Release Notes

OmniSwitch 6350/6450

Release 6.7.2.R01

These release notes accompany release 6.7.2.R01 software for the OmniSwitch 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.

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

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: support.esd.alcatel-lucent.com.

AOS 6.7.2.R01 Prerequisites

New 6350 PoE Models

The following OS6350 models contain a new PoE controller. Due to this controller there is a minimum AOS requirement of 6.7.2.R01. The models can be identified by their part number as noted below. Additionally, a minimum software sticker will be present on the chassis.

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

System Requirements

Memory Requirements

The following are the requirements for the OmniSwitch 6350/6450 Series Release 6.7.2.R01:

- 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.R01 AOS software available from Service & Support.

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

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

OmniSwitch 6450-24/P24/48/P48

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

OmniSwitch 6450-U24

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

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

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

OmniSwitch 6450-P10S/U24S

Release	Uboot/Miniboot	CPLD
6.7.2.49.R01(GA)	6.6.5.41.R02	P10S - 4 U24S – 7

OmniSwitch 6450-M/X Models

Release	Uboot/Miniboot	CPLD
6.7.2.49.R01(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
6.7.2.49.R01(GA)	6.7.1.69.R01/6.7.1.103.R01 6.7.1.30.R04 (optional)	12 (minimum) 16 (optional)
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
6.7.2.49.R01(GA)	6.7.1.30.R04	4

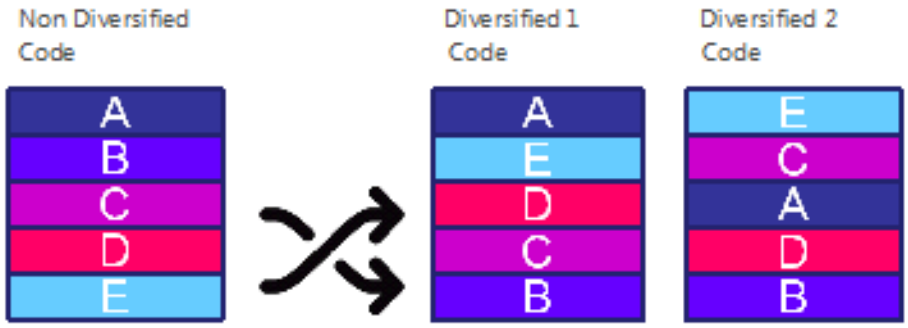
Note: Refer to the Upgrade Instructions section for upgrade instructions and additional information on Uboot/Miniboot and CPLD requirements.

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 5 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.R01	AOS 6.7.2.R01	AOS 6.7.2.R01

- X=Diversified image 1-5
- ALE will have 5 different diversified images per AOS release (R11 through R51)
- Our partner LGS will have 5 different diversified images per AOS release (L11 through L51)

6.7.2.R01 New Hardware Supported

The following OS6350 models contain a new PoE controller. Due to this controller change there is a minimum AOS requirement of 6.7.2.R01. The models can be identified by their part number as noted below. Additionally, a minimum software sticker will be present on the chassis.

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

6.7.2.R01 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
IP SAA Enhancement	OS6350/OS6450	N/A
TCM yellow traffic with DSCP parameter	OS6350/OS6450	N/A
Loopback detection	OS6350/OS6450	N/A
Introduction to statistical jitter	OS6350/OS6450	N/A
Loopback detection global / port level configuration	OS6350/OS6450	N/A
RSA key support in non-NIS mode	OS6350/OS6450	N/A
PoE enabled by default	OS6350/OS6450	N/A
Source learning hash chain-length enhancement	OS6350/OS6450	N/A
Source learning enable/disable in non-metro mode	OS6350/OS6450	N/A

Feature Summary Table

New Feature Descriptions

IP SAA Enhancement
In this enhancement for IP SAA, a software ARP refresh is implemented for ICMP packets with type SAA. An enhancement is also done to implement a stacking link flooding for IP SAA response, received on a different NI than the NI that has sent the IP SAA request

TCM yellow traffic with DSCP parameter
In this enhancement of configuring equal scheduling of yellow traffic, 802.1p and DSCP profile parameters for yellow frame can be configured, thus reducing the probability of packets being dropped. Two new CLI commands are introduced in this release, to forcefully set the priority value for each of parameters in TCAM table. Based on the profile parameter being configured, priority will be marked on the packet.

Loopback detection for 6350

Loopback detection is supported on OmniSwitch 6350.

Introduction to statistical jitter
Jitter is the variation in latency as measured in the variability over time of the packet latency across a network. A network with constant latency has no variation or jitter. In AOS, as per the old design, the inter-arrival jitter calculation is based on the Round Trip Time (RTT) difference between two successive packets. The enhanced mode is to calculate inter-arrival jitter based on the formula specified in RFC 1889.

Loopback detection global / port level configuration

Before the enhancement, the LBD frames are trapped only if the destination MAC address is matched. After enhancement instead of checking the destination MAC alone, both the Source MAC (switch's base MAC from which the LBD frame is generated) and destination MAC are verified. Thus the loop is detected once the LBD frame reaches the same switch from which it is originated.

RSA key support in non-ASA Enhanced mode

RSA key support is supported by default. It is no longer required to enable Authenticated Switch Access enhanced mode.

PoE enable by default

PoE is enabled by default. It is no longer required to enter the **'lanpower start'** command.

