Release Notes

OmniSwitch 6350/6450

Release 6.7.2.R07

These release notes accompany release 6.7.2.R07 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.

Table of Contents

Related Documentation

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

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

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

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

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

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

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

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

AOS 6.7.2.R07 Prerequisites

N/A

System Requirements

Memory Requirements

The following are the requirements for the OmniSwitch 6350/6450 Series Release 6.7.2.R07:

- 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.R07 AOS software available from Service & Support.

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

Release	Uboot/Miniboot	CPLD
6.7.2.99.R07(GA)	6.6.3.259.R01	6

OmniSwitch 6450-24/P24/48/P48

Release	Uboot/Miniboot	CPLD
6.7.2.99.R07(GA)	6.6.3.259.R01	11

OmniSwitch 6450-U24

Release	Uboot/Miniboot	CPLD
6.7.2.99.R07(GA)	6.6.3.259.R01	6

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

Release	Uboot/Miniboot	CPLD
6.7.2.99.R07(GA)	6.6.4.54.R01	11

OmniSwitch 6450-P10S/U24S

Release	Uboot/Miniboot	CPLD
6.7.2.99.R07(GA)	6.6.5.41.R02	P10S - 4 U24S – 7

OmniSwitch 6450-M/X Models

Release	Uboot/Miniboot	CPLD
6.7.2.99.R07(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
6.7.2.99.R07(GA)	6.7.1.69.R01/6.7.1.103.R01 6.7.1.30.R04 (optional)	12 (minimum) 16 (optional)

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

OmniSwitch 6350-10/P10

Release	Uboot/Miniboot	CPLD
6.7.2.99.R07(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.

6.7.2.R07 New Hardware Supported

SFP-GIG-BX-U/D
Support added for OmniSwitch 6350 uplinks.

SFP-GIG-EZX Transceiver
Support added for OmniSwitch 6450.

6.7.2.R07 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
NIS Requirements - 802.1x 2010	6350/6450	N/A
Throughput calculation on “CPE TEST HEAD” change required	6350/6450	N/A
CPE Testhead - Support for both double tagged (preserve) or single tagged (translate) environments	6350/6450	N/A
Support for setting fixed suffix to session prompt	6350/6450	N/A
Enhance AOS upgrade information to user	6350/6450	N/A
Internal Loop mechanism in for remote port mirroring	6350/6450	N/A
Configuring Layer 3 Learning on 802.1x Port	6350/6450	N/A
Fix security bypass vulnerability 00383733 with connected Stellar AP	6350/6450	N/A
Incorporate cloud CA chain also to Master CA chain	6350/6450	N/A
certifyDownloadedConfigFile command handling change	6350/6450	N/A
OS6350 Series BSMI Certifications: 4 Models: OS6350-24/-P24/-48/-P48	6350/6450	N/A
Add a DHCP Vendor Specific Option to specify Custom Activation Port	6350/6450	N/A
Support of being able to create UNP mapped to VLANs which had been learned as dynamic via MVRP	6350/6450	N/A
QoS Profile for HD VOD environment	6350/6450	N/A
OVC call-home causing excessive CPU spikes/alerts	6350/6450	N/A

FeatureSummaryTable

New Feature Descriptions

NIS Requirements - 802.1x 2010
This feature enables or disables the EAP version in header to 3 (corresponds to 2010) globally for all the 802.1x ports on the switch. By default, EAP version is 1 (corresponds to 2001).
With this command, 8021x version field of EAP packet sent from the switch can be modified. EAP header version is modified for the following EAP packets:

- EAP-Request
- EAP-Success
- EAP-Fail
- EAP-Challenge-Request

Throughput calculation on "CPE TEST HEAD" change required
This feature enables more accurate Throughput calculation.
Initially the throughput was calculated as "(packets received until recent interval * packet size) / test duration". That is now changed to "(Packet size * packets received until most recent interval)/duration until the most recent interval". This provides more accurate Throughput calculation.
Note: Throughput is calculated only when "remote-fetch-stats" option is used for unidirectional tests.

CPE Test head - Support for both double tagged (preserve) or single tagged (translate) environments
In earlier design, when CPE test was started, generator sends a "remote_start_request" frame which is single tagged with SVLAN ID and expects a response back from analyzer to start the test. In certain configuration of transit switches between generator and analyzer, the request was received as an untagged frame on analyzer. Analyzer fails to process the untagged frame and response was not sent.

