Release Notes

OmniSwitch 6350/6450

Release 6.7.2.R06

These release notes accompany release 6.7.2.R06 software for the OmniSwitch6350/6450 series of switches. The document provides important information on individual software and hardware features. Since much of the information in the release notes is not included in the hardware and software user manuals, it is important to read all sections of this document before installing new hardware or loading new software.

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

Alcatel-Lucent Enterprise.
Copyright © 2019. All rights reserved.

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.R06 Prerequisites

N/A

System Requirements

Memory Requirements

The following are the requirements for the OmniSwitch6350/6450 Series Release 6.7.2.R06:

- 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 CPLDthat is available with the 6.7.2.R06 AOS software available from Service & Support.

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

Release	Uboot/Miniboot	CPLD
6.7.2.89.R06(GA)	6.6.3.259.R01	6

OmniSwitch 6450-24/P24/48/P48

Release	Uboot/Miniboot	CPLD
6.7.2.89.R06(GA)	6.6.3.259.R01	11

OmniSwitch 6450-U24

Release	Uboot/Miniboot	CPLD
6.7.2.89.R06(GA)	6.6.3.259.R01	6

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

Release	Uboot/Miniboot	CPLD
6.7.2.89.R06(GA)	6.6.4.54.R01	11

OmniSwitch 6450-P10S/U24S

Release	Uboot/Miniboot	CPLD
6.7.2.89.R06(GA)	6.6.5.41.R02	P10S - 4 U24S – 7

OmniSwitch 6450-M/X Models

Release	Uboot/Miniboot	CPLD
6.7.2.89.R06(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
6.7.2.89.R06(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
6.7.2.89.R06(GA)	6.7.1.30.R04	4

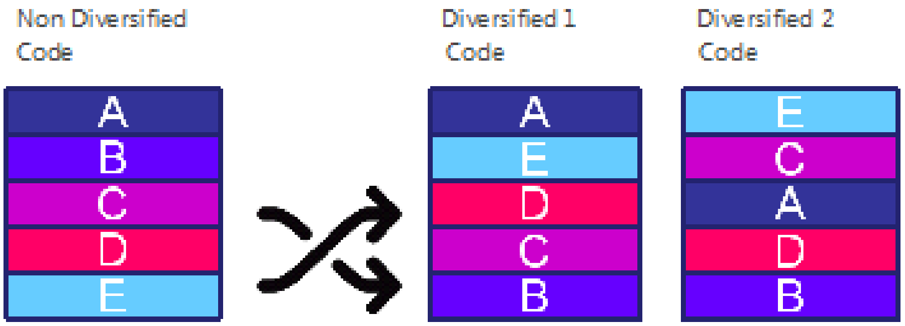
Note: Refer to the Upgrade Instructions section for upgrade instructions and additional information on Uboot/Miniboot and CPLD requirements.

CodeGuardian

Alcatel-Lucent Enterprise and LGS Innovations have combined to provide the first network equipment to be hardened by an independent group. CodeGuardian promotes security and assurance at the network device level using independent verification and validation of source code, software diversification to prevent exploitation and secure delivery of software to customers.

CodeGuardian employs multiple techniques to identify vulnerabilities such as software architecture reviews, source code analysis (using both manual techniques and automated tools), vulnerability scanning tools and techniques, as well as analysis of known vulnerabilities in third party code.
Software diversification

Software diversification randomizes the executable program so that various instances of the same software, while functionally identical, are arranged differently. The CodeGuardian solution rearranges internal software while maintaining the same functionality and performance and modifies the deliverable application to limit or prevent/impede software exploitation. There will be up to 3 different diversified versions per GA release of code.



CodeGuardian AOS Releases

Chassis	Standard AOS Releases	AOS CodeGuardian Release	LGS AOS CodeGuardian Release
OmniSwitch 6450	AOS 6.7.2.R06	AOS 6.7.2.RX6	AOS 6.7.2.LX6

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

6.7.2.R06 New Hardware Supported

SFP-1G-T Copper Transceiver
Fixed speed 1000Base-T Gigabit Ethernet Transceiver SFP MSA. Supports category 5, 5E, and 6 copper cabling up to 100m. This transceiver works only at 1000 Mbit/s speed and full-duplex mode.

SFP-DUAL-MM-N Transceiver
The SFP-DUAL-MM-N transceiver is now supported on the OmniSwitch 6350 and OmniSwitch 6450 uplink ports. Supports 1-gigabit speed only.

