

Release Notes

OmniSwitch 6350/6450

Release 6.7.2.R08

These release notes accompany release 6.7.2.R08 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.

Table of Contents

Related Documentation	3
AOS 6.7.2.R08 Prerequisites	4
System Requirements	4
Memory Requirements	4
Miniboot and FPGA Requirements for Existing Hardware	4
6.7.2.R08 New Hardware Supported	6
6.7.2.R08 New Software Features and Enhancements	7
New Feature Descriptions	8
Unsupported Software Features	10
Unsupported CLI Commands	11
Open Problem Reports and Feature Exceptions	12
Redundancy/ Hot Swap	13
CMM (Primary Stack Module) and Power Redundancy Feature Exceptions	13
Stack Element Insert/Removal Exceptions	13
Hot Swap / Insert of 1G/10G Modules on OS6450	13
Technical Support	14
Appendix A: AOS 6.7.2.R08 Upgrade Instructions	15
OmniSwitch Upgrade Overview	15
Prerequisites	15
OmniSwitch Upgrade Requirements	15
Upgrading to AOS Release 6.7.2.R08	16
Summary of Upgrade Steps.....	16
Verifying the Upgrade.....	20
Remove the CPLD and Uboot/Miniboot Upgrade Files	21
Appendix B: AOS 6.7.2.R08 Downgrade Instructions	22
OmniSwitch Downgrade Overview	22
Prerequisites	22
OmniSwitch Downgrade Requirements	22
Summary of Downgrade Steps	22
Verifying the Downgrade	23
Appendix C: Fixed Problem Reports	24

Related Documentation

The release notes should be used in conjunction with the associated manuals as listed below. User manuals can be downloaded at: <https://businessportal.al-enterprise.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://businessportal.al-enterprise.com>

AOS 6.7.2.R08 Prerequisites

With the continuous goal of preserving the environment in addition to the AOS software being preloaded on the switch and available on the Business Portal, we have begun removing the software access card previously included in the switch ship kit. For additional information or in case of special assistance, please contact Service & Support.

System Requirements

Memory Requirements

The following are the requirements for the OmniSwitch6350/6450 Series Release 6.7.2.R08: 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.R08 AOS software available from Service & Support.

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

Release	Uboot/Miniboot	CPLD
6.7.2.122.R08(GA)	6.6.3.259.R01 ¹ 6.7.2.122.R08 (optional) ²	6

OmniSwitch 6450-24/P24/48/P48

Release	Uboot/Miniboot	CPLD
6.7.2.122.R08(GA)	6.6.3.259.R01 ¹ 6.7.2.122.R08 (optional) ²	11

OmniSwitch 6450-U24

Release	Uboot/Miniboot	CPLD
6.7.2.122.R08(GA)	6.6.3.259.R01 ¹ 6.7.2.122.R08 (optional) ²	6

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

Release	Uboot/Miniboot	CPLD
6.7.2.122.R08(GA)	6.6.4.54.R01 6.7.2.122.R08 (optional) ²	11

OmniSwitch 6450-P10S/U24S

Release	Uboot/Miniboot	CPLD
6.7.2.122.R08(GA)	6.6.5.41.R02 ¹ 6.7.2.122.R08 (optional) ²	P10S - 4 U24S - 7

OmniSwitch 6450-M/X Models

Release	Uboot/Miniboot	CPLD
6.7.2.122.R08(GA)	6.7.1.54.R02 6.7.2.122.R08 (optional) ²	10M - 6 24X/24XM/P24X/48X/P48X - 11 U24SXM/U24X - 7

OmniSwitch 6350-24/P24/48/P48

Release	Uboot/Miniboot	CPLD
6.7.2.122.R08(GA)	6.7.1.69.R01/6.7.1.103.R01 6.7.1.30.R04 (optional)* 6.7.2.122.R08 (optional) ²	12 (minimum) 16 (optional)*
*The optional 6.7.1.30.R04 uboot/miniboot and CPLD version 16 is only needed for stacking support. Standalone units can remain at the previous versions.		

OmniSwitch 6350-10/P10

Release	Uboot/Miniboot	CPLD
6.7.2.122.R08(GA)	6.7.1.30.R04 ¹ 6.7.2.122.R08 (optional) ²	4

1. OmniSwitch 6350/6450 models with part numbers beginning with "904" (i.e. 904101-90) are shipped with and require uboot/miniboot version 6.7.2.113.R05.

