Release Notes

OmniSwitch 6350/6450

Release 6.7.2.R04

These release notes accompany release 6.7.2.R04 software for the OmniSwitch6350/6450 series of switches. The document provides important information on individual software and hardware features. Since much of the information in the release notes is not included in the hardware and software user manuals, it is important to read all sections of this document before installing new hardware or loading new software.

Note: The OmniSwitch 6250 is not supported in this release.

Table of Contents

Related Documentation

The release notes should be used in conjunction with the associated manuals as listed below.
User manuals can be downloaded at: https://businessportal2.alcatel-lucent.com

OmniSwitch 6450 Hardware Users Guide
Complete technical specifications and procedures for all OmniSwitch 6450 Series chassis, power supplies, and fans.

OmniSwitch 6350 Hardware Users Guide
Complete technical specifications and procedures for all OmniSwitch 6350 Series chassis, power supplies, and fans.

OmniSwitch AOS Release 6 CLI Reference Guide
Complete reference to all CLI commands supported on the OmniSwitch. Includes syntax definitions, default values, examples, usage guidelines, and CLI-to-MIB variable mappings.

OmniSwitch AOS Release 6 Network Configuration Guide
Includes network configuration procedures and descriptive information on all the major software features and protocols included in the base software package. Chapters cover Layer 2 information (Ethernet and VLAN configuration), Layer 3 information (routing protocols), security options (Authenticated Switch Access (ASA)), Quality of Service (QoS), link aggregation.

OmniSwitch AOS Release 6 Switch Management Guide
Includes procedures for readying an individual switch for integration into a network. Topics include the software directory architecture, software rollback protections, authenticated switch access, managing switch files, system configuration, using SNMP, and using web management software (WebView).

OmniSwitch AOS Release 6 Transceivers Guide
Includes transceiver specifications and product compatibility information.

Technical Tips, Field Notices, Upgrade Instructions
Contracted customers can visit our customer service website at: https://businessportal2.alcatel-lucent.com

AOS6.7.2.R04 Prerequisites

N/A

System Requirements

Memory Requirements

The following are the requirements for the OmniSwitch6350/6450 Series Release 6.7.2.R04:

- OmniSwitch 6350/6450 Series requires 256 MB of SDRAM and 128MB of flash memory. This is the standard configuration shipped.
- Configuration files and the compressed software images—including web management software (WebView) images—are stored in the flash memory. Use the **show hardware info** command to determine your SDRAM and flash memory.

Miniboot and FPGA Requirements for Existing Hardware

The software versions listed below are the minimum required version for existing models, except where otherwise noted. Switches running the minimum versions, as listed below; do not require any miniboot or CPLD upgrade.

Switches not running the minimum version required should be upgraded to the latest Uboot/Miniboot or CPLD that is available with the 6.7.2.R04 AOS software available from Service & Support.

OmniSwitch 6450-10(L)/P10(L)

Release	Uboot/Miniboot	CPLD
6.7.2.191.R04(GA)	6.6.3.259.R01	6

OmniSwitch 6450-24/P24/48/P48

Release	Uboot/Miniboot	CPLD
6.7.2.191.R04(GA)	6.6.3.259.R01	11

OmniSwitch 6450-U24

Release	Uboot/Miniboot	CPLD
6.7.2.191.R04(GA)	6.6.3.259.R01	6

OmniSwitch 6450-24L/P24L/48L/P48L

Release	Uboot/Miniboot	CPLD
6.7.2.191.R04(GA)	6.6.4.54.R01	11

OmniSwitch 6450-P10S/U24S

Release	Uboot/Miniboot	CPLD
6.7.2.191.R04(GA)	6.6.5.41.R02	P10S - 4 U24S – 7

OmniSwitch 6450-M/X Models

Release	Uboot/Miniboot	CPLD
6.7.2.191.R04(GA)	6.7.1.54.R02	10M – 6 24X/24XM/P24X/48X/P48X – 11 U24SXM/U24X - 7

OmniSwitch 6350-24/P24/48/P48

Release	Uboot/Miniboot	CPLD
6.7.2.191.R04(GA)	6.7.1.69.R01/6.7.1.103.R01 6.7.1.30.R04 (optional)	12 (minimum) 16 (optional)

Release	Uboot/Miniboot	CPLD
Note: The optional uboot/miniboot and CPLD is only needed for stacking support. Standalone units can remain at the previous versions.		