This issue is fixed with changes done to modify "remote_start_request" and "remote_start_response" frames similar to the test frames being generated. So based on the mode, these frames would either be double tagged for preserve mode (i.e. SVLAN + CVLAN) or single tagged for translate mode (i.e. innner CVLAN tag). This also applies when L2-SAA is started along with testOAM session.

Support for setting fixed suffix to session prompt
A predefined suffix can be set for the session prompt, so that it always appears in the CLI session. When set, will be added to the end of session prompt. The new suffix prompt takes effect after logging into a new session.

Enhance AOS upgrade information to user
When upgrade is initiated using 'reload working ...' command, there will be a message confirming new software details along with a prompt to user for activating the software. During completion of the reboot that happens as part of the upgrade process, a message is printed in the boot log mentioning the directory from which the switch booted up along with AOS software change info. In addition to above, the 'show system update-time' CLI will show the time and software version to which the switch was last updated.

Internal Loop mechanism for remote port mirroring
Currently, with RPMIR implementation, the mirrored traffic from the source port could only be sent to one destination. To enable support of multiple destinations for a source port, loopback mechanism is introduced in this release.
By configuring loopback, the mirrored traffic sent to the destination port of RPMIR will be looped and sent to the same port as ingress packets. These packets will be tagged with the RPMIR-VLAN.

Configuring Layer 3 Learning on 802.1x Port
Currently, 8021x clients are authenticated and moved to a specific VLAN. But there is no support to reclassify an authenticated user based on the IP address which is assigned to clients. This can be achieved with Layer 3 force learning.

Allow MVRP/GVRP VLANs for UNP profiles and all 802.1x clients.
This enhancement is to allow UNP-Profile mapping to MVRP. Earlier MVRP/GVRP VLANs were allowed for AP and its clients 802.1x classification. Now the same is allowed for all 802.1x users and its mapping to UNP profile.

Support of Global and Per port AP mode to enhance security
When an end device is detected as AP the switch marks the port on which the end device is connected as AP port. When the port is marked as AP port, the authentication for the clients connected on the AP port is bypassed. By this anyone connected through the AP port can gain access to the network without any authentication.
To control the authentication of end device on 802.1x port, A new parameter AP-mode enabled. The AP-mode can be enabled or disabled on the switch globally or on per port basis.
When AP-mode is enabled, switch detects end device as AP and it marks the port as AP port. The authentication of clients connected through that AP port is bypassed and trust-tag would be enabled internally.
When AP-mode is disabled, even the end device is a AP switch will treat it as a normal client and authentication for clients connected through the AP would be done by the switch.

OV Cirrus - Implementation of ALE CA chain to the pre-loaded certificate chain on device.
OmniSwitch has been enhanced to support connectivity to 'non-standard' Activation Server, which will have its certificate issued by ALE CA instead of a public CA. With the incorporation of ALE CA chain file, disconnection of AOS devices during HTTPS connection establishment with Activation Server at TLS verification is avoided.

OV Cirrus - Troubleshooting Command Enhancement
When action command "*certifyDownloadedConfigFile*" is given through OV Cirrus for troubleshooting, OmniSwitch does an operation equivalent to Certify command ("copy working certified" CLI command) thereby copying the configuration files along with the software images from the "Working" directory to "Certified" directory.

OV Cirrus - Enhancement to specify a 'Activation Server Port Number'
This enhancement is to add a new DHCP VSO (Activation Server Port Number) to allow a customer to specify activation server with different Port Number in "Vendor specific string'. The switch uses this Port as destination port in the Call-home request message to the Activation server.

This provides additional security of validating the tenant devices based on whether the transfer occurs on valid Activation Server Port.

OV Cirrus performance enhancements and Health-monitoring enhancements.
An enhancement has been implemented in OmniSwitch to avoid call-home causing excessive CPU spikes and alerts to NMS.

An enhancement has been implemented to avoid excessive delay on the device during VPN establishment and reporting of VPN establishment status to Activation Server.

Timeout is increased to 300 seconds to facilitate successful HTTPS connection establishment to various OV Cirrus servers (like Activation Server, CDN server etc.)

The other enhancements are:

- Default health-monitoring sampling interval is changed from 5 seconds to 10 seconds.
- Health monitoring threshold-crossing traps (trap 15,16,17) will be raised based on 1-minute average utilization crossing the defined threshold. So far, this was based on instant (sample) value crossing the threshold.