2. Uboot/Miniboot 6.7.2.122.R08 is only required for support of the Password Protected Uboot/miniboot Process feature.

Note: Refer to the [Upgrade Instructions](#) for uboot/miniboot upgrade instructions.

6.7.2.R08 New Hardware Supported

3FE46541AA -GPON SFP ONT

Platforms Supported: All OS6450 models and OS6350-10/P10.

6.7.2.R08 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
NIS Password Expiration Trap	6350/6450
NIS Config Mode	6350/6450
SNMP Objects for PoE	6350/6450
VM CPE Test-head Hardware Loopback Scaling	6450
MVLAN Support for VLAN Port Rules	6350/6450
OmniVista Features for 6.7.2.R08	6350/6450
Encrypted Usernames, Keys, Passwords and Community String	6350/6450
Password Protected Uboot/miniboot Process	6350/6450
Support for SHA-2: SHA-512, SHA-384 or SHA-25	6350/6450
DHCP Server & Snooping Simultaneous Support	6350/6450

FeatureSummary Table

New Feature Descriptions

Password Expiration Trap

Password expiration alert can be generated to inform the user of password expiration before the configured password expiry interval. The password expiration alert can be configured for individual user or all users at once. By default, the alert is set to one day before the password expiry period. The alert parameter can be used to configure the expiration alert.

Command Modified:

user password-expiration, allows to set the password expiration alert for the user.
show user, displays the password expiration notification alert set for the user.

NIS Config Mode

The OmniSwitch now has a new mode which is the Enhanced-config mode. This mode provides added switch configuration security. When the switch is running in Enhanced-config mode, only authorized users will be allowed to enter the configuration mode of the switch.

Command Modified:

user, allows to create the config mode user.
config, allows to enter the config mode with super user privileges.
aaa switch-access mode, allows to enable Enhanced-config mode in the switch.
show user, allows to view the enhanced-mode configuration privileges of the user.

SNMP Objects for PoE

OmniSwitches that are running near the threshold of PoE% utilization can now be viewed through OmniVista. All the information that are presented through the CLI is made available through SNMP table or objects. OV will collect this information periodically and highlight the switches that are near threshold of PoE% utilization. The following objects have been added:

- alaPethTotalMaxPower,
- alaPethTotalActualConsumed,
- alaPethTotalBudgetAvailable,
- alaPethTotalBudgetUsed,
- alaPethTotalPowerSupplyAvailable

VM CPE Test-head Hardware Loopback Scaling

Loopback test functionality is used to perform In-Service and Out-of-Service throughput testing in a live active network. The loopback tests can be used to validate the configured Service Level Agreements (SLAs) and QoS parameters that are associated with a service or a flow.

Prior to this release, Inward loopback test can be configured with only destination MAC and loopback port, but it was mandatory to configure destination MAC address, loopback port, and VLAN for outward loopback profile.

In this release, VLAN parameter is made optional for outward profile similar to inward profile.

More than one inward and outward profile can have the same loopback port, and a maximum number of inward profiles that can be configured is increased to 28 in addition to the 8 outward profiles.

Command Modified: loopback-test

MVLAN Support for VLAN Port Rules

In previous release, 802.1x supplicant/non-supplicant users were allowed to be mapped to a MVRP/GVRP VLAN in the following cases.

- The UNP to which user gets mapped is associated to a MVRP/GVRP VLAN
- The authentication policy to which the user gets associated is configured with a MVRP/GVRP VLAN
- Server returned VLAN is a MVRP/GVRP VLAN

In all the above cases, the MVRP/GVRP VLAN type would then be converted to UNPD-dynamic VLAN.

In this release, AOS switch will allow VLAN Group Mobility rules to be mapped to MVRP/GVRP/UNPD-dynamic VLAN. During run-time, switch will allow to assign Group Mobility rules for users learned as dynamic VLAN. If VLAN to be mapped is MVRP/GVRP VLAN, then switch would convert it to a UNPD-dynamic VLAN. If VLAN to be mapped is UNPD VLAN, then switch will accept the command without displaying any error message.

To keep the Group Mobility and UNP profile mapped to a UNPD-dynamic VLAN active after reboot, a new command is introduced, which controls the UNPD-dynamic VLAN creation associated to Group Mobility rules or UNP profile during reload scenario. This is a global status command that specifies whether UNPD-dynamic VLAN creation is allowed or not. This command will take effect only during boot up. Any runtime change to this command will be allowed, but will take effect only in subsequent reload.

