

# Release Notes - Rev. B

## OmniSwitch 9900

### 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: This release supports the OS9900 only.

Contents

Related Documentation .....	3
System Requirements .....	4
[IMPORTANT] *MUST READ*: AOS Release 8.4.1.R01 Prerequisites and Deployment Information.....	5
Licensed Features .....	6
CodeGuardian .....	7
New / Updated Hardware Support .....	8
New Software Features and Enhancements .....	9
JITC Related CLI Updates .....	11
Open Problem Reports and Feature Exceptions.....	13
Hot Swap/Redundancy Feature Guidelines .....	14
Technical Support .....	15
Appendix A: Feature Matrix.....	16
Appendix B: General Upgrade Requirements and Best Practices.....	22
Appendix C: Standard Upgrade - OmniSwitch Standalone Chassis.....	27
Appendix D: ISSU - OmniSwitch Standalone Chassis .....	29
Appendix E: Fixed Problem Reports .....	31

## **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:

[support.esd.alcatel-lucent.com](http://support.esd.alcatel-lucent.com)

- OmniSwitch 9900 Hardware User Guide
- OmniSwitch AOS Release 8 CLI Reference Guide
- OmniSwitch AOS Release 8 Network Configuration Guide
- OmniSwitch AOS Release 8 Switch Management Guide
- OmniSwitch AOS Release 8 Advanced Routing Configuration Guide
- OmniSwitch AOS Release 8 Data Center Switching Guide
- OmniSwitch AOS Release 8 Specifications Guide
- OmniSwitch AOS Release 8 Transceivers Guide

## System Requirements

### Memory Requirements

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

Platform	SDRAM	Flash
OS9900	16GB	2GB

### UBoot and FPGA Requirements

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

Switches not running the minimum version required should upgrade to the latest UBoot or FPGA that is available with the 8.4.1.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 9900 - AOS Release 8.4.1.193.R01 (GA)

Hardware	Coreboot-uboot	Control FPGA	Power FPGA
OS99-CMM	8.3.1.103.R01	2.3.0	0.8
OS9907-CFM	8.3.1.103.R01	-	-
OS99-GNI-48	8.3.1.103.R01	1.2.4	0.9
OS99-GNI-P48	8.3.1.103.R01	1.2.4	0.9
OS99-XNI-48	8.3.1.103.R01	1.3.0	0.6
OS99-XNI-U48	8.3.1.103.R01	2.9.0	0.8
OS99-GNI-U48	8.4.1.166.R01	0.3.0	0.2

---

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

**Licensed Features**

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

	License Required?
	OS9900
Data Center Features	
DCB (PFC,ETS,DCBx)	N/S
EVB	N/S
FIP Snooping	N/S
FCoE VXLAN	N/S

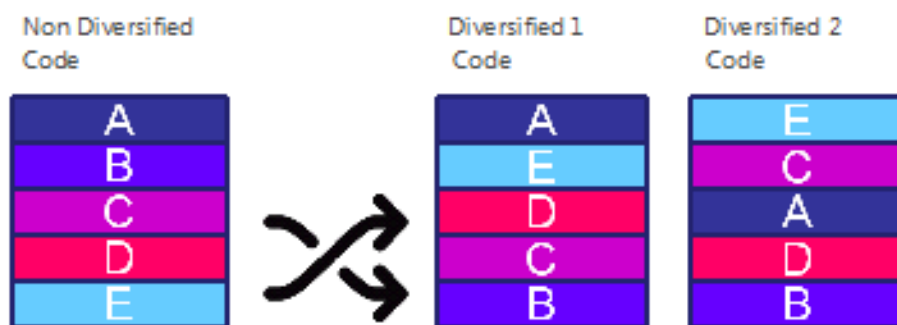
## CodeGuardian

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 5 different diversified images per AOS release (R11 through R31)
- Our partner LGS will have 3 different diversified images per AOS release (L11 through L31)

**New / Updated Hardware Support**

**OS99-GNI-U48**

OS9900 Gigabit network interface card offering 48 unpopulated wire-rate 1000Base-X SFP ports.



## **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 ‘N/A’ are included as part of the base software and do not require any license installation. Licensed features will list the name of the required license.

### **8.4.1.R01 New Feature/Enhancements Summary**

<b>Feature</b>	<b>Platform</b>	<b>License</b>
JITC Certification	OS9900	N/A
TCN Logging	OS9900	N/A
DHCP Snooping Binding Table Static Entries	OS9900	N/A
Layer 2 Profiles for UNP Access	OS9900	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.