OmniSwitch 6350-10/P10

Release	Uboot/Miniboot	CPLD
6.7.2.191.R04(GA)	6.7.1.30.R04	4

Note: Refer to the Upgrade Instructions section for upgrade instructions and additional information on Uboot/Miniboot and CPLD requirements.

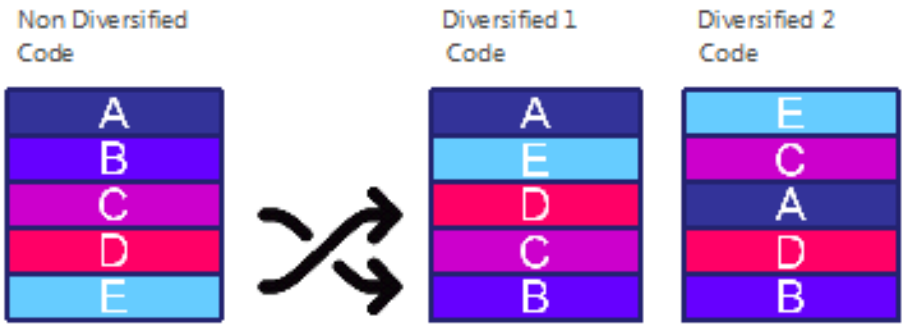
CodeGuardian

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

Chassis	Standard AOS Releases	AOS CodeGuardian Release	LGS AOS CodeGuardian Release
OmniSwitch 6450	AOS 6.7.2.R04	AOS 6.7.2.RX4	AOS 6.7.2.LX4

X=Diversified image 1-3
ALE will have 3 different diversified images per AOS release (R14 through R34)
Our partner LGS will have 3 different diversified images per AOS release (L14 through L34)

6.7.2.R04 New Hardware Supported

There is no new hardware in this release.

6.7.2.R04 New Software Features and Enhancements

The following software features are new with this release, subject to the feature exceptions and problem reports described later in these release notes:

Feature	Platform	License
Stack Topology Change Notification	OS6350/OS6450	N/A
OV Cirrus Enhancements	OS6350/OS6450	N/A
SCP Server Support	OS6350/OS6450	N/A
Multicast star-G Mode Support for IPv4	OS6350/OS6450	N/A
Extended Support of Number of IPv4 Interfaces and Static Routes.	OS6350	N/A
Disable MAC Aging for Silent Devices	OS6350/OS6450	N/A
Enhancement of DHCP Snooping Table Display	OS6350/OS6450	N/A
Delayed Start of PoE	OS6350/OS6450	N/A
DHCP Server Precedence in DHCP Client Interface	OS6350/OS6450	N/A
SNMPv3 View Based Access	OS6350/OS6450	N/A
Support to Save Configuration in RCL Script	OS6350/OS6450	N/A
Additional OUI MAC Range Support IP Phones	OS6350/OS6450	N/A

Feature Summary Table

New Feature Descriptions

Stack Topology Change Notification
This feature will send a trap whenever there is a change to the stack topology such as an NI being removed or added to the stack. Additionally, when issuing the **write memory** command, if any one of the stack NIs is down a warning will be displayed about a possible configuration purge for the down NI and ask for confirmation from the user to proceed. This feature is enabled by default.

OV Cirrus Enhancements
OV Cirrus enhancements in this release are:

- **Cloud-agent admin-state restart** : A new parameter '*restart'* is added to existing CLI command '*cloud-agent admin-state {enable|disable}*' to restart cloud-agent functionality without the need to reboot the switch. '*cloud-agent admin-state restart'* command when executed will force disable and then enable again to re-initiate Call Home automatically.

- **Periodic CallHome of OV Cirrus** : OmniSwitch is now capable of triggering automatic periodic Call Home request to Activation Server. Periodic contact with Activation Server helps retrieval of latest configuration and latest software version (if user desires so) from OV Cirrus, if OmniSwitch is in DeviceManaged state. Periodic Call Home is triggered based on a Time-to-Next-Call-Home timer value from server. If OmniSwitch is in an Error state after last Call Home, or if the OmniSwitch is in a *DeviceNotManaged* state, the time interval to next Call Home is governed by this timer value. If OmniSwitch is already in *DeviceManaged* state, the VPN connection to OV Cirrus will be kept undisturbed during each Call Home if there is no difference in VPN parameters from the previous values.