New Command: `dynamic-vlan-configuration allow`

OmniVista Features for 6.7.2.R08

A security enhancement has been implemented whereby OmniSwitch can now verify hostname while connecting to the Activation Server. The host name of the certificate issuer is validated from an SSL client (OmniSwitch) when validating the certificate.

OmniSwitch can now handle an additional TCP attribute in AOS code to accurately fetch the policy from LDAP server and apply it in the switch. Earlier, OmniSwitch could handle only two TCP attributes in the policies pushed from the LDAP server. If the LDAP server pushes the policies with three TCP attributes, then the policies were ignored and not applied in the OmniSwitch.

During Tenant migration from TOV1 to TOV2, OmniSwitch has been implemented to identify the change in VPN IP, disconnect the VPN connection with old VPN IP and establish VPN connection with new VPN IP. After tenant migration from TOV2 to TOV1, OmniSwitch will show as UP in OmniVista(OV).

Encrypted Usernames, Keys, Passwords and Community String

The community string can be configured to be stored in encrypted format in the configuration file for security purposes. It can be manually configured to be encrypted in the configuration snapshot and the configuration file. The new **hash-key** option can be used to configure the encryption. This will not impact the **show community-map** command output. The output displays the community string in plain text.

Command Modified:

snmp community map, allows encrypting the community string.

Password Protected Uboot/minibootProcess

The OmniSwitch can be secured from unauthorized access to the miniboot of the switch. The switch can be configured for miniboot access password. Note that to use this feature a miniboot upgrade to 6.7.2.122.R08 is required.

New Command:

miniboot-password, allows to create or modify miniboot password

show miniboot-password status, allows to view the password protection status of miniboot.

Enforcing Stronger Hash Algorithm

The strict-hash mode will restrict the switch from using the weak hash algorithms such as the MD5. In strict-hash mode only the strong hash algorithms like SHA256, SHA384, and SHA512 can be used. The strict-hash mode can be enabled or disabled on the switch. The switch needs to be rebooted for the configuration settings to be applied. By default, "strict-hash" mode would be disabled. When strict-hash mode is enabled, a file named StrictHashMode.cfg is generated in "/flash/switch" directory of the switch. Strict-hash mode configuration is not saved in the boot.cfg, but the enable/disable status can be viewed using CLI command.

CLI:

```
system strict-hash {enable | disable}
```

```
show system strict-hash
```

NTP in Strict-hash Mode

The Network Time Protocol (NTP) now supports Secure Hash Algorithm-1 (SHA1) when the NTP server authentication is done in strict hash mode. In this mode only SHA1 hashing can authenticate NTP servers. SHA1 is a cryptographically stronger hash function than the MD5. The MD5 keys are untrusted in this mode. The NTP server definition must be configured with one of the trusted SHA1 keys present in the key file. No new CLI is introduced, the existing CLI is used to load the SHA1 key to the switch.

DHCP Server & Snooping Simultaneous Support

In previous releases, both DHCP server and DHCP snooping functionality was not supported in the same device as they were mutually exclusive. In this release, both DHCP server and DHCP snooping functionality is supported in the same device.

No new CLI.

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	OS6350/6450
DVMRP	OS6350/6450
IS-IS	OS6350/6450
Multicast Routing	OS6350/6450
OSPF	OS6350/6450
PIM	OS6350/6450
Traffic Anomaly Detection	OS6350/6450
IPv6 Sec	OS6350/6450
IP Tunnels (IPIP, GRE, IPv6)	OS6350/6450
Server Load Balancing	OS6350/6450
VLAN Stacking / Ethernet Services	OS6350
Ethernet/Link/Test OAM	OS6350
PPPoE	OS6350
ERP	OS6350
GVRP	OS6350
IPv4/ IPv6 RIP	OS6350
VRRP	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-3171	GPON SFP which acts an on ONT is not detected more than 1 minute after insertion.	It takes approximately 70-80 second for the GPON ONT SFP to be detected and come up.
CRAOS6X-3173	When GPON SFP connected port is toggled multiple times, error messages may be displayed.	It is recommened to do a GPON SFP hot swap or its port toggle with time interval of atleast 2.5 minutes in order to avoid these errors.
CRAOS6X-3436	In 6350-P10 device, when the cable is removed from GPON SFP, LED status remains green for approximately 5 seconds.	After 5 seconds, green LED status should turn off.