- OmniSwitch 9900

#### **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.

**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

PR	Description	Workaround
222958	To improve OS9900 stability with high scale configurations the LACP default timeout changed to 30 seconds instead of 1 second.	Use the 'debug lacp slow_timeout {enable   disable}' command to modify the default timeout. Additionally, the following command will be present in the configuration file:  <b>no linkagg lacp port &lt;port&gt; actor admin-state timeout</b>
223079	Multiple errors portMgrCmm/lpCMM/linkagg/VlanMgr/MVRP/ipms/TCAM/QOS/ in swlog.	There is no known workaround at this time. This is a display issue only, no functional impact.
223453	'show unip user details' does not list the IP address of the user details.	IP address should be configured on the UNP port in the same subnet as UNP user.
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.
225983	On an OS9900 Webview can take approximately 10 seconds to display QoS conditions with ALL option.	There is no known workaround at this time.

### QoS

PR	Description	Workaround
222202	To apply a qos config file with 511 entries takes 10 minutes and results in a client unavailable error message on the console.	There is no known workaround at this time.

### ISSU/Takeover/Reload

PR	Description	Workaround
222963	Error message stpNi _VLNt error addQtag (570) illegal on NI reset during ISSU takeover with MVRP configuration.	There is no known workaround at this time. This is a display issue only, no functional impact.

## 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.
- 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 operational LED blinking green before initiating another hot swap activity.

Existing Slot	Hot-swap/Hot-insert compatibility
Empty	All modules can be inserted
OS99-CMM	OS99-CMM
OS9907-CFM	OS9907-CFM
OS99-GNI-48	OS99-GNI-48
OS99-GNI-P48	OS99-GNI-P48
OS99-XNI-48	OS99-XNI-48
OS99-XNI-U48	OS99-XNI-U48
OS99-GNI-U48	OS99-GNI-U48

**OS9900 Hot Swap/Insertion Compatibility**

### Hot Swap Procedure

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

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

## **Technical Support**

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

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

Email: [ebg\\_global\\_supportcenter@al-enterprise.com](mailto: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](http://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](http://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 8.4.1.R01 and the OS9900.

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

Feature	OS9900	Notes
<b>Management Features</b>		
USB Console Support	Y	
SNMP v1/v2/v3	Y	
NTP	Y	
PING and TRACEROUTE as a Read-Only user	Y	
USB Disaster Recovery	Y	
Automatic Remote Configuration / Zero touch provisioning	N	
IP Managed Services	Y	
SSH for read-only users	Y	
VRF	Y	
VRF - DHCP Client	Y	
Automatic/Intelligent Fabric	N	
Automatic VC	N	
Bluetooth for Console Access	N	
EEE support	N	
Embedded Python Scripting / Event Manager	N	
ISSU	Y	
OpenFlow	N	
SAA	N	
SNMPv3 FIPS Certified Cryptographic Algorithms	Y	
UDLD	N	
USB Flash	N	
Virtual Chassis (VC)	N	
VC Split Protection (VCSP)	N	
Remote Chassis Detection (RCD)	N	
Web Services & CLI Scripting	Y	
<b>Layer 3 Feature Support</b>		
ARP	Y	Static ARP with multicast MAC not supported
OSPFv2	Y	
Static routing to an IP interface name	Y	
ECMP	Y	



Feature	OS9900	Notes
IGMP v1/v2/v3	Y	
PIM-DM	Y	
IPv4 Multicast Switching	Y	
Add tags to static-route command to enable easier redistribution	Y	
BGP with graceful restart	Y	
BGP route reflector for IPv6	N	
BGP ASPATH Filtering for IPv6 routes on IPv6 peering	N	
BGP support of MD5 password for IPv6	N	
BGP 4-Octet ASN Support	Y	
GRE	N	
IP-IP tunneling	N	
IP routed port	Y	
IPv6	Y	JITC
IPv6 DHCP relay and Neighbor discovery proxy	N	
ISIS IPv4/IPv6	Y	JITC
M-ISIS	N	
OSPFv3	Y	JITC
RIP v1/v2	Y	
RIPng	N	
DHCP Server (v4, v6 with integrated support of QIP remote management)	Y	
VRRP v2	Y	
VRRP v3	N	
ARP - Proxy	Y	Static ARP with multicast MAC not supported
ARP - Distributed	N	
BFD	N	
DHCP Snooping	Y	
DHCP Snooping IP source filtering - VLAN/port-based	N	
DHCPv6 Relay	N	
IP Multinetting	N	
IPSec	Y	JITC
Server Load Balancing (SLB)	N	
<b>Multicast Features</b>		
IGMP v1/v2/v3	Y	
IPv4 Multicast Switching	Y	
PIM-DM	Y	
DVMRP	N	

