Release Notes - Rev. C

OmniSwitch 6900/6860(E)/6865

Release 8.4.1.R01

These release notes accompany release 8.4.1.R01. These release notes provide important information on individual software features and hardware modules. Since much of the information in these release notes is not included in the hardware and software user manuals, it is important that you read all sections of this document before installing new hardware or loading new software.

Note: The OS10K and OS9900 are not supported in this 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 8.4.1.R01 AOS software available from Service & Support.

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

OmniSwitch 6900-X20/X40 – AOS Release 8.4.1.170.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 8.4.1.170.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 8.4.1.170.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 8.4.1.170.R01(GA)

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

OmniSwitch 6860(E) – AOS Release 8.4.1.170.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)
OS686E-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 8.4.1.170.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.

[IMPORTANT] *MUST READ*: AOS Release 8.4.1.R01 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 8.4.1.R01 please refer to Appendix B for important best practices, prerequisites, and step-by-step instructions.

Additional Information

- All switches that ship from the factory with AOS Release 8.4.1.R01 will default to VC mode (requiring a vcboot.cfg configuring 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 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.

- Beginning in 8.4.1.R01 when configuring BFD with protocols that support echo-only mode (VRRP or static routes) the configuration of a Loopback0 address is recommended. When upgrading from a previous release the existing configuration will be accepted but a warning will display on the primary CMM which will also show up in the configuration error file. Additionally, when configuring via the CLI a warning will be displayed recommending the configuration of a Loopback0 address.

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 Installation 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	No	No	No	
Virtual Chassis	No	No	No	
IPSec	No	No	No	
OSPF v2/v3	No	No	No	
RIPng	No	No	No	
BGP	No	No	No	
IS-IS v4/v6	No	No	No	
Policy-Based Routing	No	No	No	
IPv6 static routing	No	No	No	
PIM-DM	No	No	No	
PIM-SM	No	No	No	
DVMRP	No	No	No	
VRRP/VRRPv3	No	No	No	
VRF	No	No	No	

Note: A permanent Advanced license is included in this release for all platforms.
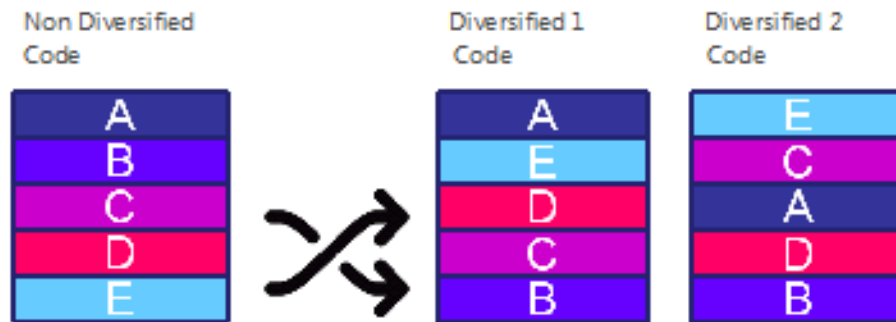
CodeGuardian

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 8.4.1.R01	AOS 8.4.1.RX1	AOS 8.4.1.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

following new hardware is being introduced in this release.

OS6860E-P24Z8

Fixed configuration chassis in a 1U form factor with:

- Sixteen (16) - 10/100/1000 BaseT PoE ports (30W PoE)
- Eight (8) - 100/1000/2.5G Base-T (75W HPoE)
- Four (4) - SFP+ (1G/10G) ports
- Two (2)- 20G virtual chassis link ports
- USB port
- Micro-USB console port
- RS-232 console port
- EMP port for out-of-band management.

Please note the following for the 2.5G ports (17-24)

- The ports will advertise either 2.5G or 1G when auto-negotiation is enabled depending on the port's configured speed. The default is 2.5G. The ports will properly auto-negotiate between 10/100/1000 when configured for 1G. They will not auto-negotiate between 10/100/1000 when configured for 2.5G.
- The changing of a port's speed, when changing between 100M/1G and 2.5G or vice-versa, is applied in port pairs. Meaning, changing the speed of one port of a pair will cause the other port's speed to change as well. The port pairs are 17/18, 19/20, 21/22, 23/24. This does not apply when changing the speed between 100M and 1G.

