Release Notes

OmniSwitch 6250/6350/6450

Release 6.7.1.R03

These release notes accompany release 6.7.1.R03 software for the OmniSwitch 6250/6350/6450 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.

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:
http://enterprise.alcatel-lucent.com/?dept=UserGuides&page=Portal

OmniSwitch 6250 Hardware Users Guide
Complete technical specifications and procedures for all OmniSwitch 6250 Series chassis, power supplies, and fans.

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 6250/6350/6450 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 6250/6350/6450 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 6250/6350/6450 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 6250/6350/6450 Transceivers Guide
Includes transceiver specifications and product compatibility information.

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

AOS 6.7.1.R03 Prerequisites

Please note the following important release specific information prior to upgrading or deploying this release. The information below covers important upgrade requirements, changes in AOS default behavior, and the deprecation of features.

- For a few seconds at the beginning of the boot up process random characters may be briefly displayed on the console of an OS6350. This is due to an initial baud rate mismatch. As soon as the bootrom is initialized the issue is automatically resolved.

System Requirements

Memory Requirements

The following are the requirements for the OmniSwitch 6250/6350/6450 Series Release 6.7.1.R03:

- OmniSwitch 6250/6350/6450 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 OS6250/6350/6450 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 6.7.1.R03 AOS software available from Service & Support.

OmniSwitch 6250 (All Models)

Release	Uboot/Miniboot	CPLD
6.7.1.86.R03(GA)	6.6.3.259.R01 6.6.4.158.R01 (optional – ships on all factory units)	12 14 (optional – ships on all factory units)
Note: The optional uboot/miniboot and CPLD upgrade fixes a known push button and LED issue and applies to existing OS6250 units, these versions will ship on all units from the factory. Refer to the Upgrade Instructions for additional information.		

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

Release	Uboot/Miniboot	CPLD
6.7.1.86.R03(GA)	6.6.3.259.R01	6

OmniSwitch 6450-24/P24/48/P48

Release	Uboot/Miniboot	CPLD
6.7.1.86.R03(GA)	6.6.3.259.R01	11

OmniSwitch 6450-U24

Release	Uboot/Miniboot	CPLD
6.7.1.86.R03(GA)	6.6.3.259.R01	6

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

Release	Uboot/Miniboot	CPLD
6.7.1.86.R03(GA)	6.6.4.54.R01	11

OmniSwitch 6450-P10S/U24S

Release	Uboot/Miniboot	CPLD

Release	Uboot/Miniboot	CPLD
6.7.1.86.R03(GA)	6.6.5.41.R02	P10S - 4 U24S – 7

OmniSwitch 6450-M/X Models

Release	Uboot/Miniboot	CPLD
6.7.1.86.R03(GA)	6.6.5.137.R02	10M – 6 24X/24XM/P24X/48X/P48X – 11 U24SXM/U24X - 7

OmniSwitch 6350-24/P24/48/P48

Release	Uboot/Miniboot	CPLD
6.7.1.86.R03(GA)	6.7.1.69.R01/6.7.1.103.R01	12

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

6.7.1.R03 New Hardware Supported

There is no new hardware being introduced in this release.

6.7.1.R03 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
Failover supplicant	OS6250/6450	N/A
Authentication Server Down	OS6250/6450	N/A
RADIUS Health Check	OS6250/6450	N/A
DHCP Snooping ISF ARP-Allow	OS6250/6450	N/A
802.1x Delay Learning	OS6250/6450	N/A

Feature Summary Table

New Feature Descriptions

Failover Supplicant

The option allows basic network access to trusted devices that failed in 802.1x supplicant authentication by subjecting the user through non-supplicant MAC authentication.

When 802.1x supplicant authentication fails, the supplicant users will be removed from 802.1x database and will be created in non-supplicant database, when the fail policy is set to MAC Authentication. The supplicant users will be classified based on non-supplicant policy. The MAC address of the failed supplicant user is sent to the RADIUS server for authentication, since the MAC address of the failed supplicant user is already present in the database.

On authentication, the user gets classified based on the returned VLAN or based on local authorization on non-supplicant policy.

Authentication Server Down Critical Voice VLAN for IP Phones

- If the authentication server is down when an IP phone is connected for the first time and the initial packet from the IP phone is not an LLDP packet, such as an EAP packet, the IP phone will not be seen as an IP phone and will not be classified according to the voice-policy UNP. In such case, the IP phone will be classified in the data-auth-server-down policy.

- After being classified, if the IP phone then sends an LLDP packet, the information will be passed on to check if that device is already classified based on data-auth-server down policy. If yes, then the client will be reauthenticated automatically (does not wait for the re-auth interval) and is moved to the voice-auth-server-down policy, if the server is still unreachable.

