Release Notes - Rev. A

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

Release 8.5R1

These release notes accompany release 8.5R1. These release notes provide important information on individual software features and hardware modules. Since much of the information in these release notes is not included in the hardware and software user manuals, it is important that you read all sections of this document before installing new hardware or loading new software.

Note – The OS9900 is not supported in AOS Release 8.5R1.
(The OS9900 is referenced in the 8.5R1 user guides but is not a supported platform in AOS Release 8.5R1)

Contents

Related Documentation

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

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

System Requirements

Memory Requirements

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

Platform	SDRAM	Flash
OS6465	1GB	1GB
OS6560	2GB	2GB
OS6860(E)	2GB	2GB
OS6865	2GB	2GB
OS6900-X Models	4GB	2GB
OS6900-T Models	8GB	2GB
OS6900-Q32	8GB	4GB
OS6900-X72	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 this AOS release software available from Service & Support.

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

OmniSwitch 6465 – AOS Release 8.5.164.R01(GA)

Hardware	Minimum UBoot	Minimum FPGA
OS6465-P6	8.5.83.R01	0.10
OS6465-P12	8.5.83.R01	0.10

OmniSwitch 6560 – AOS Release 8.5.164.R01(GA)

Hardware	Minimum Uboot	Minimum FPGA
OS6560-P24Z24	8.4.1.23.R02	0.6 (0x6)
OS6560-P24Z8	8.4.1.23.R02	-
OS6560-P48Z16	8.4.1.23.R02	0.6
OS6560 (Non-PoE Models)	8.5.83.R01	0.7

OmniSwitch 6860(E) – AOS Release 8.5.164.R01(GA)

Hardware	Minimum Uboot	Minimum FPGA*
OS6860/OS6860E (except U28)	8.1.1.70.R01	0.9 (0x9)
OS6860E-U28	8.1.1.70.R01	0.20 (0x14)
OS6860E-P24Z8	8.4.1.17.R01	0.5 (0x5)

***Note**: In previous AOS releases the FPGA version was displayed in hexadecimal format.
Beginning in 8.4.1.R01 it is displayed in decimal format.

OmniSwitch 6865 – AOS Release 8.5.164.R01(GA)

Hardware	Minimum Uboot	Minimum FPGA*
OS6865-P16X	8.3.1.125.R01	0.20 (0x14) (minimum) 0.22 (0x16) (current)
OS6865-U12X	8.4.1.17.R01	0.23 (0x17)
OS6865-U28X	8.4.1.17.R01	0.11 (0xB)

***Note**: In previous AOS releases the FPGA version was displayed in hexadecimal format.
Beginning in 8.4.1.R01 it is displayed in decimal format.

OmniSwitch 6900-X20/X40 – AOS Release 8.5.164.R01(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 8.5.164.R01(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 8.5.164.R01(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 8.5.164.R01(GA)

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

[IMPORTANT] *MUST READ*: AOS Release 8.5R1 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 please refer to Appendix B for important best practices, prerequisites, and step-by-step instructions.
- Beginning in 8.5R1, VLAN 4092 is now a reserved VLAN on all OS6560 models for future feature support and can no longer be used for user traffic. If VLAN 4092 is configured on any OS6560 models, please reconfigure the switch to use a different VLAN before upgrading to 8.5R1.
- Some switches that ship from the factory with AOS Release 8.5R1 will default to VC mode (requiring a vcboot.cfg configuration file) and attempt to run the automatic VC, automatic remote configuration, and automatic fabric protocols. Please note that since the switches default to VC mode, automatic remote configuration does not support the downloading of a 'boot.cfg' file, only the 'vcboot.cfg' file is supported.

Note: None of the ports on the OS6865 or OS6465 models default to auto-vfl so automatic VC will not run by default on newly shipped switches. However, automatic remote configuration and automatic fabric will run by default.

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

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

Licensed Features

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

	Data Center License Installation Required?
	OmniSwitch 6900
Data Center Features	
DCB (PFC,ETS,DCBx)	Yes
EVB	Yes
FIP Snooping	Yes
FCoE VXLAN	Yes
Note: All other platforms do not support Data Center features.	