QoS Profile for HD VOD environment
In IPTV Environment , streaming videos were pixilated for HD/UHD traffic when passed through OmniSwitch. This was due to the sudden burst of traffic happening inside the switch which exceeds the available buffer allocated for the same.
An enhancement has been implemented to create a profile which handles such peak rate traffic and encapsulates the new thresholds for the burst in traffic.

Unsupported Software Features

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

Feature	Platform
BGP	6350/6450
DVMRP	6350/6450
IS-IS	6350/6450
Multicast Routing	6350/6450
OSPF	6350/6450
PIM	6350/6450
Traffic Anomaly Detection	6350/6450
IPv6 Sec	6350/6450
IP Tunnels (IPIP, GRE, IPv6)	6350/6450
Server Load Balancing	6350/6450
VLAN Stacking / Ethernet Services	OS6350
Ethernet/Link/Test OAM	OS6350
PPPoE	OS6350
ERP	OS6350
GVRP	OS6350
IPv4/ IPv6 RIP	OS6350
VRRP	OS6350
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-2171	Unicast traffic drop seen for some time when linkagg ports were admin up (pending to idle) in a static linkagg or dynamic linkagg of 2 based ERP ring	The issue may be noticed in some setups that has ERP ring formed using across NI LAG. This is seen due the timing of the internal messages sent by the switch when WTR timer completes. Traffic normally recovers after few minutes when the issue is seen. Setting a custom tick value for an Alcatel debug parameter can prevent this issue from happening.

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://businessportal2.alcatel-lucent.com

Upon opening a case, customers will receive a case number and may review, update, or escalate support cases on-line. Please specify the severity level of the issue per the definitions below. For fastest resolution, please have telnet or dial-in access, hardware configuration—module type and revision by slot, software revision, and configuration file available for each switch.

Severity 1- Production network is down resulting in critical impact on business—no workaround available.
Severity 2- Segment or Ring is down or intermittent loss of connectivity across network.
Severity 3- Network performance is slow or impaired—no loss of connectivity or data.
Severity 4- Information or assistance on product feature, functionality, configuration, or installation.

Appendix A: AOS 6.7.2.R07 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.R07.
- OmniSwitch 6350 models being upgraded to AOS 6.7.2.R07.

See also Specific Upgrade Instructions For OS6350 for more upgrade instructions for OmniSwitch6350.

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 AOS Release 6.7.2.R07.

Version Requirements – Upgrading to AOS Release 6.7.2.R07

Version Requirements to Upgrade to AOS Release 6.7.2.R07			
	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,	6.7.2.99.R07(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	6.7.2.99.R07(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.R07

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.R07 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.

Specific Upgrade Instructions for OS6350

This section documents the specific upgrade requirements for an OmniSwitch 6350.

Dynamic Rules supported in 6.7.2.R04 is 193 whereas in 6.7.2.R07, it is 173. So when the switches are upgraded from pre 6.7.2.R07 (6.7.2.R01/2/3/4) to 6.7.2.R07, it is recommended to check the “show qos slice ingress” command and confirm the Dynamic Rules usage. The Dynamic Rules usage should not be more than 173 rules.

Note that If the Dynamic usage rule is more than 173 rules, the behaviour of the OmniSwitch post upgrade is not as expected.

For a smooth upgrade to 6.7.2.R07 in OS6350, the user has to manually confirm prior to upgrade, that existing QoS configuration / TCAM entries usage is not more than 173 rules.

Upgrading - Step 1. FTP the 6.7.2.R07 Files to the Switch

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

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

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

Upgrading - Step 2. Upgrade Uboot/Miniboot and AOS

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

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

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

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

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

Upgrading - Step 3. Upgrade the CPLD

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

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

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

Single Switch Procedure

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

The switch will upgrade the CPLD and reboot.

Stack Procedure

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

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

The stack will upgrade the CPLD and reboot.

Proceed to Verifying the Upgrade to verify the upgrade procedure.

Verifying the Upgrade

The following examples show what the code versions should be after upgrading to AOS Release 6.7.2.R07.