OS6865-U12X

The OmniSwitch 6865-U12X is a 1-GigE and 10-GigE platform designed for demanding electrical & severe temperature environments. Fixed-configuration, hardened, fan-less chassis in a 2U form factor.

- Two (2) - SFP+ 1G/10G ports.
- Six (6) – 100Base-FX / 1000Base-X SFP ports
- Four (4) - 10/100/1000Base-T PoE+ ports (75W HPoE per port)
- USB port
- RJ-45 console port
- Two (2) - power supply connectors for external power supplies
- Operates at a wider temperature range from -40°C to 74°C. (65°C without airflow)
- OS6865-BP - AC power supply providing 180W of system and PoE power
- OS6865-BP-D- DC power supply (24V/48V) providing 180W (@48V) or 140W (@24V) of system and PoE power.
- Load sharing and mixing of AC and DC power supplies is supported allowing up to 300W of PoE power.

OS6865-U28X

The OmniSwitch 6865-U28X is a 1-GigE and 10-GigE platform designed for demanding electrical & severe temperature environments. Fixed-configuration, hardened, fan-less chassis in a 1U form factor.

- Four (4) - SFP+ 1G/10G ports.
- Twenty (20) – 100Base-FX / 1000Base-X SFP ports
- Four (4) - 10/100/1000Base-T PoE+ ports (75W HPoE per port)
- USB port

- RJ-45 console port

- Two (2) power supply connectors for external power supplies

- Operates at a wider temperature range from -40°C to 74°C. (65°C without airflow)

- OS6865-BP - AC power supply providing 180W of system and PoE power

- OS6865-BP-D- DC power supply (24V/48V) providing 180W (@48V) or 140W (@24V) of system and PoE power.

- Load sharing and mixing of AC and DC power supplies is supported allowing up to 280W of PoE power.

Transceivers

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

OS6860(E)	OS6865
QSFP-4X10G-SR	OS6865-CBL-40/100/300
SFP-10G-T	iSFP-100-MM*
SFP-DUAL-MM-N	iSFP-100-SM15*

*Supported on OS6865-U12X and OS6865-U28X

New Software Features and Enhancements

The following software features are being introduced with the 8.4.1.R01 release, subject to the feature exceptions and problem reports described later in these release notes. Features listed as 'Base' are included as part of the base software and do not require any license installation. Features listed as "Data Center" require a license to be installed.

8.4.1.R01 New Feature/Enhancements Summary

Feature	Platform	License
JITC Certification	All	N/A
TCN Logging	All	N/A
DHCP Snooping Binding Table Static Entries	All	N/A
Layer 2 Profiles for UNP Access	All	N/A
VRRP Delay on BFD Tracking	All	N/A
VRRP Delay on Takeover	All	N/A
Multicast Over SPB-M Optimization	All	N/A

JITC Certification

AOS release 8.4.1.R01 & later includes DoD specific features to meet the Unified Capabilities Requirements (UCR) 2013 in support of the Joint Interoperability Test Certification process. The DoD specific features are available for the following OmniSwitch platforms. JITC certification is currently pending.

- o OmniSwitch 6900 family
- o OmniSwitch 6860 family
- o OmniSwitch 6865 family

TCN Logging

New "Topology Change Port" field to display the port or link aggregate on which a TCN is received. This information is available on each switch and can be used to track down the source of the topology change within the network.

DHCP snooping Binding Table Static Entries

New CLI command to display the contents of the DHCP Snooping binding table using the configuration snapshot format. There is also a command option to display only static or dynamic table entries. The configuration snapshot output format can easily be saved so that the entries can be reused at a later time or on another switch.