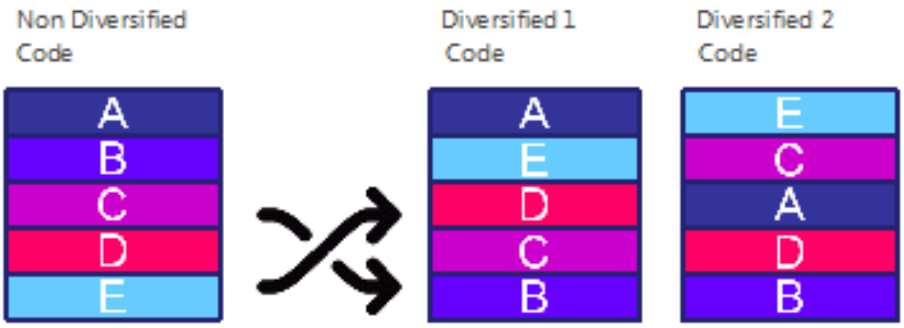
CodeGuardian

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 3 different diversified versions per GA release of code.



CodeGuardian AOS Releases

Standard AOS Releases	AOS CodeGuardian Release	LGS AOS CodeGuardian Release
AOS 8.5.R01	AOS 8.5.RX1	AOS 8.5.LX1

- X=Diversified image 1-3
- ALE will have 3 different diversified images per AOS release (R11 through R31)
- Our partner LGS will have 3 different diversified images per AOS release (L11 through L31)

Please contact customer support for additional information.

New / Updated Hardware Support

The following new hardware is being introduced in this release.

OmniSwitch 6560-24Z8
Fixed configuration chassis in a 1U form factor with:

- Sixteen (16) - 10/100/1000 BaseT ports
- Eight (8) - 100/1000/2.5G Base-T ports
- Two (2) - SFP+ (1G/10G) ports
- USB port
- RJ-45 console port

OmniSwitch 6560-24Z24
Fixed configuration chassis in a 1U form factor with:

- Twenty-four (24) - 100/1000/2.5G Base-T ports
- Four (4) - SFP+ (1G/10G) ports
- Two (2)- 20G virtual chassis VFL ports
- USB port
- RJ-45 console port

OmniSwitch 6465-P6
Fixed configuration, fanless, din-mountable, industrial hardended chassis:

- Four (4) - 10/100/1000 BaseT 802.3at PoE+ ports (Two ports support 60W HPoE)
- Two (2) - SFP 100/1000FX ports
- USB port
- RJ-45 console port
- Two (2) Alarm connectors (1-input, 1-output)

OmniSwitch 6465-P12
Fixed configuration, fanless, din-mountable, industrial hardended chassis:

- Eight (8) - 10/100/1000 BaseT 802.3at PoE+ ports (Four ports support 60W HPoE)
- Four (4) - SFP 100/1000FX ports
- USB port
- RJ-45 console port
- Two (2) Alarm connectors (1-input, 1-output)

OS6465-BPN-H
Din-mountable, 180W AC power supply providing both system and up to 150W of PoE power.

OS6465-BPN
Din-mountable, 75W AC power supply providing both system and up to 45W of PoE power.

Note: The OS6465-P6 and OS6465-P12 models can work with a third party power supply as long as the power supply complies with defined system power specification. Please refer to the datasheet and Hardware Users Guide for more information.

Transceivers

Support for the following transceivers has been added to this release for the platforms listed below. Please refer to the Transceivers Guide for additional details on other existing transceivers and the supported platforms.

Platform Support	Transceivers	
OS6465-P6/P12	ISFP-GIG-SX	ISFP-100-MM
	ISFP-GIG-LX	ISFP-100-SM15
	ISFP-GIG-LH40	ISFP-100-SM40
	ISFP-GIG-LH70	
	ISFP-GIG-BX-D	
	ISFP-GIG-BX-U	
	ISFP-GIG-T	
OS6560-24Z8/24Z24/48Z16	Supports the same transceivers as existing OS6560 models. Please refer to the Transceivers Guide.	
OS6900-Q32, OS6900-QNI-U3	QSFP-40G-CLR	

New Software Features and Enhancements

The following software features are being introduced this 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 "Data Center" require a license to be installed.