Source learning hash chain length enhancement

Hash chain length enhancement is to modify the depth of the hash chain length of FBD table (bucket size) used while writing MAC addresses in ASIC in the AOS platform. This feature enhancement is to change the hash chain length from default value (bucket size is 4) to 8 through a CLI command with mode options "default" and "extend" respectively. The hash chain length value is "default". The modification of hash chain length done at runtime is be effective only during boot-up and hence when this command is executed, a warning message is displayed on the console that the change will be effective only after the next reload / reboot of the switch or stack. This enhancement is applicable to both XOR and CRC modes and it is recommended to use the default bucket size unless there are collisions observed in the source learning table.

Source learning enable/disable in non-metro mode

Currently we have a limitation in AOS, that enabling / disabling of source-learning can be done only in Metro OmniSwitch units. This feature implementation now allows source-learning enable / disable for non-metro units also.

This provides the user an option to enable or disable source MAC learning on a specified port or linkagg. Any port, except those already activated with 'software' learning, can be set to source learning enabled / disabled by users. This feature is restricted to maximum of 48 ports (including Linkagg ports) across system.

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, OSPFv3	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

Software Feature	Unsupported CLI Commands
	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.

PR	Description	Workaround
217634	Up-link port is not coming up on an OS6450 when connected to OS6350 using a direct-attached (DAC) cable.	There is no known workaround at this time.

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.

When hot-swapping any element of the stack it must be replaced by the same model. For example an OS6450-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's support web page at: support.esd.alcatel-lucent.com.

Upon opening a case, customers will receive a case number and may review, update, or escalate support cases on-line. Please specify the severity level of the issue per the definitions below. For fastest resolution, please have 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.R01 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.R01.
- OmniSwitch 6350 models being upgraded to AOS 6.7.2.R01.

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.R01.

Version Requirements – Upgrading to AOS Release 6.7.2.R01

Version Requirements to Upgrade to AOS Release 6.7.2.R01			
	AOS	**Uboot/Miniboot**	**CPLD**
6450-10/10L/P10/P10L 6450-24/P24/48/P48 6450-U24 6450-24L/P24L/48L/P48L 6450-P10S 6450-U24S 6450-10M 6450-24X 6450- 24XM,24X,P24X,P48X,	6.7.2.49.R01 GA	6.6.3.259.R01 6.6.3.259.R01 6.6.3.259.R01 6.6.4.54.R01 6.6.5.41.R02 6.6.5.41.R02 6.7.1.54.R02 6.7.1.54.R02 6.7.1.54.R02	6 11 6 11 4 7 6 7 11
6350-24/P24/48/P48 6350-10/P10	6.7.2.49.R01 GA	6.7.1.69.R01/6.7.1.103.R01 (minimum) 6.7.1.30.R04 (optional) 6.7.1.30.R04	12 (minimum) 16 (optional) 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.R01

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.R01 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 6.7.2.R01 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 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 6.7.2.R01.

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.R01     15510736   Alcatel-Lucent Base Software
KFos.img        6.7.2.R01     2511585    Alcatel-Lucent OS
KFeni.img       6.7.2.R01     5083931    Alcatel-Lucent NI software
KFsecu.img      6.7.2.R01     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:                 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.
   -> rm KFfpga.upgrade_kit
   -> rm kfu-boot.bin
   -> rm kfminiboot.bs

Appendix B: AOS 6.7.2.R01 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.R01.
  OmniSwitch 6350 models being downgraded from AOS 6.7.2.R01.

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.R01. 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
```

Appendix C: Fixed Problem Reports

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

PR NUMBER	SUMMARY
155409	The "show ip dos statistics" output is not updated.
220514	Packet drop noticed in ip-ping SAA probes.
209640	Static dhcp binding entry over written to dynamic entry when client receives an ip dynamically on that port.
212485	LBD is not detecting loop.
213255	No SNMP trap sent when primary link of linkagg is disconnected.
218889	Lack of entry in show ip helper dhcp-snooping port.
221521	IPC congestion and IPC pool depletion noticed in unit-1 due to which unit-2 in a stack crashed.
221625	OS6450 – switch crashed after enabling static-querier.
222440	Switch crashed as the tNetTask was waiting for the semaphore held by udpRly.
222666	\\AAA\\802.1x\\ Display issue is notice in 802.1x feature after the takeover.
222834	sFlow sampling rate issue.
223039	All the ports went operationaly down when applying the QoS.
223492	OS6450 QoS issue with port range condition.
223528	\\SYSTEM\\MEMORY\\ Memory leak notice due to SSH session.
223530	Client authentication issue even when RADIUS server is reachable.
223544	ERROR: system is busy message when "show configuration snapshot" command is ran even without any active session doing a "show configuration snapshot".
223261	Static ARP entries are getting created in boot.cfg.
223658	EAP failure packet received when disconnect/reconnect supplicant IP Phone.
223673	OS6350 Username and password displayed in Boot-UP sequence.
223679	Port going down due to STP violation even through no bpdu is received on the port.
223711	High cpu due to webview task during captive portal re-direction in BYOD.
223838	No understandable logs generated from switch when a loop is detected.
223906	Multicast source got cleared in 5 seconds.
224320	High cpu due to tWirlpool task.
224322	SSL(88) Data: Warning in ssl_lib.c message seen in switch logs.
224500	OS6450 - 802.1x command is not possible with a specific UNP name “AuthFail”.
224518	Three EAP failures sent by the switch to supplicant IP phone.
224853	AOS 6.7.1.108.R04 DHCP Decline sent by switch during RCL contains garbage in servername field.
225264	OS6350 got crashed while setting temperature threshold in non-primary unit.