Layer 2 Profiles for UNP Access Ports

Layer 2 profiles can now be assigned to UNP access ports. A Layer 2 profile determines how control frames received on a UNP access port are processed. Each time a port is configured as a UNP access port, the default Layer 2 profile (unp-def-access-profile) is assigned to that port. Custom Layer 2 profiles can be created and assigned to a port if the default profile settings are not sufficient.

New CLI command to enable LPS and configure a static MAC address on an LPS port. This was previously a two-step process that involved enabling LPS with one command first, then configuring the static MAC address on the LPS port with another command. Now this process is achieved through the use of a single LPS command. In addition, specifying a VLAN for the static MAC address is optional. When a VLAN is not specified, the default VLAN for the LPS port is used. If the default VLAN for the LPS port is changed, the VLAN for the static MAC address is automatically changed to the new VLAN.

VRRP Delay on Takeover and VRRP Delay on BFD Tracking

A configurable delay option for VRRP address tracking policies has been added. The delay option value specifies the amount of time to wait after a VRRP address track is detected as operationally up and before the associated virtual router's priority value is incremented by the tracking policy's priority value. Configuring the delay time for an address tracking policy helps to prevent the loss of device connectivity that may occur before a virtual router prematurely becomes the master. For example, configuring a delay time allows the switch routing tables to stabilize before the master router resumes the master role.

Enabling BFD for an address tracking policy requires a Loopback0 interface on the local switch. The IP address of this interface will serve as the source IP address of BFD packets.

Multicast Over SPB-M Multicast Optimization

SPBM uses the Intermediate System-Intermediate System (IS-IS) protocol to build sets of symmetric shortest path trees (SPTs) through the network that are used to transport traffic entering the SPBM domain. When non-unicast traffic enters the SPBM domain, multicast filtering is performed on a per-SAP, per-service basis to make sure traffic is only sent out on SAP ports associated with a LAN that has devices requesting specific streams. This helps to alleviate the overhead of forwarding unnecessary traffic, especially in networks that carry large amounts of multicast traffic.

An SPBM backbone edge bridge performs the multicast filtering using the logic of IGMP Snooping. The filtering is applied on a per-service basis to limit the traffic going out of each SAP port, as well as traffic going out across each backbone port. The SPBM bridge will monitor the IGMP queries and requests from SAPs and network virtual ports to build the stream membership association logic and timing in the same manner as is done on a standard IGMP Snooping bridge.

Note: Tandem mode is being supported as an Early Availability feature only.

Queue Profile Enhancement (Early Availability)
Queue profile enhancement on OS6860/OS6860E to allow traffic shaping and scheduler selection on a per queue basis. Traffic shaping allows modification of CIR and PIR, and scheduler selection allows selection of the SP or WRR scheduler. WRR scheduler allows weight to be modified.

 Example configurations for egress queue scheduling are as below:

```
-> qos qsp 7 import qsp "qsp-1"
-> qos qsp "qsp-7" qp 6 pir 1 weight 40 scheduler wrr
-> qos qsp "qsp-7" qp 7 weight 40 scheduler wrr
-> qos qsp "qsp-7" qp 8 cir 40
```

Note: The traffic shaping and scheduler configuration should be handled very carefully as it has high impact on traffic flows through the network. Please consult with technical support before deploying the feature.

Complete Technical Support Log Files
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.

JITC Related CLI Updates

The following CLI has been added or modified in this release.

Feature	Command
JITC	aaa jitc admin-state
	show aaa jitc config
Swlog	swlog advanced
	swlog size-trap-threshold
	show swlog
RADIUS	aaa radius-server
	show aaa Server
IPSec	ipsec default-discard
	show ipsec policy
IP	ip tcp half-open-timeout
	show ip tcp half-open-timeout
IPv6	ipv6 echo
	ipv6 icmp rate-limit
	ipv6 static route
	show ipv6 information
	modify boot parameters
	show ipv6 emp-interfaces
	show ipv6 emp-routes
	show ipv6 interface
OSPFv3	ipv6 ospf restart
	ipv6 ospf restart initiate
	ipv6 ospf restart-interval
	ipv6 ospf restart-helper
	ipv6 ospf restart-helper strict-lsa-checking
	ipv6 ospf area
	ipv6 ospf area nssa-translator-role
	ipv6 ospf area nssa-translator-stab-interval