8.5R1 New Feature/Enhancements Summary

Feature	Platform
VC of 8 for OS6560	6560
VC of 8 for OS6865 and mixed VC of OS6860/OS6865	6860, 6865
Power supply management Alarm relay configuration	6465
USB as backup and restore	6465, 6560, 6860, 6865
1588v2 End-to-end Transparent Clock	6465
MACSec static keys	6465
IPv6: Support on OS6560	6560
IPv6: Route Leak between VRFs	6860, 6865, 6900
Vertical specific signature phase 1	6860(E)
Enhancement of 'show health statistics' command to display Limits	6465, 6560, 6860, 6865, 6900
NAPALM Support	6465, 6560, 6860, 6865, 6900
OV Cirrus Cloud-agent Enhancements	6465, 6560, 6860, 6865, 6900
Configurable System-Default UNP-Profile settings	6860, 6865, 6900
Support for FQDN	6465, 6560, 6860, 6865, 6900
Early Availability	
OSPFv2 – Stub area Support	6560 (EA)
VC of 2 Support on 6465 (1G links)	6465 (EA)

VC of 8 on 6560
Increases the number of OS6560s supported in a VC to 8.

VC of 8 on 6865 and mixed VC of 6860/6865
Increases the number of OS6865s supported in a VC to 8 and allows OS6860 and OS6865 models to be mixed in a VC.

Power Supply Management on OS6465
Allows the OmniSwitch 6465-P6 and P12 models to be configured for the type of power supply attached.

Alarm Relay Configuration on OS6465
Allows for the configuration of the input and output alarm relays on the OmniSwitch 6465. The alarm relay feature is used for notification whenever there is a system event on the switch or an alarm input. Notification is either by an alarm output, trap or by logging a SWLog message.

There is a single line alarm input to the switch which can be connected to an external source. External sources can be temperature, proximity, or door open sensors as examples. The alarm input status is also indicated to the user by the alarm input LED.

There is a single line alarm output from the switch. The alarm output is user configurable for associating any system event or an alarm input. Alarm output status is also indicated to the user by the alarm output LED.

USB as backup and restore
Enables the Running and/or Certified configurations to automatically be saved to a USB drive.

1588v2 End-to-end Transparent Clocking
Feature is supported on OS6465.

MACSec static keys
Adds support for MACSec static keys on OmniSwitch 6465 platforms.

- OS6465-P6 and P12 - MACSec is supported on all ports.
- Due to the encryption/decryption required for MACSec, any OmniSwitch ports with MACSec enabled will not achieve wire-rate performance.
- MACSec supports a key-chain size of 4 only.
- To confirm MACSec support use the **show interface capability** command. MACSec support is listed in the "**MACSec Supported**" field with the module exceptions noted above.

IPv6: Support on OS6560
IPv6 is now supported on the OmniSwitch 6560.

IPv6: Route Leak between VRFs
Supports the leaking of IPv6 routes across VRFs using route-maps.

Vertical specific signature phase 1
Adds default support for the education vertical specific signatures Echo360, Canvas, and Kahoot.

Enhancement of 'show health statistics' command to display Limits
The show health port command is enhanced to view the currently configured device threshold level. The "Limit" output field is displayed in the health statistics which shows the current configured device threshold levels.

NAPALM Support
This AOS release introduces driver support for NAPALM (Network Automation and Programmability Abstraction Layer with Multivendor support). NAPALM supports several methods to connect to devices, manipulate configurations and retrieve data. AOS NAPALM is a python library which can be plugged into NAPALM to manage OmniSwitch devices. To install the AOS NAPALM driver perform the following:

1. Retrieve the source code from the Service & Support site and extract to a desired folder.
2. Change directory to the source code folder and type:

```
-> python setup.py install
```

3. Import the library to begin using, for example:

```
#!/usr/bin/python
import napalm_base as napalm
driver = napalm.get_network_driver('aos')
device = driver(hostname='10.1.2.93', username='admin', password='switch')
device.open()
device.get_facts()
device.get_interfaces()
```

OV Cirrus Cloud-agent Enhancements
In this release, the "restart' parameter has been added to the "cloud-agent admin-state disable force" CLI command. The restart option implicitly triggers “disable force” followed by “enabled”. This will enable a user to restart call-home from OV Cloud.

The CLI command "show cloud agent admin status" has been enhanced to display the status of the certificate on switch, received from the activation server - whether consistent or inconsistent. A new CLI command "cloud-agent remove-inconsistent-certificate" is added to remove the inconsitent certificate on the switch. If the certificate status is inconsistent, the CLI command can be used to remove the certificate received from the Activation server on all units of the VC.