- **PreprovisionFailed Retry**: If OmniSwitch gets into '*PreprovisionFailed*' state due to failure in pre-provisioning server connectivity or failure during pre-provisioning transactions, a retry mechanism is introduced in AOS. With this, OmniSwitch automatically does "Hello OV" with a periodicity of 30 minutes by default. If Time-to-Next-Call-Home value is offered to OmniSwitch during pre-provision phase, the periodicity is instead governed by this timer value.This enhancement provides an option for the users to rectify possible errors and for the OmniSwitch to get out of '*PreprovisionFailed*' state and proceed with the next transaction.

- **FQDN support for NTP server** : NTP server configuration can also be configured with hostname/FQDN. The CLI commands "show ntp client, show ntp client server-list" will now display IP address as well as FQDN format according to the format in which the particular server was configured.

- **Default NTP pool server configuration for OV Cirrus :** A new provision for configuring default NTP servers is added, when the DHCP server does not send any NTP configuration to cloud agent. This avoids issues during deployment, in which the certificate verification has failed due to mismatch in time as NTP configuration is not present in the switch. The NTP pool server configuration provides a default NTP source for cloud operations, when there is no NTP server specified in the device configuration file and none is supplied by DHCP.

- **Hostname in FQDN format**: Configuring hostname for the redirect server in FQDN format is added to the "*aaa redirect-server*" CLI command. In the OV Cirrus, when the OV/UPAM is migrated to another Virtual Machine or the OV Virtual Machine is restarted and gets new IP, then the new IP should be reconfigured to all affected switches/APs. To avoid this problem OV Cloud requires FQDN to be configured Instead of IP.

Additional OUI MAC Range Support IP phones
The IP phone MAC range is updated to automatically apply the QoS IP phone priority for the packets received from the source MAC in the following range:

MAC Address Range	Description
00:80:9F:00:00:00 to 00:80:9F:FF:FF:FF	Enterprise IP Phones Range
78:81:02:00:00:00 to 78:81:02:FF:FF:FF	Communications IP Phones Range
00:13:FA:00:00:00 to 0:13:FA:FF:FF:FF	Lifesize IP Phones Range
48-7A-55-00-00-00 to 48-7A-55-FF-FF-FF	ALE 8008 IP Phone MAC Range

SCP Server Support
SCP utilizes an underlying SSH connection and transfers file over this tunnel. The underlying SSH tunnel ensures data integrity, user authentication and protection against snooping. SCP makes use of remote command execution facility provided by SSH.
The switch can act as an SCP server for sending or receiving files from the workstation. You can send software files to the switch by using standard SCP client software located on a host workstation. This is normally done to load or upgrade the switch software.
SCP file transfer requests originating from command-line based SCP clients will be accepted. However, SCP requests originating from GUI-based SSH clients will not be accepted.

Multicast Star-G mode Support for IPv4
When multiple hosts are a part of single multicast group, every host will have an unique entry in the IPMC table. This occupies more hardware entries in IPMC thus affecting other normal multicast services. In such a scenario, configuring star-G (*, G) mode for the multicast group reduces the IPMC index utilization by preventing creation of multiple multicast entries. Single star-G entry for the multicast group is created in the IPMC table.

Extended Support of Number of IPv4 Interfaces and Static Routes
OmniSwitch supports increase of static routes and IP interfaces to 64 and 32 respectively. Use **ip tables extend** command to extend the number of IPv4 interfaces and IPv4 static routes supported on the switch by reducing the number of IPv6 neighbor entries to 76.

Disable MAC Aging for Silent Devices
The OmniSwitch supports the flush of MAC address table when MAC aging timeout happens for non-supplicant client. The flushed MAC addresses are authenticated only upon reception of traffic from client. This causes many silent device MAC address to be flushed from the switch.
In the OmniSwitch, by default, the inactivity logout is enabled and the MAC is flushed out after MAC aging. The feature allows to disable the inactivity logout so the MAC entry is re-programmed in the switch after MAC aging without any re-authentication initiated by the switch. This avoids the MAC address timeout for non-supplicant users.

Enhancement of DHCP Snooping Table Display
This enhances the display of DHCP binding table entries for easier troubleshooting. The DHCP-snooping binding table entry can be viewed in ascending order with respect to slot /port , IP address, or linkagg.

Delayed Start on PoE
This feature allows to set a delay timer to delay the power supply to the PoE port when the NI is rebooted. The provision is applicable only for reboot.

DHCP Server Precedence in DHCP Client Interface
A 30 second time window is activated when DHCP client interface is created with server-preference enabled. First preference is given for the OVCirrus server, the client waits for 30 seconds from the time of sending discovery even after receiving OFFER from other servers other than OVCirrus.
DHCP server preference for the DHCP client can be configured. This allows the DHCP client to accept the lease from the preferred server from the multiple DHCP offers received.

