	
Map Groups	Y	Y	Y	
Switch Groups	Y	Y	Y	
Policy Lists	Y	Y	Y	
Policy based routing	Y	Y	Y	
Ingress/Egress bandwidth limit	Y	Y	Y	
Tri-color marking	Y	Y	Y	
QSP Profiles 2/3/4	Y	Y	Y	
Metro Ethernet Features				
Ethernet Services	Y	Y	Y	
Ethernet OAM (ITU Y1731 and 802.1ag)	Y	Y	Y	
Security Features				
Access Guardian – UNP	Y	Y	Y	
Access Guardian - BYOD	N	Y	Y	
Interface Violation Recovery	Y	Y	Y	
Learned Port Security (LPS)	Y	Y	Y	
LLDP Rogue Detection	Y	Y	Y	
TACACS+ Client	Y	Y	Y	
TACACS+ command based authorization	Y	Y	Y	
Accounting	Y	Y	Y	
Application Monitoring and Enforcement (Appmon)	N	Y	N	
ARP Poisoning Protection	Y	Y	Y	
Application Fingerprinting	Y	N	N	
COA Extension support for RADIUS (BYOD)	N	Y	Y	
mDNS Snooping/Relay (BYOD)	N	Y	Y	
UPNP/DLNA Relay (BYOD)	N	Y	Y	

Feature	OS6900	OS6860(E)	OS6865	Notes
Switch Port location information pass-through in RADIUS requests (BYOD)	N	Y	Y	
Captive Portal	N	Y	Y	
Quarantine Manager	N	Y	Y	
Radius test tool	Y	Y	Y	
Storm Control	Y	Y	Y	
PoE Features				
802.1af and 802.3at	N	Y	Y	
Auto Negotiation of PoE Class-power upper limit	N	Y	Y	
Display of detected power class	N	Y	Y	
LLDP/802.3at power management TLV	N	Y	Y	
HPOE support (60W/75W)	N	Y (60W)	Y (75W)	
POE Time Of Day Support	N	Y	Y	
Data Center Features				
CEE DCBX Version 1.01	Y	N	N	
Data Center Bridging (DCBX/ETS/PFC)	Y	N	N	
EVB	Y	N	N	
FCoE / FC Gateway	Y	N	N	
FIP Snooping	Y	N	N	
IPv4 over SPB	Y	Y	Y	
RFP on SPB UNI port	Y	N	N	
SPB	Y	Y	Y	
VXLAN	Q32/X72	N	N	
VM/VXLAN Snooping	Y	N	N	
Other Features				
Dying Gasp	N	Y	Y	
Update MAC Range for IP Phones	Y	Y	Y	
Auto LLDP Vlan assignment for IP touch phones	N	Y	Y	

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 one of the last four 7.3.4.R02 Maintenance Release Builds: (270,273,299,310).	**Upgrading from any other 7.X Release**
OS6900 – VC	ISSU – Supported Standard - Supported	ISSU – Not Supported Standard - Supported
OS6900 – Standalone	ISSU – N/A Standard - Supported	ISSU – N/A Standard - Supported

AOS Release 7 Upgrade Paths

	Upgrading from 8.3.1.R01 GA	**Upgrading from 8.2.1.353.R01 Maintenance Release or higher**	**Upgrading from any other 8.X Release**
OS6860-VC	ISSU – Supported Standard - Supported	ISSU – Supported Standard - Supported	ISSU – Not Supported Standard - Supported
OS6860-Standalone	ISSU – N/A Standard - Supported	ISSU – N/A Standard - Supported	ISSU – N/A Standard - Supported
OS6900 – VC	ISSU – Supported Standard - Supported	N/A	ISSU – Not Supported Standard - Supported
OS6900 – Standalone	ISSU – N/A Standard - Supported	N/A	ISSU – N/A Standard - Supported
OS6865 - VC	ISSU – Supported Standard - Supported	N/A	N/A
OS6865 - Standalone	ISSU – N/A Standard - Supported	N/A	N/A

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:

- OS6900 - Tos.img
- OS6860 – Uos.img
- OS6865 – Uos.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. (**Note**: This document will be available at a future date after completion of Common Criteria certification).