Configurable System Default UNP Profile Settings
UNP System Default profiles are dynamically created to accommodate device traffic received on UNP access ports that is not classified into a user-defined UNP service profile. This type of profile is defined to carry traffic for an SPB service or for a VXLAN service based on the dynamic service setting for the UNP access port on which the traffic is received. For example:

- If the dynamic service value is set to SPB, then a System Default profile is dynamically created with attributes to define an SPB SAP.
- If the dynamic service value is set to VXLAN, then the System Default profile is dynamically created with attributes to define a VXLAN SAP.

One of the attributes defined for a System Default profile SAP is an SPB I-SID or VXLAN VNID. This value is dynamically calculated using a global default base service number, global default modulo number, VLAN tag of the UNP port traffic, and the UNP port domain value. The global base service and modulo number values are now user-configurable.

Once the SPB I-SID or VXLAN VNID number for a SAP is determined, that number is used to derive a System Default profile name that is saved to the switch configuration file. For example:

- The name of an SPB System Default profile is “SystemDefaultISID”, where “ISID” is the calculated attribute value for the profile. For example, if the calculated I-SID number is 10100030, then the SPB profile “SystemDefault10100030” is created.

- The name of a VXLAN System Default profile is “SystemDefaultVNID”, where “VNID” is the calculated attribute value for the profile. For example, if the calculated VNID number is 10000100, then the VXLAN profile “SystemDefault10001000” is created.

Additional configurable global values for dynamic services associated with the SPB or VXLAN SAPs defined for System Default profiles include the following:

- The multicast mode (head-end or tandem) for an SPB or VXLAN service.
- VLAN translation for an SPB or VXLAN service.
- A multicast group IP address for a VXLAN service.

- A far-end IP address list name for a VXLAN service.

Support for FQDN to enable name based connectivity
Allows the configuration of a Fully Qualified Domain Name (FQDN) for OV Cirrus, Access Guardian (BYOD redirect to server), OpenFlow, sFlow, SNMP, and Switch Logging features.

Open Problem Reports and Feature Exceptions

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

System / General / Display

PR	Description	Workaround
230177	Counters remain null for "show service counters" while sending bidirectional unicast traffic over SPB network in 6860 and 6900 platforms.	There is no known workaround at this time. This is a display issue only.
231269	On an OS6560 VLAN 4092 is reserved for future feature support and should not be used for user traffic. No configuration error is displayed when configuring VLAN 4092.	Do not configure VLAN 4092 on an OS6560 since it is a reserved VLAN.
231889	When Static Bridging MACs are moved from one port to another on the same NI and learned as Dynamic Filtering, the entry for filtering MAC is not seen in the source learning table. But when the MAC is moved between ports on different NIs, both Static Bridging and Dynamic Filtering MAC entries are seen in the source learning table.	There is no known workaround at this time. This is a display issue only.
232434	Traffic drop seen after mac-movement when traffic being sent across two VXLAN access ports.	There is no known workaround at this time.

QoS

PR	Description	Workaround
229053	On an OS6560, 10% of P7 traffic loss is observed over P0 traffic when max egress-bandwidth is enabled.	There is no known workaround at this time.
229438	On an OS6560-P48Z16 with high data traffic rate incoming from port 1-32 oversubscribing the output within same range port may cause higher priority to drop over lower priority partially.	There is no known workaround at this time.
231481	On OS6560-P48 models, ARP entries are not logged when using the policy rule log command.	There is no known workaround at this time.
231678	Intermittently, for a UNP user in block or filtering state, the mac-aging timer internally gets set back to the default value after a VC takeover.	There is no known workaround at this time.
231881	User-port filter for BGP packets only filters on destination TCP port and not source TCP port.	There is no known workaround at this time.
231935	After creating an ethernet-service with an svlan and adding an nni port, trying to change the default classification properly displays the error "Can't set default classification on network port". However, if the port is reset with the 'qos reset port' command, the default classification can be changed and no error is displayed.	There is no known workaround at this time.
CRAOS8X-1362	On an OS6560 ISF will not work properly on a UNP port with UNP policy list applied.	There is no known workaround at this time.

Hardware

PR	Description	Workaround
231100	When default classification of QoS aware port is set as DSCP and DEI egress is enabled, the egressing traffic is not set with DEI bit.	There is no known workaround at this time.
231453	In OS6465-P12/P6 the Source Photonics iSFP-100-MM transceiver (SP-FE-FX-IDFM) has a ddm alarm low when connected between 6465-P12/6465-P6/6865-U12X.	There is no known workaround at this time.
231672	QSFP-40G-C7M Molex (1110409177) connected between OS99-CNI-U8 and 6900-X72 keeps flapping.	There is no known workaround at this time.
232278	In 6560 all models, Source Photonics SFP-Dual-MM-N (SPG-DR-FX-CDFC-AL2) when inserted into the 10G port the status shows “up” and port LED blinking green without any cable connected.	There is no known workaround at this time.