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, 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 Enterprise support web page at: <https://businessportal.al-enterprise.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.R08 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.R08.
 OmniSwitch 6350 models being upgraded to AOS 6.7.2.R08.

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.

NOTE: 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 this AOS Release.

Version Requirements - Upgrading to AOS Release 6.7.2.R08

Version Requirements to Upgrade to AOS Release 6.7.2.122.R08 (GA)				
	Minimum Uboot/Miniboot	Optional Uboot/Miniboot	Minimum CPLD	Optional CPLD
6450-10/10L/P10/P10L	6.6.3.259.R01	6.7.2.122.R08*	6	6
6450-24/P24/48/P48	6.6.3.259.R01		11	11
6450-U24	6.6.3.259.R01		6	6
6450-24L/P24L/48L/P48L	6.6.4.54.R01		11	11
6450-P10S	6.6.5.41.R02		4	4
6450-U24S	6.6.5.41.R02		7	7
6450-10M	6.7.1.54.R02		6	6
6450-U24X/SXM	6.7.1.54.R02		7	7
6450- 24XM,24X,P24X,P48X	6.7.1.54.R02		11	11
6350-24/P24/48/P48	6.7.1.69.R01/6.7.1.103.R01		6.7.2.122.R08*	12
6350-10/P10	671.30.R04	4		4

* 6.7.2.122.R08 is only required for the support of the Password Protected Uboot/miniboot Process feature.

Upgrading to AOS Release 6.7.2.R08

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.R08 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.R08 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(OS6450) - kfu-boot.bin, kfminiboot.bs (optional)
 - Uboot/Miniboot Files(OS6350) -kf3miniboot.bs ,kf3u-boot-p10.bin, kf3u-boot.bin (optional)
 - AOS Files (OS6450) - KFbase.img, KFeni.img, KFos.img, KFsecu.img
 - AOS Files (OS6350) - 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 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.R08.

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 an example of a successful image file upgrade.

```
-> show microcode
-----+-----+-----+-----+
Package           Release           Size             Description
-----+-----+-----+-----+
KFbase.img        6.7.2.122.R08    18130755        Alcatel-Lucent Enterprise Base Softw
KFos.img          6.7.2.122.R08    3562484         Alcatel-Lucent Enterprise OS
KFeni.img         6.7.2.122.R08    6152493         Alcatel-Lucent Enterprise NI software
KFsecu.img        6.7.2.122.R08    648189          Alcatel-Lucent Enterprise Security M
KFdiag.img        6.7.2.122.R08    2411898         Alcatel-Lucent Enterprise Diagnostic
```

Note:The *diag.img* file (i.e. *KFdiag.img*) is for switch diagnostics only and is not required as part of an AOS upgrade, it can be safely removed from the switch. However, some switches may ship from the factory with a diagnostics image file so it has been included in the example above. If using a software upgrade package from Service & Support the diagnostics image file will not be included.

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   : 6.7.2.122.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, for example.

```
->rmKFfpga.upgrade_kit  
->rmkfu-boot.bin  
->rm kfminiboot.bs
```

Appendix B: AOS 6.7.2.R08 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.R08.
- OmniSwitch 6350 models being downgraded from AOS 6.7.2.R08.

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.R08. 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 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:
 -> `copy working certified`