6.7.2.R06 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
Introduction of Salt and Hash-Salt for RADIUS, TACACS+ and LDAP servers	OS6350/OS6450	N/A
Link Aggregation Statistics Support	OS6350/OS6450	N/A
Non-Unicast/Multicast load balancing on Link Agg	OS6350/OS6450	N/A
Preserve LPS configuration on delayed NI Bootup	OS6350/OS6450	N/A
POE Port Status Enhancements	OS6350/OS6450	N/A
Support of Initial URL Redirection during UPAM BYOD session.	OS6350/OS6450	N/A

Feature Summary Table

New Feature Descriptions

Link Aggregation Statistics Support
This feature enables to view the cumulative statistics output value of all ports in the linkagg. To display the statistics for a linkagg, all the physical ports in the linkagg are identified, and relevant statistics are aggregated and displayed for various show commands. The LAG statistics for accounting, counters, counters errors, traffic values are displayed. Link aggregation statistics will be displayed for static and dynamic link aggregation only.

Introduction of Salt and Hash-Salt for RADIUS, TACACS+ and LDAP servers
In server configuration commands of RADIUS, TACACS+ and LDAP, two new parameters “salt” and “hash-salt” is supported that add randomness for the encryption of key. If no salt values is provided, then the system time (24-hour value format) will be taken as default salt value.

Non-Unicast/Multicast load balancing on Link Agg
Hashing is an algorithm widely used by Link aggregation module for load balancing traffic on link agg ports. Hashing was applied only for unicast traffic and not for non-unicast traffics like unknown unicast, broadcast, multicast traffics. This feature provides the user an option to enable the hashing for non-unicast traffic at a global level, which will load balance the non-unicast traffic across all ports in the link agg. By default, hash control setting for non-unicast traffic is disabled.

Preserve LPS configuration on delayed NI Bootup
The chassis management module (CMM) creates the LPS database of the ports when the boot configuration file (boot.cfg) is parsed by the CMM. In an event when the stack is rebooting and any NI with LPS configuration comes up with a delay or is not up during the parsing of the boot.cfg file by the CMM then the LPS configuration for that NI is not applied.
However, the LPS functionality is enhanced to store the LPS configuration in the configuration manager. Whenever a NI comes up the configuration manager receives a NI UP message from the CMM. When the configuration manager receives a NI UP message it verifies if it has any stored configuration for that NI. If the configuration is present for that NI, then it is applied.

In an event when configuration manager is unable to apply the configuration, the configuration is applied by a retry mechanism by checking the NI state.

Note:
The boot.cfg file must be stored with the correct LPS configurations in accordance with the number of ports in the switch.

POE Port Status Enhancements
The 'status' field output descriptions of the 'show lanpower slot' command is now enhanced to provide more detailed explanations on POE.

Support of Initial URL Redirection during UPAM BYOD session.
AOS devices can now append the initial URL to the redirect URL returned from OV Cirrus server. This means that for a BYOD user, after the second level authentication is successful in OV Cirrus, the initial URL page is displayed when the fixed URL is not configured.

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-672	OVCloud : Device console hang during call-home restart once VPN failed.	Wait until CLI timeout.
CRAOS6X-1796	After configuring LPS for all slots ports and when the slot id is changed, the LPS configuration was preserved in the NI, even after issuing write memory flash-synchro command.	There is no known workaround at this time.
CRAOS6X-2139	When an OmniSwitch is loaded with AoS image and reloaded, an error message "*Corrupted entry in dhcpClient.db file*" is displayed during boot up.	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 configurations, different images etc.).
- When removing modules from the stack (powering off the module and/or pulling out its stacking cables), the loop back stacking cable must be present at all times to guarantee redundancy. If a module is removed from the stack, rearrange the stacking cables to establish the loopback before attempting to remove a second unit.
- When inserting a new module in the stack, the loopback has to be broken. Full redundancy is not guaranteed until the loopback is restored.

Stack Element Insert/Removal Exceptions

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

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

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

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

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

Technical Support

Alcatel-Lucent technical support is committed to resolving our customer's technical issues in a timely manner. Customers with inquiries should contact us at:

Region	Phone Number
North America	800-995-2696
Latin America	877-919-9526
Europe Union	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484

Email:ebg_global_supportcenter@al-enterprise.com

Internet: Customers with Alcatel-Lucent service agreements may open cases 24 hours a day via Alcatel-Lucent Enterprise support web page at: https://businessportal2.alcatel-lucent.com

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

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

Appendix A: AOS 6.7.2.R06 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.R06.
- OmniSwitch 6350 models being upgraded to AOS 6.7.2.R06.