Feature	Command
	ipv6 ospf area area-summary
	show ipv6 ospf restart
	show ipv6 ospf
	show ipv6 ospf area
	show ipv6 ospf neighbor
BGP	ip bgp neighbor ttl-security
	ipv6 bgp neighbor ttl-security
	show ip bgp neighbors
	show ipv6 bgp neighbors
Key Management	security key-chain
	security key
	security key-chain key
	show security key-chain
	show security key
Keychain Management – OSPF	ip ospf interface auth-type
	show ip ospf interface
Key Management - ISIS	ip isis auth-type
	ip isis level auth-type
	ip isis vlan hello-auth-type
	ip isis vlan level hello-auth-type
	show ip isis vlan
	show ip isis status
Session Management	ssh login-grace-time
SNMP	snmp snmp-engineid-type
	show snmp snmp-engineid
Not Supported	ip pim register-rate-limit
	ipv6 pim register-rate-limit

Open Problem Reports and Feature Exceptions

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

System / General

PR	Description	Workaround
223665	Upon bootup of the 6860E-P24Z8, the message "SOC unit 0 attached to PCI device BCM56340_A0:phy_8481_firmware_set: Another PHY already exist on same broadcast MDIO address" is displayed.	There is no known workaround at this time. This is a display issue only, there is no functional impact.
224454	HAVLAN and distributed ARP cannot exist on the same OS6900 chassis.	There is no known workaround at this time.
224874	On OS6900-Q32 broadcast and multicast traffic, "Input packets" in the "show interface traffic" CLI and "InMcastPkts/ InBcastPkts" in "show interface counters" CLI is shown as "0" though traffic flows fine. Also "show interface accounting" CLI doesn't display total of TX and RX packets.	There is no known workaround at this time.
224909	During a flash synchronization, a Webview php message similar to "5960: Webview GET return failed. Object: sysObjectID, Index: 0, reason: no answer received (timeout)" may display on the console.	There is no known workaround at this time. This is a display issue only, there is no functional impact.
225373	get-next operation failed or had errors. Agent returned string with an invalid length OF 0 octets which is outside the range of (SIZE (1..32)) for ALCATEL-IND1-DA-MIB:alaDaUNPEndPoinProfile3.2.	There is no known workaround at this time.
225623	RFC2889 congestion control back pressure is not functional on an OS6865-U28X.	There is no known workaround at this time.

ISSU

PR	Description	Workaround
224893	During ISSU from 8.3.1.R02, the reloaded slave chassis failed to join the VC due to the vcm sync failure on an OS6900 or OS6860(E).	Reconfigure the VC to have only a single member port between two devices for each VFL by administratively disabling the additional member ports.

Hardware

PR	Description	Workaround
223291	Copper port LEDs on os6865-U28x are light in color compared to fiber port LEDs.	There is no known workaround at this time.
224473	On an OS6865-U28X, upon boot-up or toggling the interface, some of the interfaces with 1G copper SFP are in half duplex mode.	Administratively disable and re-enable the interface.
224980	When operating at 100M on an OS99-GNI-U48, the bi-directional dual speed SFP-DUAL-BX-D/U (Oplink TRBCG1CDBC000E2G / TRBCG1CUBC000E2G) cause the link LED to remain on even after the fiber cable is removed.	There is no known workaround at this time.
225506	On an OS6865 a power supply displays an error message and doesn't display as down or unplugged when the power cord is removed.	Re-connect the power cord.
225507	On an OS6865-U28X the VC LED for the primary and slave chassis blinks the appropriate number of times to indicate the chassis-id but then turns off before blinking again. It should remain on after blinking, similar to the other OS6865 models.	There is no known workaround at this time.
226089	On an OS6865-U28X with a mix of an AC and DC power supply @ 24V the PoE power budget is 160W, it should be 200W.	There is no known workaround at this time.