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	6.7.2.R07	15510736	Alcatel-Lucent Base Software
KFos.img	6.7.2.R07	22511585	Alcatel-Lucent OS
KFeni.img	6.7.2.R07	25083931	Alcatel-Lucent NI software
KFsecu.img	6.7.2.R07	597382	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	Description
Case: 00414470 00483803 CRAOS6X-2704	<p>Summary: OS6450 (Stack of 5 units) High CPU due to Ipni task.</p> <p>Explanation: 100% CPU spike noticed in the primary unit. This issue was seen due to stale entry in the socket list. Also, the stale entry has received information, which makes IPNI task to wait in a continuous loop and triggered CPU spike.</p> <p> Click for Additional Information</p>
Case: 00411547 00444117 CRAOS6X-2773	<p>Summary: OS6450 - IP Phones disconnection and LLDP errors on those ports.</p> <p>Explanation: LLDP frames tagged with VLAN ID 4095. ALE IP phones, never sends LLDP frames with VLAN ID 4095 tagged. Code changes done to avoid LLDP errors in swlogs</p> <p>This happens in the following scenarios:</p> <ul style="list-style-type: none"> • When the phone connected to the port goes for reboot, • When we apply "802.1x initialize <slot/port>" on the port • When the phone re-authenticates <p> Click for Additional Information</p>
Case: 00421719 CRAOS6X-2780	<p>Summary: OS6450: Switch crashed generating pmd due to suspended task sshd_ct0.</p> <p>Explanation: Switch had crashed with the suspended task "sshd_ct0". SSH session was created few seconds before the switch crash. From the tt of sshd_ct0, it shows that ssh is waiting for the authentication from tacacs server. sshd_ct0 task has taken the ipc global semaphore and in suspended state. tCsCSMtask is in pending state, it did not send heart beat message to tCsCSMtask2. As tCsCSMtask2 did not receive heartbeat message for 45 seconds, it rebooted the switch with PMD. Crash occurred while accessing null pointer in select (zcselect) call API. Defensive fix mechanism is added to handle the observed issue.</p> <p> Click for Additional Information</p>
Case: 00411610 CRAOS6X-2807	<p>Summary: 802.1x authentication error (No EAP session matching state) during re-authentication.</p> <p>Explanation: Randomly, 802.1x authentication fails during re-authentication with reason code 38 No EAP session matching state. In issue state, switch is sending several 0 in the state attribute.</p> <p> Click for Additional Information</p>

Case: 00424491 CRAOS6X-2858	Summary: OS6450 after authentication there is not access to the Management IP. Explanation: UNP policies are mapped to a same VLAN, when the user authentication becomes successful, the information is not forwarded to the Source learning table; hence the MBI (Mac Block Index) is mapped to the first policy in hardware. 🔒 Click for Additional Information
Case: 00433962 CRAOS6X-2907	Summary: OS6450 - Alert and alarm level switch logs during bootup. Explanation: During switch boot up, few logs are seen in ALERT and ALARM level of severity which seems incorrect. MON DEC 29 01:47:18 2003 CSM-CHASSIS alert == CSM == P54 =====> This CMM is Role: 1 MON DEC 29 01:47:25 2003 CSM-CHASSIS alert == CSM == loading config_manager.lnk from /flash/working/KFbase.img MON DEC 29 01:48:02 2003 VLAN alarm VMN: Conn Ctrl frame mode 46 🔒 Click for Additional Information
Case: 00435008 CRAOS6X-2920	Summary: OS6450-P48 not shutting down after reaching danger threshold Explanation: Switch shutdown should be done by hardware during danger temperature condition. Code changes are done to shut down the NI after danger threshold temperature is reached, if shutdown is not initiated by the hardware. 🔒 Click for Additional Information
Case: 00434970 CRAOS6X-2932	Summary: A synchronized stack is no longer synchronized after a reboot (by command or power failure), show running-directory : Running Configuration : NOT SYNCHRONIZED, Stacks Reload On Takeover: ALL NIs (CMM Only Config OUT-OF-SYNC) Explanation: The running configuration goes out-of-sync due to NTP configuration. When NTP server is configured with a host-name instead of an IP address, the configuration is applied only after boot-up completion as it requires DNS resolution. At the end of this process, an out-of-sync message is sent. In general, whenever a configuration is applied after a reboot, it is coming from a CLI command or any other interface and not from the boot.cfg file. 🔒 Click for Additional Information
Case: 00439464 CRAOS6X-2944	Summary: saa RTT 300 ms delay limit is not working. Explanation: RTT being greater than twice the value of max RTT of that ping session. Max RTT value gets updated comparing it with the previous max-value of RTT during the session.Code