The type of DHCP server sending offers will be identified by the VSI string (option 43) configuration.
When server-preference is enabled, the following precedence order is followed:

1. OVCloud : "alenterprise"
2. OVClient : "alcatel.nms.ov2500"
3. OXO : "alcatel.a4400.0"
4. Others / Undesired : Identified by absence of VSI string

SNMPv3 View Based Access
An SNMP user can include or exclude the specific OIDs in the SNMP view and can have restricted access to the MIBs based on the include or exclude list of OIDs present in the view. The views can be associated with any number of users.
A new CLI command is introduced to create or remove an SNMP view with include or exclude option.
snmp view viewname oid-tree {include | exclude}
no snmp view viewname oid-tree {include | exclude}

Support to Save Configuration in RCL Script
The OmniSwitch downloads the script file from the FTP/SFTP server and runs the commands in the script file. The script file contains all the configurations, and **write memory**, **copy working certified** commands.

Unsupported Software Features

CLI commands and Web Management options may be available in the switch software for the following features. These features are not supported:

Feature	Platform
BGP	6350/6450
DVMRP	6350/6450
IS-IS	6350/6450
Multicast Routing	6350/6450
OSPF	6350/6450
PIM	6350/6450
Traffic Anomaly Detection	6350/6450
IPv6 Sec	6350/6450
IP Tunnels (IPIP, GRE, IPv6)	6350/6450
Server Load Balancing	6350/6450
VLAN Stacking / Ethernet Services	OS6350
Ethernet/Link/Test OAM	OS6350
PPPoE	OS6350
ERP	OS6350
GVRP	OS6350
IPv4/ IPv6 RIP	OS6350
VRRP	OS6350
HIC/ BYOD / Captive Portal	OS6350
mDNS Relay	OS6350
IPMVLAN (VLAN Stacking Mode)	OS6350
IPMC Receiver VLAN	OS6350
OpenFlow	OS6350
License Management	OS6350
Loopback Detection	OS6350
SAA	OS6350
Ethernet Wire-rate Loopback Test	OS6350
Dying Gasp	OS6350

Unsupported CLI Commands

The following CLI commands are not supported in this release of the software:

Software Feature	Unsupported CLI Commands
AAA	aaa authentication vlan single-mode aaa authentication vlan multiple-mode aaa accounting vlan show aaa authentication vlan show aaa accounting vlan
CPE Test Head	test-oam direction bidirectional test-oam role loopback
Chassis Mac Server	mac-range local mac-range duplicate-eeprom mac-range allocate-local-only show mac-range status
DHCP Relay	ip helper traffic-suppression ip helper dhcp-snooping port traffic-suppression
Ethernet Services	ethernet-services sap-profile bandwidth not-assigned
Flow Control	flow
Hot Swap	reload ni [slot] # [no] power ni all
Interfaces	show interface slot/port hybrid copper counter errors show interface slot/port hybrid fiber counter errors
QoS	qos classify fragments qos flow timeout
System	install power ni [slot]

Open Problem Reports and Feature Exceptions

The problems listed here include problems known at the time of the product's release. Any problems not discussed in this section should be brought to the attention of the Service and Support organization as soon as possible. Please contact customer support for updates on problem reports (PRs) where no known workaround was available at the time of release.

CR	Description	Workaround
CRAOS6X-784	In OmniSwitch, after applying policies from OV Cirrus, when a reload or takeover is applied and saved, a *boot.cfg.err* file is generated while booting up. This is due to limitation in policy name being above 32 characters.	The policy name should be modified to be less than 32 characters.

Redundancy/ Hot Swap

CMM (Primary Stack Module) and Power Redundancy Feature Exceptions

- Manual invocation of failover (by user command or Primary pull) must be done when traffic loads are minimal.
- Hot standby redundancy or failover to a secondary CMM without significant loss of traffic is only supported if the secondary is fully flash synchronized with the contents of the primary's flash.
- Failover/Redundancy is not supported when the primary and secondary CMMs are not synchronized (i.e., unsaved configurations, different images etc.).
- When removing modules from the stack (powering off the module and/or pulling out its stacking cables), the loop back stacking cable must be present at all times to guarantee redundancy. If a module is removed from the stack, rearrange the stacking cables to establish the loopback before attempting to remove a second unit.
- When inserting a new module in the stack, the loopback has to be broken. Full redundancy is not guaranteed until the loopback is restored.