IP / IPv6

PR	Description	Workaround
225590	The show ip/ipv6 multicast tunnel command is not functional.	Use the 'show ip multicast forward' command.

Link Aggregation

PR	Description	Workaround
225135	Linkagg port level rate-limiting not supported.	There is no known workaround at this time.

Openflow

PR	Description	Workaround
199279	Openflow ports that are part of a linkagg are learning mac-addresses dynamically on the Slave chassis.	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.

Virtual Chassis

PR	Description	Workaround
224726	A VC split is sometimes seen during recovery from VCSP split protection state when there are less number of chassis (less than or equal 2) in the active Master and more number of chassis (more than or equal to 6) in the protection Master. This issue is seen only when the VC is recovered in a linear topology (not forming a ring).	This issue can be avoided by connecting both the VFL links (of each chassis) to form a ring topology during recovery from VCSP split protection state.

Access Guardian

PR	Description	Workaround
226198	AG_CMM process restarts when removing UNP profile used for captive-portal authentication while the captive portal session is still alive.	Logout of the captive portal session so the configurations are removed gracefully.

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**.

enterprise.alcatel-lucent.com - Alcatel-Lucent and the Alcatel-Lucent Enterprise logo are trademarks of Alcatel-Lucent. To view other trademarks used by affiliated companies of ALE Holding, visit: enterprise.alcatel-lucent.com/trademarks. All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Neither ALE Holding nor any of its affiliates assumes any responsibility for inaccuracies contained herein (2017).

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	
Remote Chassis Detection (RCD)	N	N	N	
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	

Feature	OS6900	OS6860(E)	OS6865	Notes
ECMP	Y	Y	Y	
IGMP v1/v2/v3	Y	Y	Y	
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	

Feature	OS6900	OS6860(E)	OS6865	Notes
PIM-DM	Y	Y	Y	
DVMRP	Y	Y	Y	
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	

Feature	OS6900	OS6860(E)	OS6865	Notes
QoS Feature Support				
QSP Profiles	Y	Y	Y	
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	

Feature	OS6900	OS6860(E)	OS6865	Notes
mDNS Snooping/Relay (BYOD)	N	Y	Y	
UPNP/DLNA Relay (BYOD)	N	Y	Y	
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: - 8.3.1.R01 or 8.3.1.R02 GA - 8.3.1.R01 or 8.3.1.R02 maintenance release	Upgrading from any other release
OS6860-VC	ISSU – Supported* Standard - Supported	ISSU – Not Supported Standard - Supported
OS6860-Standalone	ISSU – N/A Standard - Supported	ISSU – N/A Standard - Supported
OS6900 – VC	ISSU – Supported* Standard - Supported	ISSU – Not Supported Standard - Supported
OS6900 – Standalone	ISSU – N/A Standard - Supported	ISSU – N/A Standard - Supported
OS6865 - VC	ISSU – Supported Standard - Supported	ISSU – Not Supported Standard - Supported
OS6865 - Standalone	ISSU – N/A Standard - Supported	ISSU – N/A Standard - Supported
*Note: When performing an ISSU upgrade on an OS6900 or OS6860(E) from any 8.3.1.R02 release please reconfigure the VC to have only a single member port between two devices for each VFL by administratively disabling the additional member ports. Please refer to PR 224893.		

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
```

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

- 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              8.4.1.170.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

- 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            8.4.1.170.R01           210697424 Alcatel-Lucent OS
```

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

-> show running-directory

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

11. Certify the Software Upgrade

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

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

-> show running-directory

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

Appendix E: Fixed Problem Reports

The following problem reports were closed or are in verification in AOS Release 8.4.1.R01.