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.R06.

Version Requirements - Upgrading to AOS Release 6.7.2.R06

Version Requirements to Upgrade to AOS Release 6.7.2.R06			
	AOS	**Uboot/Miniboot**	**CPLD**
6450-10/10L/P10/P10L	6.7.2.89.R06(GA)	6.6.3.259.R01	6
6450-24/P24/48/P48		6.6.3.259.R01	11
6450-U24		6.6.3.259.R01	6
6450-24L/P24L/48L/P48L		6.6.4.54.R01	11
6450-P10S		6.6.5.41.R02	4
6450-U24S		6.6.5.41.R02	7
6450-10M		6.7.1.54.R02	6
6450-24X		6.7.1.54.R02	7
6450-24XM,24X,P24X,P48X,		6.7.1.54.R02	11
6350-24/P24/48/P48	6.7.2.89.R06(GA)	6.7.1.69.R01/6.7.1.103.R01 (minimum) 6.7.1.30.R04 (optional)	12 (minimum) 16 (optional)
6350-10/P10		6.7.1.30.R04	4

- The OS6450 "L" models were introduced in AOS Release 6.6.4.R01 and ship with the correct minimum versions, no upgrade is required.
- Uboot/Miniboot versions 6.6.4.158.R01 and 6.6.4.54.R01 were newly released versions in 6.6.4.R01.
- CPLD versions 14, 6, and 11 were newly released versions in 6.6.4.R01.

- Uboot/Miniboot version 6.6.3.259.R01 was previously released with 6.6.3.R01.
- CPLD version 12 was previously released with 6.6.3.R01.
- IMPORTANT NOTE: If performing the optional upgrade BOTH Uboot/Miniboot and CPLD MUST be upgraded.
- The 6.7.1.30.R04 uboot/miniboot and CPLD 16 for the 6350-24/48 models is only needed for stacking support. Standalone units can remain at the previous version.

Upgrading to AOS Release 6.7.2.R06

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.R06may 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 OmniSwitch6350.

Dynamic Rules supported in 6.7.2.R04 is 193 whereas in 6.7.2.R06 it is 173. So when the switches are upgraded from pre 6.7.2.R06 (6.7.2.R01/2/3/4) to 6.7.2.R06 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.R06 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.R06 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.R06.

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 6.7.2.112.R05   18130755 Alcatel-Lucent Enterprise Base Softw
KFos.img 6.7.2.112.R05      3562484 Alcatel-Lucent Enterprise OS
KFeni.img 6.7.2.112.R05     6152493 Alcatel-Lucent Enterprise NI software
KFsecu.img 6.7.2.112.R05     648189 Alcatel-Lucent Enterprise Security M
KFdiag.img 6.7.2.112.R05    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.R06 Downgrade Instructions

OmniSwitch Downgrade Overview

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

- OmniSwitch 6450 models being downgraded from AOS 6.7.2.R06.
  OmniSwitch 6350 models being downgraded from AOS 6.7.2.R06.

  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 models with 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.R06. Previous AOS releases are compatible with the Uboot/Miniboot and CPLD versions shipping from the factory.

Summary of Downgrade Steps

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

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

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

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

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

3. Proceed to Step 2.

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

Downgrading - Step 2. Downgrade the AOS

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

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

2. Once the switch reboots, certify the downgrade:
   - If you have **a single CMM** enter:
   ```
   -> copy working certified
   ```
   - If you have **redundant CMMs** enter:
   ```
   -> copy working certified flash-synchro
   ```