Stack Element Insert/Removal Exceptions

- All insertions and removals of stack elements must be done one at a time and the inserted element must be fully integrated and operational as part of the stack before inserting another element.

- When hot-swapping any element of the stack it must be replaced by the same model. For example, anOS6450-P24 model can only be hot-swapped with another OS6450-P24 model.

Hot Swap / Insert of 1G/10G Modules on OS6450

- Inserting a 10G module into a slot that was empty does not require a reboot.
- Inserting a 10G module into a slot that had a 10G module does not require a reboot.
- Inserting a 10G module into a slot that had a 1G module requires a reboot.
- Inserting a 1G module into a slot that was empty requires a reboot.
- Inserting a 1G module into a slot that had a 1G module does not require a reboot.
- Inserting a 1G module into a slot that had a 10G module requires a reboot.

Note: Precision Time Protocol (PTP) is not supported when the OS6450-U24S is in stacking mode. If the OS6450-U24S is in stacking mode, or one of the hot swap scenarios above causes it to boot up in stacking mode, PTP will be disabled.

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
Europe 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 Alcatel-Lucent service agreements may open cases 24 hours a day via Alcatel-Lucent Enterprise support web page at: https://businessportal2.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 telnet or dial-in access, hardware configuration—module type 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.

Appendix A: AOS 6.7.2.R04 Upgrade Instructions

OmniSwitch Upgrade Overview

This section documents the upgrade requirements for an OmniSwitch. These instructions apply to the following:

- OmniSwitch 6450 models being upgraded to AOS 6.7.2.R04.
- OmniSwitch 6350 models being upgraded to AOS 6.7.2.R04.

Prerequisites

This instruction sheet requires that the following conditions are understood and performed, BEFORE upgrading:

- Read and understand the entire Upgrade procedure before performing any steps.
- 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 users will be affected by this procedure.
  - Have a working knowledge of the switch to configure it to accept an FTP connection through the Network Interface (NI) Ethernet port.
- Read the Release Notes prior to performing any upgrade for information specific to this release.
- All FTP transfers MUST be done in binary mode.

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

OmniSwitch Upgrade Requirements

These tables list the required Uboot/Miniboot, CPLD and AOS combinations for upgrading an OmniSwitch. The Uboot/Miniboot and CPLD may need to be upgraded to the versions listed below to support AOS Release 6.7.2.R04.

Version Requirements – Upgrading to AOS Release 6.7.2.R04

Version Requirements to Upgrade to AOS Release 6.7.2.R04			
	AOS	**Uboot/Miniboot**	**CPLD**
6450-10/10L/P10/P10L	6.7.2.191.R04 GA	6.6.3.259.R01	6
6450-24/P24/48/P48		6.6.3.259.R01	11
6450-U24		6.6.3.259.R01	6
6450-24L/P24L/48L/P48L		6.6.4.54.R01	11
6450-P10S		6.6.5.41.R02	4
6450-U24S		6.6.5.41.R02	7
6450-10M		6.7.1.54.R02	6
6450-24X		6.7.1.54.R02	7
6450- 24XM,24X,P24X,P48X,		6.7.1.54.R02	11
6350-24/P24/48/P48	6.7.2.191.R04 GA	6.7.1.69.R01/6.7.1.103.R01 (minimum) 6.7.1.30.R04 (optional)	12 (minimum) 16 (optional)
6350-10/P10		6.7.1.30.R04	4
• The OS6450 "L" models were introduced in AOS Release 6.6.4.R01 and ship with the correct minimum versions, no upgrade is required. • Uboot/Miniboot versions 6.6.4.158.R01 and 6.6.4.54.R01 were newly released versions in 6.6.4.R01. • CPLD versions 14, 6, and 11 were newly released versions in 6.6.4.R01. • Uboot/Miniboot version 6.6.3.259.R01 was previously released with 6.6.3.R01. • CPLD version 12 was previously released with 6.6.3.R01.			

- IMPORTANT NOTE: If performing the optional upgrade BOTH Uboot/Miniboot and CPLD MUST be upgraded.
- The 6.7.1.30.R04 uboot/miniboot and CPLD 16 for the 6350-24/48 models is only needed for stacking support. Standalone units can remain at the previous version.

Upgrading to AOS Release 6.7.2.R04

Upgrading consists of the following steps. The steps must be performed in order. Observe the following prerequisites before performing the steps as described below:

- Upgrading an OmniSwitch to AOS Release 6.7.2.R04 may require two reboots of the switch or stack being upgraded. One reboot for the Uboot/Miniboot or AOS and a second reboot for the CPLD.
- Refer to the Version Requirements table to determine the proper code versions.
- Download the appropriate AOS images, Uboot/Miniboot, and CPLD files from the Service & Support website.