Feature	OS9900	Notes
IPv6 Multicast Switching (MLD v1/v2)	N	
IPv6 Scoped Multicast Addresses	N	
PIM-SM	Y	
PIM-SSM	Y	
PIM-SSM Static Map	N	
PIM-BiDir	N	
Static Layer 2 Multicast	N	
<b>Monitoring/Troubleshooting Features</b>		
Extended ping and traceroute	Y	
Port mirroring	Y	
Port monitoring	Y	
Switch logging / Syslog	Y	
RMON	EA	
SFlow	N	
Policy based mirroring	N	
Port mirroring - remote	N	
TDR	N	
<b>Layer 2 Feature Support</b>		
802.1q	Y	
Spanning Tree (802.1ad, 802.1w, MSTP, PVST+, Root Guard)	Y	PVST+ and STP loopguard not supported on OS9900.
LLDP (802.1ab)	Y	
Link Aggregation (static and LACP)	Y	
STP Loop Guard	EA	
DHL	N	
ERP v1/v2	N	
HAVLAN	N	
Loopback detection - Edge (Bridge)	Y	
Loopback detection - SAP (Access)	N	
MVRP	Y	
Private VLANs	N	
Source Learning - Distributed Mode	N	
SIP Snooping	N	
<b>QoS Feature Support</b>		
Qos Policy	Y	Not supported on CPU generated packets.
Qos policy logging	N	
Port trust	Y	
QSP Profiles	Y	OS9900 - QSP 1 and 5 only.

Feature	OS9900	Notes
Per port rate limiting	N	
802.1p / ToS / DSCP priority mapping	Y	
Auto-Qos prioritization of NMS/IP Phone Traffic	Y	
Control packet priority	Y	
IPv6 QoS	N	
ACL - IPv4	Y	
ACL - IPv6	N	
MAC Groups	Y	
Network Groups	Y	
Port Groups	Y	
Agg ID in Port Group	N	
Service Groups	Y	
Map Groups	Y	
Switch Groups	Y	
Policy Lists	Y	
Egress Policy Rules	N	
Policy based routing	N	
PBM	N	
Port Ingress/Egress bandwidth limit	Y	
Tri-color marking	N	
Strict Priority	Y	
WRR	Y	
WRR+SP	Y	
QSP Profiles 2/3/4	N	
<b>Metro Ethernet Features</b>		
Ethernet Services	N	
Ethernet OAM (ITU Y1731 and 802.1ag)	EA	
<b>Security Features</b>		
Access Guardian - UNP	Y	(802.1x, MAC, default profile, binding classification, atomic classification).  User role not supported. Ingress/Egress bandwidth not supported. Extended classification not supported. Location-Policy, Time-Policy not supported. SAP port configuration not supported.
Access Guardian - BYOD	N	
Interface Violation Recovery	EA	
Learned Port Security (LPS)	Y	

Feature	OS9900	Notes
LLDP Rogue Detection	Y	
TACACS+ Client	Y	
TACACS+ command based authorization	EA	
Accounting	N	
Application Monitoring and Enforcement (Appmon)	N	
ARP Poisoning Protection	Y	
Application Fingerprinting	N	
COA Extension support for RADIUS (BYOD)	N	
mDNS Snooping/Relay (BYOD)	N	
UPNP/DLNA Relay (BYOD)	N	
Switch Port location information pass-through in RADIUS requests (BYOD)	N	
Captive Portal	Y	
Quarantine Manager	N	
Radius test tool	N	
Storm Control	N	
<b>PoE Features</b>		
802.1af and 802.3at	Y	
Auto Negotiation of PoE Class-power upper limit	Y	
Display of detected power class	Y	
LLDP/802.3at power management TLV	Y	
HPOE support (60W/75W)	Y (75W)	
POE Time Of Day Support	Y	
<b>Data Center Features</b>		
CEE DCBX Version 1.01	N	
Data Center Bridging (DCBX/ETS/PFC)	N	
EVB	N	
FCoE / FC Gateway	N	
FIP Snooping	N	
IPv4 over SPB	N	
RFP on SPB UNI port	N	
SPB	N	
VXLAN	N	
VM/VXLAN Snooping	N	