PR	Summary
211072	Queries on command show lanpower slot 1/1 update-from
214291	aaa accounting packet from the switch not honoring the user-name received from radius 214368 OS6860 switch port going shutdown state when LLDP packet is receivedin a non-supplicant.
215401	Both Master and Master Split Topology holds the VC EMP Address.
216961	OS6860 QoS issue to drop multicast traffic.
218705	AP with LACP agg on OS6860 does not power up after switch reboot.
220187	4xOS6900VC NTP synchronization issue in slave unit.
221158	Command to deny specific multicast IP from a range using the static-rp
221560	Ntp.keys and pre-banner.txt files not synchronized between chassis of 6860 VC.
221760	[TYPE`]OS6900: Query on Maximum number of link aggregation groups.
221870	SNMPWALK value to find the port for a vlan is different from 6860 to other AOS switches.
222250	SPB imported routed not forwarding traffic.
222277	Unable to Ping devices in SPB imported network from the switch after the upgrade to 8.3.1 from 8.2.1.
222320	OS6860: Unable to authenticate to a Radius server if the Radius server resides on a local vlan.
222662	Os6900 VC: Getting demo license manager notification although permanent license is installed in a VC.
222804	bcd arp alarm messages on 6XOS6860 VC.
223165	OS6860E-P24: policy action maximum depth command does not accept the value 16.4M.
223302	REST feature: PUT/POST mib got error.
223315	UNP ports in OS6860E VC moved to blocking status.
223334	The Chassis-1 crashed and LACP linkagg instability issue noticed.
223389	VC: Pre-banner.txt file is not synchronized in VC.
223446	OS6860 STP parameters showing incorrect results.
223448	Clarification needed for the 2008-4359, 2007-1870, 2014-2323 and 2016-2109 CVEs.

223474	swlog appid snm_getuser disappears from config.
223477	2xOS6860 Incomplete configuration in vcboot.cfg.
223487	SSP TELECOM, INC: OS6860: Devices connected to Helper switch unable to reach the network after VCSP.
223498	UNI is not transparent for frames with the destination MAC address 01:00:0C:CC:CC:CC.
223502	"show log swlog timestamp" command does not display the switch logs.
223506	NTP fails to work after loading new keys.
223559	OS6860 : RCA requested for the switch reboot.
223618	ipni data warning(4) ipni_handle_ipms_pkt(2224) warning message seen in switch logs.
223622	OS6860- SPB L3vpn ping issue with the code 8.3.1.160.R02.
223624	Ping source-interface as Numeric IP Interface name.
223674	Grep inside the vrf displays the information from default vrf.
223701	OS6860 STP convergence issue on SPB.
223705	OS6860 unable to login to the switch.
223708	OS6860 - Error while retrieving 'show log swlog'.
224009	OS6860E switch displays invalid temperature after code upgrade.
224081	Os6860: Incorrect dying Gasp trap format in syslog message.
224088	SRC IP of the SNMP get-response is not the same as the SNMP get-requested IP interface of the OS6900.
224133	SSH is not enabled on OS6860 after automatic remote configuraiton fail's.
224249	'Show interface alias' command output display issue in a 3 unit Virtual chassis of OS6860E.
224317	Is saa time calculated in micro and mili seconds?
224342	RCD split protection doesn't work.
224357	Port mirroring accepting 2 destination port configuration.
224505	OS6860:(8.3.1.160.R02): Tagging few Vlans in DHL links on the switch OS6860 caused network outage.
224634	Not showing license details on executing 'show license-info' command; however, shows Permanent Advanced.
224838	OS9907:Clarification required on the fan behavior.

224856	Os6860: Incorrect date format in dying Gasp trap of syslog message.
224941	Virtual-IP address of the SLB cluster is not reachable in the same network (same VLAN).
224967	Interrupt processing for Helix4 based systems (6860,6865) needs to move to userspace.
225140	OS6860 need explanation about the swlog intfCmm Mgr error(2) cmmEsmDrv_ifXTableGet:13655 Slot/Port o
225180	OS6860 VC - Radius packets from master EMP IP are not forwarded.
225269	Error in SNMPWALK, test done in slave chassis to find the MAC-address attached to the interface.
225519	"force-l3-learning" command is not saved in the vcboot.cfg on OS6860.