Summary of Upgrade Steps

1. FTP all the required files to the switch
2. Upgrade the Uboot/Miniboot and AOS images as required. Reboot the switch.
3. Upgrade the CPLD as required. (Switch automatically reboots).
4. Verify the upgrade and remove the upgrade files from the switch.

Upgrading - Step 1. FTP the 6.7.2.R04 Files to the Switch

Follow the steps below to FTP the AOS, Uboot/Miniboot, and CPLD files to the switch.

1. Download and extract the upgrade archive from the Service & Support website. The archive will contain the following files to be used for the upgrade:
   - Uboot/Miniboot Files – kfu-boot.bin, kfminiboot.bs (optional)
   - AOS Files (6450) – KFbase.img, KFeni.img, KFos.img, KFsecu.img
   - AOS Files (6350) – KF3base.img, KF3eni.img, KF3os.img, KF3secu.img
   - CPLD File - KFfpga_upgrade_kit (optional)
2. FTP (Binary) the Uboot/Miniboot files listed above to the **/flash** directory on the primary CMM, if required.
3. FTP (Binary) the CPLD upgrade kit listed above to the **/flash** directory on the primary CMM, if required.
4. FTP (Binary) the image files listed above to the **/flash/working** directory on the primary CMM.
5. Proceed to Step 2.

Note: Make sure the destination paths are correct when transferring the files. Also, when the transfer is complete, verify the file sizes are the same as the original indicating a successful binary transfer.

Upgrading - Step 2. Upgrade Uboot/Miniboot and AOS

Follow the steps below to upgrade the Uboot/Miniboot (if required) and AOS. This step will upgrade both Uboot/Miniboot and AOS once the switch/stack is rebooted. If an Uboot/Miniboot upgrade is not required skip to rebooting the switch to upgrade the AOS.

1. Execute the following CLI command to update the Uboot/Miniboot on the switch(es) (can be a standalone or stack).
   -> update uboot all
   -> update miniboot all
   - If connected via a console connection update messages will be displayed providing the status of the update.
   - If connected remotely update messages will not be displayed. After approximately 10 seconds issue the '**show ni**' command, when the update is complete the **UBOOT-Miniboot Version** will display the upgraded version.

WARNING: DO NOT INTERRUPT the upgrade process until it is complete. Interruption of the process will result in an unrecoverable failure condition.

2. Reboot the switch. **This will update both the Uboot/Miniboot (if required) and AOS**.
   -> reload working no rollback-timeout
3. Once the switch reboots, certify the upgrade:
   - If you have **a single CMM** enter:
   -> copy working certified

   - If you have **redundant CMMs** enter:
   -> copy working certified flash-synchro
4. Proceed to Step 3 (Upgrade the CPLD).

Upgrading - Step 3. Upgrade the CPLD

Follow the steps below to upgrade the CPLD (if required). Note the following:

- The CMMs must be certified and synchronized and running from Working directory.
- This procedure will automatically reboot the switch or stack.

WARNING: During the CPLD upgrade, the switch will stop passing traffic. When the upgrade is complete, the switch will automatically reboot. This process can take up to 5 minutes to complete. Do not proceed to the next step until this process is complete.

Single Switch Procedure

1. Enter the following to begin the CPLD upgrade:
   -> update fpgacmm

The switch will upgrade the CPLD and reboot.

Stack Procedure

Updating a stack requires all elements of the stack to be upgraded. The CPLD upgrade can be completed for all the elements of a stack using the 'all' parameter as shown below.

1. Enter the following to begin the CPLD upgrade for all the elements of a stack.
   -> update fpgani all

The stack will upgrade the CPLD and reboot.

Proceed to Verifying the Upgrade to verify the upgrade procedure.

Verifying the Upgrade

The following examples show what the code versions should be after upgrading to AOS Release 6.7.2.R04.

Note: These examples may be different depending on the OmniSwitch model upgraded. Refer to the Version Requirements tables to determine what the actual versions should be.