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 8.5R1.

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

Feature	6465	6560	6860(E)	6865	6900	Notes
Management Features						
Automatic Remote Configuration / Zero touch provisioning	Y	Y	Y	Y	Y	
Automatic/Intelligent Fabric	Y	Y	Y	Y	Y	
Automatic VC	N	Y	Y	Y	Y	
Bluetooth for Console Access	N	N	Y	N	N	
EEE support	N	N	Y	Y	Y	
Embedded Python Scripting / Event Manager	Y	Y	Y	Y	Y	
IP Managed Services	N	N	Y	Y	Y	
ISSU	N	Y	Y	Y	Y	
NTP	Y	Y	Y	Y	Y	
OpenFlow	N	N	Y	N	Y	
Remote Chassis Detection (RCD)	N	N	N	N	Y	
SAA	Y	N	Y	Y	Y	
SNMP v1/v2/v3	Y	Y	Y	Y	Y	
UDLD	Y	Y	Y	Y	Y	
USB Disaster Recovery	Y	Y	Y	Y	Y	
USB Flash	Y	Y	Y	Y	Y	
Virtual Chassis (VC)	N	Y	Y	Y	Y	
Virtual Chassis Split Protection (VCSP)	N	Y	Y	Y	Y	
VRF	N	N	Y	Y	Y	
VRF – IPv6	N	N	Y	Y	Y	IPv6 multicast routing and MLDv1 and v2 are not supported in VRF
VRF – DHCP Client	N	N	Y	Y	Y	
Web Services & CLI Scripting	Y	Y	Y	Y	Y	
Layer 3 Feature Support						
ARP	Y	Y	Y	Y	Y	
ARP - Distributed	N	N	N	N	Y	
ARP - Proxy	Y	Y	Y	Y	Y	
BFD	N	N	Y	Y	Y	

Feature	6465	6560	6860(E)	6865	6900	Notes
BGP with graceful restart	N	N	Y	Y	Y	
BGP route reflector for IPv6	N	N	Y	Y	Y	
BGP ASPATH Filtering for IPv6 routes on IPv6 peering	N	N	Y	Y	Y	
BGP support of MD5 password for IPv6	N	N	Y	Y	Y	
BGP 4-Octet ASN Support	N	N	Y	Y	Y	
DHCP Client / Server	N	Y	Y	Y	Y	
DHCP Relay	Y	Y	Y	Y	Y	
DHCPv6 Server	N	N	Y	Y	Y	
DHCPv6 Relay	Y	Y	Y	Y	Y	
DHCP Snooping	N	Y	Y	Y	Y	
DHCP Snooping IP source filter	N	Y	Y	Y	Y	
ECMP	Y	Y	Y	Y	Y	
IGMP v1/v2/v3	Y	Y	Y	Y	Y	
IPv4 Multicast Switching	Y	Y	Y	Y	Y	
GRE	N	N	Y	Y	Y	
IP-IP tunneling	N	N	Y	Y	Y	
IP routed port	Y	Y	Y	Y	Y	
IPv6	Y	Y	Y	Y	Y	
IPv6 DHCP relay and Neighbor discovery proxy	Y	Y	Y	Y	Y	
IP Multinetting	Y	Y	Y	Y	Y	
IPSec (IPv6)	N	N	Y	Y	Y	
ISIS IPv4/IPv6	N	N	Y	Y	Y	
M-ISIS	N	N	Y	Y	Y	
OSPFv2	N	N	Y	Y	Y	
OSPFv3	N	N	Y	Y	Y	
PIM-DM	N	N	Y	Y	Y	
RIP v1/v2	Y	Y	Y	Y	Y	
RIPng	Y	Y	Y	Y	Y	
VRRP v2	N	Y	Y	Y	Y	
VRRP v3	N	Y	Y	Y	Y	
Server Load Balancing (SLB)	N	N	Y	Y	Y	
Static routing	Y	Y	Y	Y	Y	
Multicast Features						
DVMRP	N	N	Y	Y	Y	
IGMP v1/v2/v3	Y	Y	Y	Y	Y	
IPv4 Multicast Switching	Y	Y	Y	Y	Y	
IPv6 Multicast Switching (MLD v1/v2)	Y	Y	Y	Y	Y	