- During this re-authentication process, the device/authentication details in supplicant or non-supplicant table will be modified to initial state, but the old VPA association and the MAC address will not be deleted/modified until the server returns the result of the new authentication. If the returned/classified VLAN/UNP of new authentication is same as the old VLAN/UNP, then the device/authentication details in supplicant or non-supplicant table will be updated. If the returned/classified VLAN/UNP of new authentication is different from the old VLAN/UNP, then the VPA is updated for new VLAN. Additionally, the old MAC entry for that device will be removed and new entry will be added.

RADIUS Health Check

The RADIUS health check feature is introduced to poll the RADIUS server to check the server status (UP or DOWN). The feature allows for configuring the RADIUS server polling for a specific server and to set the desired polling interval between 20 to 3600 seconds. The username and password for the RADIUS polling can be set per server. Apart from polling the RADIUS server at the set interval, the RADIUS health check can also be used to determine the action to be taken when the RADIUS authentication server status is changed from down to up. When the RADIUS health check feature is enabled for a RADIUS sever, the RADIUS server is probed at the set interval and the operational status is updated. If the operational status is up, then it checks if the failover option is enabled for this server. If the failover option is enabled then it checks with the AAA server, if the server is configured for 802.1x or MAC Authentication. Upon receiving a message from AAA, it will check the users in the auth-server down state and trigger re-authentication for supplicant, non-supplicant or both.

DHCP Snooping ISF ARP-Allow

By default ARP packets are checked against binding entries and are allowed only when a valid binding entry for that client on the port is already present. By enabling DHCP Snooping IP source filter ARP-allow, ARP packets are not checked against the binding entries and are allowed to pass through transparently.
DHCP Snooping and ISF must be enabled before enabling this function.
On enabling this feature an entry is made in the ISF table hence the number of binding entry is reduced by one.
Currently this feature is not available in Web View.

802.1x Delay Learning

To avoid 802.1x clients from getting into the auth-server-down state by attempting an early authentication before the switch is rebooted, the delay learning interval can be set for 802.1x clients. This delays the 802.1x authentication process until the switch is rebooted. By default, the delay-learning interval is set to 120 seconds.

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	OS6250/6350/6450
DVMRP	OS6250/6350/6450
IS-IS	OS6250/6350/6450
Multicast Routing	OS6250/6350/6450
OSPF, OSPFv3	OS6250/6350/6450
PIM	OS6250/6350/6450
Traffic Anomaly Detection	OS6250/6350/6450
IPv6 Sec	OS6250/6350/6450
IP Tunnels (IPIP, GRE, IPv6)	OS6250/6350/6450
Server Load Balancing	OS6250/6350/6450
CPE Testhead	OS6350
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
Stacking	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

Software Feature	Unsupported CLI Commands
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.

PR	Description	Workaround
N/A	There are currently no known problems.	N/A

Fixed Problem Reports

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

PR	Description
214639	OS6450: Openflow: Satistics retrieved from switch showing in different order.
216480	SSH session getting ended when ssh test done from Nagios server.
216612	No OFPVID_PRSENT flag set, in VLAN_VID action field in statistics replying packets.
216645	OS6450 crashed with LicMgr, NISup, tCsCSMtask2 and tCS_PRB task suspended.
216967	OS6450-P10L port not coming up after hard reboot.
217079	Switch accepting only the first ACK packet and dropping the rest in daisy chain scenario
217750	Received packets are dropped when 2 instances of SAAs are running.
217769	Incorrect Mac movement display on OS6450.
217920	[TYPE1]Error Message is thrown while trying to view the "userPrivPasswordTable" file.
217943	ARP Packets dropped by IPSF after mac movement
218075	While sending CLI commands to DUT via script, multiple junk characters like ?\b? ?<bs>? are introducing
218565	High memory load during loop and security non-regression test in AOS 6.6.5.180
218786	PER3175 Requirement 9 asks is not working
218789	Issue with health-check status after a reboot
218791	QoS error message after applying NAC QOS guests rules
218913	Classification issue with MAB devices with health-check configured
218962	DHCP issue with cisco phone in auth server down mode
218967	show aaa server output not clear for health check
218970	VPA missing for VLAN 1 error message on linkagg
218972	[EDF NAC TEST] in 6.7.1 non supplicants still has connectivity issues every 30 secs
219039	logs missing when Radius server became UP again in health check context
219040	PER3194 randomly doesn't work
219049	[TYPE1] Match count is not getting incremented after takeover while setting LDAP application to Loop
219132	Issue with PER 3199 when switch radius status UP to DOWN
219305	Stack split occurred in stack of 8 OS6250 Resiliency set up on upgrade to build 61.R03 from 671.50.R
219425	Supplicants Cisco IP phone gets authenticated as non supplicants
219506	Dshell variable not set to 1 by default
219549	Non supplicants MAB device takes times to get authenticated in 6.7.1.67