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          8.3.1.160.R02          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:

- OS6900 **-** Tos.img
- OS6860 – Uos.img
- OS6865 – Uos.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**: This document will be available at a future date after completion of Common Criteria certification).

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. 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          8.3.1.160.R02           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.R02.

PR	Summary
209918	Fix done under PR 197661 (tx loss frames on SPB interface ports) not working for SNMP.
211072	Queries on command show lanpower slot 1/1 update-from.
211111	OS6900: DDM issue: Input value is 0 when unidirectional failure happens.
211133	kernel: [689541.680000] error writing 94 to 13, read back fffffff5/-11 ret -11 count 5.
211558	LBD not working with DHL setup.
213122	If the authentication server is reachable via front panel ports it is authenticated locally, but still tries to authenticate via ASA.
214291	aaa accounting packet from the switch not honoring the user-name received from radius in a non-supplicant authentication.
215317	switch crashed due trapmgr stack while revmoing snmp configuration from switch.
215347	OS6900 no mac address learnt on Linkagg port.
215517	8.x SSH session syslog missing the host name, need to be similar to 6.x.
218434	unable to create static SAP when the dynamic rule is active on the switch.
219596	Security advisory CERT-IST/AV-2016.0702 Vulnerabilities in PHP CVE-2016-5399, CVE-2016-6207 – Fixed.
220674	Memory leak on OS6860 when running a script to take show log swlog slot 1/1 output.
220685	OS6860E: Interface range error.
220850	OS6900 - Continuous error logs "pmmnid library(plApi) error".
221069	Need to check ssh vulnerability- Strong ciphers and hmac ciphers on 8x switch.
221081	OS10K chassis has lost SNMP access to OV2500 server.
221306	Split-Topology status seen on Main VC's slaves.
221349	831R01-CCE: RSA key not generated when "cert.d" directory is not available in "/flash/switch" directory.
221367	VCSP doesn’t work after takeover on a VC of 4.
221478	SSH key changes on a VC on takeover.
221502	The OS6900 switch is using "Acconting-On" message in radius packet (accounting packets) instead of "Start” message.

221532	6860: Cannot apply "unp port port-template" on a range of ports.
221558	OS6900 running 7.3.4.273.R02 SSH to loopback/vlan IP address not possible until ICMP packet send.
221570	OS6860: UNP Port shows as blocking and device unreachable.
221581	SSH connection issue between OS9700 and OS6860 with the AOS 8.3.1.314.R01.
221585	On OS9900 the output of "show power supply" and "show chassis" are not consistent in regard to the regard to the remaining power.
221592	VC of 2X6900: IP connectivity issue over on SPB BEB.
221672	The information in the "About" page on switch's webview is outdated.
221673	bcmd sdk info(5) Parity error seen on OS6860.
221675	Unable to ping the device which falls under the default UNP profile.
221760	OS6900: Query on Maximum number of link aggregation groups.
221784	OS6900 VC - Kernel Warning due to deletion of alive ARP.
221863	OS9900- The "copy running certified flash-synchro" does not synchronize the chassis.
221866	OS9900 -Autoneg disabled does not apply on OS99-GNI-48 even when the port running at 100/1000.
222019	Errors seen on OS6860 Switches lGetGportFromChassisSlotUnitDport@2448: Port not found (chassis 1, slot 1, unit 0, dport 25)
222081	LGS 178-181: Possible exploit due to mempy without bounds check in Radius interface. LGS "Important”.
222114	OS6900 - Continuous "cp: write error: No space left on device" and slow telnet connectivity.
222165	OS6860 need explanation about the swlog.
222294	OS6860 needs to know why the check box present on the Captive Portal page on 8.3.1.
222428	PC is getting classified in default vlan.
222633	OS10K VC went down root cause analysis.
222744	Unable to configure qos qsi on linkagg-0.
222769	switches rebooted due to high memory due to appMonNi task.
222791	Loss of OSPF routes on the OS10K.