Feature	6465	6560	6860(E)	6865	6900	Notes
PIM-DM	N	N	Y	Y	Y	
PIM-SM	N	N	Y	Y	Y	
PIM-SSM	N	N	Y	Y	Y	
PIM-SSM Static Map	N	N	Y	Y	Y	
PIM-BiDir	N	N	Y	Y	Y	
Monitoring/Troubleshooting Features						
Ping and traceroute	Y	Y	Y	Y	Y	
Policy based mirroring	N	N	Y	Y	Y	
Port mirroring	Y	Y	Y	Y	Y	
Port monitoring	Y	Y	Y	Y	Y	
Port mirroring - remote	Y	Y	Y	Y	Y	
Port mirroring – remote over linkagg	N	N	Y	Y	Y	
RMON	Y	Y	Y	Y	Y	
SFlow	Y	Y	Y	Y	Y	
Switch logging / Syslog	Y	Y	Y	Y	Y	
TDR	N	N	Y	N	N	
Layer 2 Feature Support						
802.1q	Y	Y	Y	Y	Y	
DHL	Y	Y	Y	Y	N	
ERP v2	Y	N	Y	Y	Y	
HAVLAN	N	N	Y	Y	Y	
Link Aggregation (static and LACP)	Y	Y	Y	Y	Y	
LLDP (802.1ab)	Y	Y	Y	Y	Y	
Loopback detection – Edge (Bridge)	Y	Y	Y	Y	N	
Loopback detection – SAP (Access)	N	N	Y	Y	Y	
Spanning Tree (1X1, RSTP, MSTP)	Y	Y	Y	Y	Y	
Spanning Tree (PVST+, Loop Guard)	N	N	Y	Y	Y	
MVRP	Y	Y	Y	Y	Y	
Private VLANs	N	N	Y	Y	Y	
SIP Snooping	N	N	Y	N	N	
SPB	N	N	Y	Y	Y	
QoS Feature Support						
802.1p / DSCP priority mapping	Y	Y	Y	Y	Y	
IPv4	Y	Y	Y	Y	Y	
IPv6	Y	Y	Y	Y	Y	

Feature	6465	6560	6860(E)	6865	6900	Notes
Auto-Qos prioritization of NMS/IP Phone Traffic	Y	Y	Y	Y	Y	
Groups - Port	Y	Y	Y	Y	Y	
Groups - Service	Y	Y	Y	Y	Y	
Groups - Map	Y	Y	Y	Y	Y	
Groups - Switch	Y	Y	Y	Y	Y	
Ingress/Egress bandwidth limit	Y	Y	Y	Y	Y	
MAC Groups	Y	Y	Y	Y	Y	
Network Groups	Y	Y	Y	Y	Y	
Per port rate limiting	N	N	Y	Y	Y	
Policy Lists	Y	Y	Y	Y	Y	
Policy based routing	N	N	Y	Y	Y	
Tri-color marking	N	N	Y	Y	Y	
QSP Profiles 1	Y	Y	Y	Y	Y	
QSP Profiles 2/3/4	N	N	Y	Y	Y	
QSP Profiles 5	Y	Y	N	N	N	
Metro Ethernet Features						
Ethernet Services (VLAN Stacking)	Y	N	Y	Y	Y	
Ethernet OAM (ITU Y1731 and 802.1ag)	Y	N	Y	Y	Y	
Security Features						
Access Guardian – Bridge	Y	Y	Y	Y	Y	
Access Guardian - Access	N	N	Y	Y	Y	
Application Fingerprinting	N	N	N	N	Y	
Application Monitoring and Enforcement (Appmon)	N	N	Y	N	N	
ARP Poisoning Protection	Y	Y	Y	Y	Y	
BYOD - COA Extension support for RADIUS	N	Y	Y	Y	N	
BYOD - mDNS Snooping/Relay	N	Y	Y	Y	N	
BYOD - UPNP/DLNA Relay	N	Y	Y	Y	N	
BYOD - Switch Port location information pass-through in RADIUS requests	N	Y	Y	Y	N	
Captive Portal	N	Y	Y	Y	N	
Interface Violation Recovery	Y	Y	Y	Y	Y	
Learned Port Security (LPS)	Y	Y	Y	Y	Y	
LLDP	Y	Y	Y	Y	Y	