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.img6.7.2.112.R07   18130755 Alcatel-Lucent Enterprise Base Softw
KFos.img6.7.2.112.R073562484 Alcatel-Lucent Enterprise OS
KFeni.img6.7.2.112.R07 6152493 Alcatel-Lucent Enterprise NI software
KFsecu.img6.7.2.112.R07648189 Alcatel-Lucent Enterprise Security M
KFdiag.img6.7.2.112.R07    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            : 6.6.4.158.R01,
Product ID Register         : 05
Hardware Revision Register  : 30
FPGA Revision Register      : 014
```

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

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

```
ASIC - Physical 1:          MV88F6281 Rev 2,
FPGA - Physical 1:          0014/00,
UBOOT Version :             n/a,
UBOOT-miniboot Version :    6.6.4.158.
```

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

Remove the CPLD and Uboot/Miniboot Upgrade Files

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

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

Appendix B: AOS 6.7.2.R07 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.R07.
- OmniSwitch 6350 models being downgraded from AOS 6.7.2.R07.

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

  Note: The OmniSwitch PoE model switch the new PoE controller require a minimum of AOS Release 6.7.2.R01 and cannot be downgraded to any earlier 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.R07. Previous AOS releases are compatible with the Uboot/Miniboot and CPLD versions shipping from the factory.

Summary of Downgrade Steps

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

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

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

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

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

3. Proceed to Step 2.

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

Downgrading - Step 2. Downgrade the AOS

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

1. Reboot the switch. **This will downgrade the 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      6.6.5.R02   15510736  Alcatel-Lucent Base Software
KFos.img        6.6.5.R022511585  Alcatel-Lucent OS
KFeni.img       6.6.5.R025083931 Alcatel-Lucent NI software
KFsecu.img      6.6.5.R02597382 Alcatel-Lucent Security Management
```

Appendix C: Fixed Problem Reports

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

CR/PR NUMBER	Description
Case: 00373018 00309967 *CRAOS6X-2111*	**Summary:** 802.1x supplicant PCs are classified in wrong policy after successful authentication **Explanation**: In old releases, after teh client reboot, there was a logic to check if the client is already classified as either supplicant or non-supplicant. If client is classified as non-supplicant then the switch will flush the MAC address from both non-supplicant table and hardware mac table. In the later releases, the logic to check if the client is already classified as non-supplicant is missing and confirmed as software bug. Click for Additional Information
Case: 00366850 *CRAOS6X-2014*	**Summary:** Supplicant users connected behind Phones were moving to Guest role after re-authentication. **Explanation**: The reason for the client failing while re-auth was due to delay from PC to respond to RADIUS request packet. The RADIUS Challenge request from server has been forwarded by Switch to PC, however no response in 30 sec, hence switch tried sending Challenge Req for the second time. The client took around 10-15 sec to respond for challenge req and also responding for both the challenge requests, for which switch was mismatching the response IDs which it needs to forward to RADIUS server. Click for Additional Information
Case: 00374253 *CRAOS6X-2105*	**Summary:** OS6450 HD video is pixilated due to packet drops. **Explanation**: The VOD unicast traffic is bursty and High Definition at a 25 Frames per second which a 100 MB port may not be able to handle.The packet drops are seen interface internal queue. The issue is seen every time a HD VOD is streamed. As a workaround, disabling the Tail drop the issue is resolved. Click for Additional Information
Case: 00383733 *CRAOS6X-2189*	**Summary:** Third party AP's connected to an 802.1x port with port mobility is detected as Stellar AP. **Explanation**: Stellar AP classification is currently done based on the capabilities on the LLDP packet. If the capability is marked as WLAN access point, classify the device as Stellar AP and enable trust tagging on this port. Classified all devices as Stellar AP's and fixed to identify Stellar AP's based on the ALE preparatory TLV's solving the issue of any third party AP being identified as Stellar AP .New CLI commands introduced to disable AP mode. Click for Additional Information