219663	Users get authenticated in auth server policy when switch boot
219664	Users not re-authenticated as soon as radius server is seen up
219666	EAP failure packets received in auth serv down context
219750	After a reload no devices are able to get authenticated
219033	When a part of health check command is updated, server_oper_status, primary and backup status will not go down(or change) for short period of time.
218969	QoS error message observed after loading EDF customer configuration has been fixed as part of EDF ARP enhancement. The new CLI command introduced is: **ip helper dhcp-snooping ip-source-filter** *enable / disable.*
219147	In case of supplicant failover to non-supplicant, back up of VLAN id is taken to avoid NI out of resource.

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 configs, 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.

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: 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: esd.support@alcatel-lucent.com

Internet: Customers with Alcatel-Lucent service agreements may open cases 24 hours a day via Alcatel-Lucent's support web page at: service.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 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 6.7.1.R03 Upgrade Instructions

OmniSwitch Upgrade Overview

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

- OmniSwitch 6250 models being upgraded to AOS 6.7.1.R03.
- OmniSwitch 6450 models being upgraded to AOS 6.7.1.R03.
- OmniSwitch 6350 models being upgraded to AOS 6.7.1.R03.
-

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 6.7.1.R03.

Version Requirements - Upgrading to AOS Release 6.7.1.R03

Version Requirements to Upgrade to AOS Release 6.7.1.R03

	AOS	**Uboot/Miniboot**	**CPLD**
6250-24/P24/8M/24M	6.7.1.86.R03 GA	6.6.3.259.R01 (minimum) 6.6.4.158.R01 (optional)	12 (minimum) 14 (optional)
6450-10/10L/P10/P10L	6.7.1.86.R03 GA	6.6.3.259.R01	6
6450-24/P24/48/P48	6.7.1.86.R03 GA	6.6.3.259.R01	11
6450-U24	6.7.1.86.R03 GA	6.6.3.259.R01	6
6450-24L/P24L/48L/P48L	6.7.1.86.R03 GA	6.6.4.54.R01	11
6350-24/P24/48/P48	6.7.1.86.R03 GA	6.7.1.69.R01 6.7.1.103.R01	12

- 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.

- If an OS6250 is currently running the minimum versions listed above, then Uboot/Miniboot and CPLD upgrades are not required. However, CPLD 14 and Uboot/Miniboot 6.6.4.158.R01 fixed a known push button and LED issue (PR 176235). If you have an OS6250 that requires these fixes then upgrading both the Uboot/Miniboot and CPLD to the versions listed is required.
- If an OS6250 is already running AOS Release 6.6.3.R01 then the Uboot/Miniboot and CPLD versions should already be at the minimum versions listed above.
- If an OS6250 is running an AOS Release prior to 6.6.3.R01 the Uboot/Miniboot and CPLD will need to be upgraded. If an upgrade is required it is recommended to upgrade to the latest available versions.

Upgrading to AOS Release 6.7.1.R03

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 6.7.1.R03 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. (A reboot is required).
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 6.7.1.R03 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
   - AOS Files (6250/6450) – 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 a 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 fpga cmm

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 fpga ni 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 6.7.1.R03.

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       6.7.1.R03    15510736   Alcatel-Lucent Base Software
KFos.img         6.7.1.R03    2511585    Alcatel-Lucent OS
KFeni.img        6.7.1.R03    5083931    Alcatel-Lucent NI software
KFsecu.img       6.7.1.R03    597382     Alcatel-Lucent Security Management
```

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:                   OS6250-24,
  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.R01,
  POE SW Version :              n/a
```

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.

```
-> rm KFfpga.upgrade_kit
-> rm kfu-boot.bin
-> rm kfminiboot.bs
```

Appendix B: AOS 6.7.1.R03 Downgrade Instructions

OmniSwitch Downgrade Overview

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

- OmniSwitch 6250 models being downgraded from AOS 6.7.1.R03.
- OmniSwitch 6450 models being downgraded from AOS 6.7.1.R03.
  OmniSwitch 6350 models being downgraded from AOS 6.7.1.R03.

Note: The OmniSwitch 6350 requires a minimum of AOS Release 6.7.1.R01 and cannot be downgraded to any 6.6.X release.

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 6.7.1.R03. 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 – KFbase.img, KFeni.img, KFos.img, KFsecu.img
   - AOS Files (6350) – 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 downgrade the 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.R02   2511585   Alcatel-Lucent OS
KFeni.img        6.6.5.R02    5083931  Alcatel-Lucent NI software
KFsecu.img       6.6.5.R02     597382  Alcatel-Lucent Security Management
```