Verifying the Software Upgrade

To verify that the AOS software was successfully upgraded, use the show microcode command as shown below. The display below shows a successful image file upgrade.

```
-> show microcode
  Package          Release      Size     Description
-----------------+--------------+--------+----------------------------------
KFbase.img        6.7.2.191.R04   18130755 Alcatel-Lucent Enterprise Base Softw
KFos.img          6.7.2.191.R04    3562484 Alcatel-Lucent Enterprise OS
KFeni.img         6.7.2.191.R04    6152493 Alcatel-Lucent Enterprise NI softwar
KFsecu.img        6.7.2.191.R04     648189 Alcatel-Lucent Enterprise Security M
KFdiag.img        6.7.2.191.R04    2411898 Alcatel-Lucent Enterprise Diagnostic
```

Verifying the U-Boot/Miniboot and CPLD Upgrade

To verify that the CPLD was successfully upgraded on a CMM, use the show hardware info command as shown below.

```
-> show hardware info

CPU Type                    : Marvell Feroceon,
Flash Manufacturer          : Numonyx, Inc.,
Flash size                  : 134217728 bytes (128 MB),
RAM Manufacturer            : Samsung,
RAM size                    : 268435456 bytes (256 MB),
Miniboot Version            : 6.6.4.158.R01,
Product ID Register         : 05
Hardware Revision Register  : 30
FPGA Revision Register      : 014
```

You can also view information for each switch in a stack (if applicable) using the show ni command as shown below.

```
-> show ni
Module in slot 1
Model Name:                 OS6450-24,
Description:                24 10/100 + 4 G,
Part Number:                902736-90,
Hardware Revision:          05,
Serial Number:              K2980167,
Manufacture Date:           JUL 30 2009,
Firmware Version:           ,
Admin Status:               POWER ON,
Operational Status:         UP,
Power Consumption:          30,
Power Control Checksum:     0xed73,
CPU Model Type :            ARM926 (Rev 1),
MAC Address:                00:e0:b1:c6:b9:e7,
ASIC - Physical 1:          MV88F6281 Rev 2,
FPGA - Physical 1:          0014/00,
UBOOT Version :             n/a,
UBOOT-miniboot Version :    6.6.4.158.
```

Note: It is OK for the 'UBOOT Version' to display "n/a". The 'UBOOT-miniboot' version should be the upgraded version as shown above.

Remove the CPLD and Uboot/Miniboot Upgrade Files

After the switch/stack has been upgraded and verified the upgrade files can be removed from the switch.

1. Issue the following command to remove the upgrade files.
   ->rmKFfpga.upgrade_kit
   ->rmkfu-boot.bin
   ->rm kfminiboot.bs

Appendix B: AOS 6.7.2.R04 Downgrade Instructions

OmniSwitch Downgrade Overview

This section documents the downgrade requirements for the OmniSwitch models. These instructions apply to the following:

- OmniSwitch 6450 models being downgraded from AOS 6.7.2.R04.
  OmniSwitch 6350 models being downgraded from AOS 6.7.2.R04.

  Note: The OmniSwitch 6350-10/P10 require a minimum of AOS Release 6.7.1.R04 and cannot be downgraded to any other release.

  Note: The OmniSwitch PoE models with the new PoE controller require a minimum of AOS Release 6.7.2.R01 and cannot be downgraded to any other release.

- OS6350-P10 (903966-90)
- OS6350-P24 (903967-90)
- OS6350-P48 (903968-90)

Prerequisites

This instruction sheet requires that the following conditions are understood and performed, BEFORE downgrading:

- Read and understand the entire downgrade procedure before performing any steps.
- The person performing the downgrade 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 users will be affected by this procedure.
  - Have a working knowledge of the switch to configure it to accept an FTP connection through the Network Interface (NI) Ethernet port.
- Read the Release Notes prior to performing any downgrade for information specific to this release.
- All FTP transfers MUST be done in binary mode.

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

OmniSwitch Downgrade Requirements

Downgrading the Uboot/Miniboot or CPLD is not required when downgrading AOS from 6.7.2.R04. Previous AOS releases are compatible with the Uboot/Miniboot and CPLD versions shipping from the factory.

Summary of Downgrade Steps

1. FTP all the required AOS files to the switch
2. Downgrade the AOS images as required. (A reboot is required).
3. Verify the downgrade.

Downgrading - Step 1. FTP the 6.6.5 or 6.7.1 Files to the Switch

Follow the steps below to FTP the AOS files to the switch.

1. Download and extract the appropriate archive from the Service & Support website. The archive will contain the following files to be used for the downgrade:
   - AOS Files (OS6450) – KFbase.img, KFeni.img, KFos.img, KFsecu.img
   - AOS Files (OS6350) – KF3base.img, KF3eni.img, KF3os.img, KF3secu.img

2. FTP (Binary) the image files listed above to the **/flash/working** directory on the primary CMM.

3. Proceed to Step 2.

Note: Make sure the destination paths are correct when transferring the files. Also, when the transfer is complete, verify the file sizes are the same as the original indicating a successful binary transfer.