Case: **00393783** **00399319** **00394233** *CRAOS6X-2028*	**Summary:** pethPsePortOnOffNotification traps generated by 6450 switch. **Explanation**: This trap is normally generated when the port power status flaps between Up and Down. Fix made to generate traps only when the link flap seen. 🔒 Click for Additional Information
Case: **00402849** *CRAOS6X-2454*	**Summary:** User login failure except default user after upgrade. **Explanation**: The users are stored in UserTable7 in later releases instead of User Table 5. UserTable5 is not copied to UserTable7, only works with the default user "admin" with default password. 🔒 Click for Additional Information
Case: **00401554** *CRAOS6X-2458*	**Summary:** OS6450 read privilege issue not working. **Explanation**: User needs to authenticate in windows server and they will get privilege for read access. There is no issues with the authentication. The issue with the privilege, once the user is authenticated with Read privilege. The user is able to get the outputs for some commands not for all. Fixed to allow the users are able to get the output for all the show commands with Read and write privileges. 🔒 Click for Additional Information
Case: **00395255** *CRAOS6X-2475*	**Summary:** Authentication Issue due to corrupted NAS identifier. **Explanation**: OS6450 while sending the additional Radius attribute “NAS-Identifier” in Access-Request packet to server, the server was not accepting this request due to the NAS-Identifier field containing * (star). Fixed to avoid corruption of NAS Identifier. 🔒 Click for Additional Information
Case: **00418174** **00398480** *CRAOS6X-2379*	**Summary:** Momentary high CPU is noticed during on-boarding and during every Call Home request (3 hours once) in 6350 switches. **Explanation**: Momentary high CPU is noticed during on-boarding and during every Call Home request in 6350-P10 switches running 672.R06. Fix provided to avoid the traps and high CPU is a momentary CPU with no impact to production. 🔒 Click for Additional Information
Case: **00376856** *CRAOS6X-2142*	**Summary:** OS6450-SNMP community string missed after switch upgrade. **Explanation**: Due to the smaller SNMP community string with less characters, the length was not calculated correctly. So the additional length of the string has allowed random characters to be present in the string which has caused this issue and error prompt "%". Fixed to have no

	restrictions in characters in applying the community string and having more than one community string is possible. Click for Additional Information
Case: 00396875 *CRAOS6X-2343*	**Summary:** Password in radius server with space is getting rejected. **Explanation**: In 672R06 code, the password in the radius server with space is getting rejected and unable to get authenticated. Click for Additional Information
Case: 00396842 *CRAOS6X-2344*	**Summary:** OS6350 - Pixilation to the video stream. **Explanation**: Intermediate pixelization and jitters on the clients connected to the OS6350 switch. The HD-VOD stream used is a unicast stream with CBR: 8K. The VOD unicast is burst traffic and High Definition at 25 Frames per second. Packet loss is seen at the time of the pixel image. The client connected port is 100mbps port it will discard the packets which exceed the port bandwidth. Fix provided to increase per-port buffer and per Q buffer limit. Click for Additional Information
Case: 00407807 00417824 *CRAOS6X-2544*	**Summary:** OS6450: SFTP get requests are getting disconnected and OV2500 backup failed. **Explanation**: Failures are happening randomly during get and the issue is due to SFTP than SSH. Click for Additional Information
Case: 00409807 *CRAOS6X-2577*	**Summary:** OV2500 receives httpServerSoSAttackTrap. **Explanation**: When the switch receives unknown URL from the client, it will send HttpDoS trap. Code changes done on AOS 6.7.2.R07 to avoid HttpDoS trap raised due to "/favicon", as this Favicon.ico is added by browser. Click for Additional Information
Case: 00413038 *CRAOS6X-2412*	**Summary:** Switch lost connection to OV- Cirrus after internet connection flapped. **Explanation**: Call-home failed because switch got a timeout (in 30 seconds) while waiting for a response from Activation Server. The Activation Server could be busy handling hundreds of requests and might take more than 30 seconds to respond to switch. Fix increases the connect timeout value from 30 seconds to 300 seconds to make sure that failure comes only when Activation Server doesn't respond within 300 seconds. This will give 300 second time interval to establish a connection from switch to Activation Server. Click for Additional Information

Case: 00419227 *CRAOS6X-2751*	**Summary:** OS6450: show ntp server status does not show any information. **Explanation**: The NTP task fails to add the NTP server IP resolved in a NTP server pending list. NTP task then fails to configure this NTP server and it is not added in the NTP server active list. The configured NTP server is not considered as an active NTP server and is not available to share status information. Fixed to have the NTP server IP in active list and to show the status information. 🔒 Click for Additional Information
Case: 00402986 *CRAOS6X-2516*	**Summary:** OS6350 switch - Failing to configure dot1x port with particular UNP profile name. **Explanation**: The issue is specific to OS6350 switches because it has a condition check not to allow Captive portal commands. In which the character 'C' is checked from the input parameters. In this case, UNP name had character C in it, due to which the error was thrown. Fixed to throw error only in case of Captive portal commands applied to the switch. 🔒 Click for Additional Information

- Lock Icon (🔒) - Indicates credentials required to log into the Business Portal website.
- Click on the associated URL for more information.