---

Feature	OS9900	Notes
Other Features		
Dying Gasp	N	
Update MAC Range for IP Phones	N	
Auto LLDP Vlan assignment for IP touch phones	N	

## **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 VC (when applicable) 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 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 GA or 8.3.1.R01 maintenance release	Upgrading From 8.3.1.R02 GA Release
OS9900 - Standalone (Dual-CMM)	ISSU - Not Supported Standard - Supported	ISSU - Supported Standard - Supported
OS9900 - Standalone (Single-CMM)	ISSU - N/A Standard - Supported	ISSU - N/A Standard - Supported

### 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 switch during the ISSU process.
- Knowledge of various aspects of AOS directory structure, operation and CLI commands can be found in the user guides. Recommended reading includes:
  - Release Notes - for the version of software you're planning to upgrade to.
  - The 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

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.

```
OS9900-> show system
System:
  Description: Alcatel-Lucent Enterprise OS9900 8.3.1.314.R01 Service Release, September 05,
2016.,
  Object ID: 1.3.6.1.4.1.6486.801.1.1.2.1.12.1.1,
  Up Time: 0 days 0 hours 1 minutes and 44 seconds,
  Contact: Alcatel-Lucent, http://enterprise.alcatel-lucent.com
  Name: OS9900,
  Location: Unknown,
  Services: 78,
  Date & Time: FRI OCT 31 2016 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:

```
OS9900-> rm *.log
OS9900-> 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:

```
OS9900-> 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'**:

```
OS9900-> 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:

```
OS9900-> show tech-support
OS9900-> show tech-support layer2
OS9900-> 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.

```
OS9900-> 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 using a standard upgrade procedure please refer to [Appendix C](#) for specific steps to follow.

## Appendix C: Standard Upgrade - OmniSwitch Standalone Chassis

These instructions document how to upgrade a standalone 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:

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

```
OS9900-> 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....
```

### 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.

```
OS9900-> show microcode
 /flash/working
Package      Release      Size  Description
-----+-----+-----+-----
Mos.img      8.4.1.193.R01  210697424 Alcatel-Lucent OS
Meni.img     8.4.1.193.R01  114810228 Alcatel-Lucent NI
Mhost.img    8.4.1.193.R01  50274908  Alcatel-Lucent Host Image
```

```
-> 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.

```
OS9900-> copy running certified
```

```
-> show running-directory
```

**CONFIGURATION STATUS**

```
Running CMM      : MASTER-PRIMARY,  
CMM Mode        : VIRTUAL-CHASSIS MONO CMM,  
Current CMM Slot : CHASSIS-1 A,  
Running configuration : WORKING,  
Certify/Restore Status : CERTIFIED
```

**SYNCHRONIZATION STATUS**

```
Running Configuration : SYNCHRONIZED
```

## Appendix D: ISSU - OmniSwitch Standalone Chassis

These instructions document how to upgrade a modular 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:

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

```
OS9900-> mkdir /flash/issu_dir
```

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

```
OS9900-> 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:

```
OS9900-> ls /flash/issu_dir
Mos.img  Meni.img  Mhost.img  issu_version  vcboot.cfg  vcsetup.cfg
```

### 9. Upgrade the image files using ISSU:

```
OS9900-> 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)

```
OS9900-> show issu status
Issu pending
```

This indicates that the ISSU is completed

```
OS9900-> 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.

## 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.

```
OS9900-> show microcode
/flash/working
Package           Release           Size             Description
-----+-----+-----+-----
-
Mos.img           8.4.1.193.R01    210697424       Alcatel-Lucent OS
Meni.img          8.4.1.193.R01    114810228       Alcatel-Lucent NI
Mhost.img         8.4.1.193.R01    50274908        Alcatel-Lucent Host Image
```

## 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:

```
OS9900-> copy running certified
-> show running-directory
CONFIGURATION STATUS
Running CMM           : MASTER-PRIMARY,
CMM Mode              : VIRTUAL-CHASSIS DUAL CMMs,
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.

223602	Correction to make chassis reach ready state without any NI presents in the chassis.
223887	Dynamic ARP not updated while static ARP resolves the ping issue.
224357	Port mirroring accepting 2 destination ports in configuration.
224838	Clarification required on the fan behavior to prevent being set to 100% after CMM extraction.
226109	In 9900 VRRP, OSPF flapping issue due to NI4 down: niMgrProcessHealthCheckTimeout: health check reset for ni.