	<p>changes has been done to correct the RTT timer.</p> <p> Click for Additional Information</p>
<p>Case: 00438512 CRAOS6X-2951</p>	<p>Summary: OV2500 no notification after upgrade to version 4.4R02.</p> <p>Explanation: Error message confirmed as a bug and fixed.</p> <p> Click for Additional Information</p>
<p>Case: 00458688 00452687 CRAOS6X-2977</p>	<p>Summary: All LLDP links not showing up in Omni vista 2500 map.</p> <p>Explanation: After upgrading OS6450 switches from 6.6.5.R02 to 6.7.2.195.R04 and reloading, some of the switches are sending wrong MAC address in LLDP frames sent out.</p> <p>Due to this issue, LLDP link will not be shown in NMS for the switch.</p> <p>While looking at the LLDP neighbour switch, chassis MAC would be updated as follows with a random string such as "0f:f4:c8:00:00:00".</p> <p> Click for Additional Information</p>
<p>Case: 00441743 CRAOS6X-3023</p>	<p>Summary: OS6450 Reauthentication timer increase from 5min, when authentication done through TACACS+ server.</p> <p>Explanation: OS6450 switch is successfully authenticated by TACACS+ protocol configured in CPPM server; however, it reauthenticates for every 5 mins. Hence refresh timer value for reauthentication interval has been increased through debug variable.</p> <p> Click for Additional Information</p>
<p>Case: 00446219 CRAOS6X-3090</p>	<p>Summary: Mobile tagging for a VLAN is not deleted for a port after link disconnection, when using "vlan port <slot/port> default vlan restore disable" command.</p> <p>Explanation: By default, VLAN restore is enabled on mobile ports, meaning VLAN assignments are dropped when port traffic ages out. To retain VLAN assignment when port traffic ages out, use: vlan port slot/port default vlan restore disable. However, mobile tagging for a VLAN is not deleted for a port after link disconnection or if link is disabled by command. The consequence is that the client device connected to the port is receiving Router Advertisement (RA) from all the retained VLANs & installing routes to different gateways.</p> <p> Click for Additional Information</p>

Case: 00461634 CRAOS6X-3143	Summary: OS6450: RCA for PMD generation. Explanation: OS6450 switch crashed and generated PMD due to the suspended task "NTPDaemon". 🔒 Click for Additional Information
Case: 00467692 CRAOS6X-3217	Summary: OS6450-P24 rebooted with PMD and saved only half of the config. Explanation: RADIUS CLI task had suspended due to data translation exception. Corrupted configuration file shows no configuration was available starting from 802.1x. Possible cause for the crash in this case is due to insufficient space in destination buffer space while doing memory copy. Code changes done to avoid the crash of RADIUS task. 🔒 Click for Additional Information
Case: 00468531 CRAOS6X-3222	Summary: Inconsistent behavior of RESERVED linkagg port with respect to LLDP frames. Explanation: RESERVED linkagg ports are not supposed to send any frames out. LLDP entries are seen for both ATTACHED and RESERVED ports causing inconsistent neighbor ship links in NMS. 🔒 Click for Additional Information
Case: 00478878 00480273 00470331 CRAOS6X-3250	Summary: OS6350-P24 switch rebooted with PMD after enabling 802.1x on its ports. Explanation: From Crash.pmd, we could observe that the switch crashed due to ONEX task. Once switch has performed authentication of AP and successfully classified AP into vlan it will mark the port as AP port. Further client traffic from the AP would be processed by ONEX and inform Source-learning module to program MAC in hardware. Switch has crashed while sending message to Source-Learning. 🔒 Click for Additional Information
Case: 00479690 CRAOS6X-3359	Summary: OS6450-P10 stack: Secondary unit port part of a static linkagg between OS6450 stack and OS6900 VC not joining the lag after switch reload. Explanation: When used SFP (1 Gig) to form stacking, with non-redundant stacking cable, issue was seen. In case, SFP+ (SFP-10G-SR) is used to stack the switches, no issue seen even with non-redundant stacking connectivity. Hence the issue was with SFP (1 Gig) used as stacking cable, however having redundant Stacking (SFP (1 Gig)), no issue seen as port part of unit-2 is joining the linkagg. 🔒 Click for Additional Information
Case 00483394 CRAOS6X-3459	Summary: OS6450 switch connectivity issue

	<p>Explanation: Tunnel Termination Interface look up is used to identify interface and classify according to its L2 or L3 table. TTI lookup will be enabled for mobile ports. When a device connected on a mobile port is classified based on GM rules, an entry would be programmed in TTI. This would be done for untagged packets. Hence, for subsequent packets vlan would be obtained from TTI entry itself. There is no need to trap the packets to CPU for vlan classification. In issue state TTI entry has been removed. This causes untagged traffic to be trapped to CPU for vlan classification, causing arp/ping failed.</p> <p> Click for Additional Information</p>
<p>Case: 00464072 00472135 00455864 <i>CRAOS6X-3276</i> <i>CRAOS6X-3101</i></p>	<p>Summary: OS6450 switch auto-reboots due to IPC memory depletion.</p> <p>Explanation: Swlog enhanced to generate log/trap as IPC memory pool depletes and crosses threshold of 70%.</p> <p> Click for Additional Information</p>
<ul style="list-style-type: none"> • Lock Icon () - Indicates credentials required to log into the Business Portal website. • Click on the associated URL for more information. 	