Downgrading - Step 2. Downgrade the AOS

Follow the steps below to downgrade the AOS. This step will downgrade the AOS once the switch/stack is rebooted.

1. Reboot the switch. **This will downgradethe AOS**.
   -> reload working no rollback-timeout

2. Once the switch reboots, certify the downgrade:
   - If you have **a single CMM** enter:

   -> copy working certified
   - If you have **redundant CMMs** enter:

   -> copy working certified flash-synchro

Proceed to Verifying the Downgrade

Verifying the Downgrade

To verify that the AOS software was successfully downgraded use the show microcode command as shown below. The example display below shows a successful image file downgrade. The output will vary based on the model and AOS version.

```
-> show microcode

Package          Release        Size       Description
-----------------+--------------+----------+-------------------------------------------
KFbase.img       6.6.5.R02   15510736  Alcatel-Lucent Base Software
KFos.img         6.6.5.R022511585  Alcatel-Lucent OS
KFeni.img        6.6.5.R025083931 Alcatel-Lucent NI software
KFsecu.img       6.6.5.R02597382 Alcatel-Lucent Security Management
```

Appendix C: Fixed Problem Reports

The following table lists the previously known problems that were fixed in this release.

CR/PR NUMBER	SUMMARY
CRAOS6X-67 TS 00273920	AOS crashed with suspension of the task "tahw_l2 "
CRAOS6X-73 TS 00274322	Unit 2 in the stack of 4 OS6450 switches without any external influence.
CRAOS6X-163 TS 00276622	OS6450 DHCPv6 not forwarded with 'ipv6 multicast status enable'
CRAOS6X-188 TS 00280451	Unit crashed with PMD on a OS6450 Stack
CRAOS6X-190 TS 00276752	6450: Topology Age does not reset when BPDU with TC bit set is received
CRAOS6X-212 TS 00274055	The switch fails to forward the DHCP client packet from the client to the server.
CRAOS6X-239 TS 00286893	OS6350-Unable to clear/cancel the DHCP server assigned IP address leases.
CRAOS6X-251 TS 00285427	OS6450 : RCA for the Primary unit crash.
CRAOS6X-288 TS 00276042	MACs status are filtering after reauthentication with 802.1x when PC reboots
CRAOS6X-300 TS 00288245	Unable to configure the Queue Bandwidth for QOS ports via WebView
CRAOS6X-305 TS 00290204	Randomly client connected to the AOS switch loses network connectivity
CRAOS6X-312 TS 00271660	NTP vulnerability: "CVE-2013-5211" on OS6450
CRAOS6X-447 CRAOS6X-53 TS 00272549	High CPU due to WebView/SsApp
CRAOS6X-503 TS 00292083	Wifi-Express LLDP messages are discarded by OmniSwitch
CRAOS6X-598 TS 00289497	MKB: OS6450- switch lost management IP (Old ref# 1-187700626/1-209109641)
CRAOS6X-620 TS 00297573	OS6450-P48/P24 & OS6350-P10 : LLDP configuration error
CRAOS6X-658 TS 00299031	OS6350: 802.1x port not flushing the PC MAC-address
CRAOS6X-663 TS 00298317	Config corrupt after 6450 stack reboot
PR 226927 SR 1-209350669	SSLv3 general query on the cipher / SSL-Poodle vulnerability check
PR 227663 SR 1-210816121	OS6450: Incorrect detection of non-STP traffic as STP traffic on User Ports to shutdown port via QoS.
PR 229855 SR 1-213478430	QoS User Port was shut down due to STP BPDU but for LLDP traffic.
PR 230349 SR 1-214904381	OS6450 crash when using 802.1q command with interface ranges
PR 230441 SR 1-214973201	AP1101 toggles up/down, LAN port remains up OS6450 (defaultWLANProfile used)
PR 230520	IGMP Static Group does not work in all failure cases of stacked 6450.

SR 1-215218640	
PR 230708 SR 1-215560901	VLAN 1 client not working in linkagg tagging with Vlan1 in latest release.
PR 230632 SR 1-215032601	OS6450: fan failure logs/traps not generated.
PR 230931 SR 1-217218738	Issue: Hash-key feature is not available in TACACS+ server
PR 232174 SR 1-220174470	OS6450: Unable to enable option 82 with port-alias.