Feature	6465	6560	6860(E)	6865	6900	Notes
MACSec	Y	N	Y	N	N	
Quarantine Manager	N	N	Y	Y	N	
Radius test tool	Y	Y	Y	Y	Y	
Storm Control	N	N	Y	Y	Y	
TACACS+ Client	Y	Y	Y	Y	Y	
TACACS+ command based authorization	N	N	Y	Y	Y	
PoE Features						
802.1af and 802.3at	Y	Y	Y	Y	N	
Auto Negotiation of PoE Class-power upper limit	Y	Y	Y	Y	N	
Display of detected power class	Y	Y	Y	Y	N	
LLDP/802.3at power management TLV	Y	Y	Y	Y	N	
HPOE support	Y(60W)	Y (95W)	Y (60W)	Y (75W)	N	
Time Of Day Support	Y	Y	Y	Y	N	
Data Center Features						
CEE DCBX Version 1.01	N	N	N	N	Y	
Data Center Bridging (DCBX/ETS/PFC)	N	N	N	N	Y	
EVB	N	N	N	N	Y	
FCoE / FC Gateway	N	N	N	N	Y	
VXLAN	N	N	N	N	Q32/X72	
VM/VXLAN Snooping	N	N	N	N	Y	
FIP Snooping	N	N	N	N	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).

Note: In most cases it is not necessary to perform a uboot/miniboot upgrade. If a uboot/miniboot upgrade is required it must be performed prior to upgrading AOS. Refer to UBoot and FPGA Requirements table for minimum requirements.

Supported Upgrade Paths and Procedures

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

Platform	**AOS Releases Supporting ISSU to 8.5R1 (GA)**
OS6900	8.4.1.170.R01 (GA) 8.4.1.229.R02 (GA) 8.4.1.233.R02 (MR) 8.4.1.141.R03 (GA)
OS6860(E)	8.4.1.170.R01 (GA) 8.4.1.229.R02 (GA) 8.4.1.233.R02 (MR) 8.4.1.141.R03 (GA)
OS6865	8.4.1.170.R01 (GA) 8.4.1.229.R02 (GA) 8.4.1.141.R03 (GA)
OS6560	8.4.1.229.R02 (GA) 8.4.1.141.R03 (GA)
Note: For any switch with a multicast configuration ISSU is only supported from 8.4.1.R02 GA or MR. Earlier releases must use a standard upgrade.	

8.5R1 ISSU Supported Releases

Prerequisites

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

- Be the responsible party for maintaining the switch's configuration.
- Be aware of any issues that may arise from a network outage caused by improperly loading this code.
- Understand that the switch must be rebooted and network access may be affected by following this procedure.
- Have a working knowledge of the switch to configure it to accept an FTP connection through the EMP or Network Interface (NI) Ethernet port.
- Read the GA Release Notes prior to performing any upgrade for information specific to this release.
- Ensure there is a current certified configuration on the switch so that the upgrade can be rolled-back if required.
- Verify the current versions of UBoot and FPGA. If they meet the minimum requirements, (i.e. they were already upgraded during a previous AOS upgrade) then only an upgrade of the AOS images is required.
- Depending on whether a standalone chassis or VC is being upgraded, upgrading can take from 5 to 20 minutes. Additional time will be needed for the network to re-converge.
- The examples below use various models and directories to demonstrate the upgrade procedure. However any user-defined directory can be used for the upgrade.

- If possible, have EMP or serial console access to all chassis during the upgrade. This will allow you to access and monitor the VC during the ISSU process and before the virtual chassis has been re-established.

- Knowledge of various aspects of AOS directory structure, operation and CLI commands can be found in the Alcatel-Lucent OmniSwitch User Guides. Recommended reading includes:
    - Release Notes - for the version of software you're planning to upgrade to.
    - The AOS Switch Management Guide
        - Chapter – Getting Started
        - Chapter - Logging Into the Switch
        - Chapter - Managing System Files
        - Chapter - Managing CMM Directory Content
        - Chapter - Using the CLI
        - Chapter - Working With Configuration Files
        - Chapter - Configuring Virtual Chassis

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

Switch Maintenance

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

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

```
6900-> show system
System:
  Description:  Alcatel-Lucent OS6900-X20 8.4.1.233.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
```

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

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

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

- If upgrading a standalone chassis or VC using a standard upgrade procedure please refer to Appendix 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
- OS6560 – 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           8.5.164.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:

- OS6900 **-** Tos.img
- OS6860 – Uos.img
- OS6865 – Uos.img
- OS6560 – 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: The following examples use **issu_dir** as an example ISSU directory name. However, any directory name may be used. Additionally, if an ISSU upgrade was previously performed using a directory named **issu_dir**, it may now be the *Running Configuration*, in which case a different ISSU directory name should be used.

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

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

3. Clean up existing ISSU directories

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

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

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

```
OS6900-> ssh 127.10.2.65

Password:switch
```

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

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

6. Log out of the Slave chassis:

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

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

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

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

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

9. Upgrade the image files using ISSU:

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

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

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

This indicates that the ISSU is completed

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

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

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

10. Verify the Software Upgrade

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

```
OS6900-> show microcode
   /flash/working
```

```
   Package           Release                 Size     Description
-----------------+------------------------+--------+-----------------------------------
Tos.img           8.5.164.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 this AOS Release.

PR	Summary
229358	LGS 256: Session manager clean up tries to free wrong pointer.
226593	LGS 126: cfg_parser accesses buffer out-of-bounds.
226592	LGS 125: Multiple Vulnerabilities in openssh 6.0.
231019*	SNMP v3 stopped working on OS6900.
231152	Unable for copy from /flash to /uflash
230783	Application Visibility for OS6900 doesn't work as for OS6860, only first port stats are displayed.
230964	OS6900 VC(8.4.1.229.R02): Disable/enable MVRP crashes the VC
230803*	“lldpXMedRemInventoryTable” empty data.
230896	Switch rebooted once the user password was changed after the expiry.
231229	OS6860 does not show the complete output of show service counters.
231351	OS6900: "no vrrp trap" command is not shown under "show configuration snapshot".
231401	Swlogs filled with logs "RUNNING event:22, sourceChassisId 0 sourceSlotum 0".
231282*	Interface configuration is not shown in “show configuration snapshot” and also the configuration is missing in vcboot.cfg.
231496	OS6860-48 : After AOS upgrade Topology age OID is not working.
230826	OS6900 need clarification for the following log. 2017 Dec 21 08:12:12 SparoLab50S swlogd: vcmNi lib rary(plApi) error(2) [1513843932.208328] plGetVflStringFromIfIndex@11171: Invalid ifIndex 0 (context 0).
231658	OS6860E - Flood-rate limit mbps on multicast traffic does not work as expected.
230456	OSPF routes are not getting advertised due to interface MTU size.
231825*	Aos generates the messsage "AOS generates the logs message "udpRelay tcam warning(4) ds_tcamIPPortBind(1424): rule Id for cid(1) slot (1) is not available".
231722	OS6860 NTP broadcast command error.
231940	Need assistance in DoS type Unicast dest-ip/ multicast-mac logs
231639	After hard/soft reboot, POE service starts before network service on slave unit of VC of 2 x OS6860-P24. As such, MITEL IP Phones are unable to boot up properly.
230589	UNP Access IP classification rule issue with 8.4.1.229.R02
231202*	vcmNi crash due to CLI debug command - buffer overflow
232084	OS6860E high CPU issue due to process avahi-daemon.
231972	OS6860E : UNP port display issue.
232048	Client connected to AOS switch fails to get an IP address when DHCP snooping is enabled with QOS Userports.
232317*	OS6900 SNMP WALK error message.
232286	Os6900: Default route is chosen instead of Static route.
232341	OS6900 Internal DHCP Config Option 43
231668	OS6860E-P48 : Non-existent next hop is seen in the BGP path.
231980*	OS6900: CapManAccess:Init message has noticed while executing CLI command on SSH session.
232218	OS6900-X20 error message while executing the show commands

232188	The ip Helper is not forwarding DHCP packets to the DHCP server in vlan 600 but work correctly with.
229361	LGS 259: Memory leak parsing CLI traceroute command
229365	LGS 263: Memory leak parsing IPV6 CLI ping command
229367	LGS 265: File descriptor resource leak when CLI fails to break out of jail
229366	LGS 264: Memory leak parsing ipv6 CLI traceroute command
229362	LGS 260: Memory leak parsing CLI ping command
230667	OS6860 VC crash
230613	Display issue with the command show lldp remote-system med inventory
230896	Switch rebooted once the user password was changed after the expiry.
230891	OS6900- VRF name disappears once apply tab to complete a command
230970	OSPF stuck in EXST state after applying the qos.

* – In Verify.