Proceed to Verifying the Downgrade

Verifying the Downgrade

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

```
-> show microcode

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

Appendix C: Fixed Problem Reports

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

CR/PR NUMBER	Description
Case: 00371909 *CRAOS6X-2070*	**Summary:** Missing some TV multicast channels on floor switches. **Explanation**: Multicast traffic drop on some of the floor seen with OS 6450 switches. The multicast traffic is learned on the non-primary port of the linkagg configured between core & edge switches. The multicast flow is dropped in the switch and rebooting the switch resolved the issue. 🔒 Click for Additional Information
Case: 00372266 *CRAOS6X-2085*	**Summary:** Query on "show running-directory" with the respective OID value. **Explanation:** configChangeStatus value and show running-directory output were different. This behavior was observed in 672R03,R04,and R05 releases. 🔒 Click for Additional Information
Case: 00370056 ***CRAOS6X-2078***	**Summary:** OS6450: The age for dynamic routes resets after the switch uptime crosses 828.5 days **Explanation:** Dynamic routes are flapping after the switch uptime crosses 828.5 days. The issue is seen only after the switch is UP for more than 828.5 days. The routes flap leading to temporary connectivity loss. The connectivity is automatically restored as the routes are repopulated (without user intervention). 🔒 Click for Additional Information
Case: 00362333 **Case: 00367120** *CRAOS6X-1933*	**Summary:** Radius "Class" attribute is modified by ALE before being sent to accounting server. **Explanation:** Accounting tab is not seen for the 802.1X authenticated wired clients on the Access tracker of the clear pass server even though the accounting information was sent to the clear pass server. OS6450 not sending the class 25 attribute exactly (in the RADIUS accounting request packet) as it was sent by the CPPM RADIUS server in the access-accept. The switch was removing the trailing zeros in the class 25 attribute which is causing the accounting tab not to be displayed in the clear pass access tracker. 🔒 Click for Additional Information
Case: 00360320 *CRAOS6X-1908*	**Summary:** OS6450-48 crashed and reboot.

	Explanation: OS6450-48 crashed unexpectedly after a user SSH to the switch. The switch crashed due to Memory Allocation Failure. 🔒 Click for Additional Information
Case: **00361820** *CRAOS6X-1885*	**Summary:** OS6350 DHCP problem – Options 66. **Explanation:** DHCP Server needs to provided TFTP Address to IP Phones when using Option 66. The command 'option dhcp-tftp-server "x.x.x.x"; ' is not considered and the Option 66 is not available in the DHCP Offer. 🔒 Click for Additional Information
Case: **00357100** *CRAOS6X-1803*	**Summary:** OS6450: Unable to communicate with router. **Explanation:** OS6450 unable to communicate with the router and error logs has been observed during the issue state. *I2C_do_transaction: i2cread get fail! tmp_len[2] = len[2] - rxtx_len[0] channel* *SYSTEM error i2cLM77ReadReg: Error writing LM77 Register 0 02d0 device 1 Temp sensor 0x48* *PRB-CHASSIS error Error reading temperature sensor* When I2C tries to read the CPLD register periodically for GBIC status, Fan status, Power status value, temperature etc. and if it is fails, logs are seen. 🔒 Click for Additional Information
Case: **00357528** *CRAOS6X-1800*	**Summary:** The "session login-attempt" feature does not apply to http / https connections. **Explanation:** The "session login-attemp" feature does not apply to http / https connections. Even if the loging-attemp setting is changed to 6, 3 login-attemp is applied to http / https connection. 🔒 Click for Additional Information
Case: **00357956** *CRAOS6X-1787*	**Summary:** Vulnerability- NTP mode 6. **Explanation:** Configured OS6450 and OS6350 as NTP client . NTP Mode 6 Vulnerability detected by Nessus Scanner on the releases 6.7.2.R04 and 6.7.2.R05. The feature was added to the code to restrict NTP Clients to response to Mode 6 queries: ->*ntp restrict default no-query* 🔒 Click for Additional Information

Case: **00350100** *CRAOS6X-1780*	**Summary:** "show lldp <slot> remote-system" hangs the CLI. Switch crashed. **Explanation:** With the usage of the command "show lldp <slot> remote-system, the CLI hung so another session was started from a different window. When that CLI entered dshell the switch crashed. 🔒 Click for Additional Information
Case: **00355203** **Case:** **00357931** **Case:** **00363540** **Case:** **00363826** **Case:** **00348239** **Case:** **00348239** *PR: CRAOS6X-1754*	**Summary:** OS6450 - SSH Error while trying to perform backup from OmniVista. **Explanation:** Following error is seen on OS6450 while trying to perform backup from OmniVista and the backup is failing: *SSH error [SSH 20] sshd_exchange_identification: select: S_iosLib_INVALID_FILE_DESCRIPTOR* This issue is seen only when OmniVista is used to back up the switch config via SFTP. SFTP from any device to the switch also fails. By increasing the waiting time of the SELECT function and the additional time has been added to the timeout value, which would allow the write process to become ready for the data transfer to continue. 🔒 Click for Additional Information
Case: **00354629** *CRAOS6X-1744*	**Summary:** OS6350: Mark all management traffic to 802.1p. **Explanation:** The 802.1p field is not marked by policy although traffic is matching (use the command show qos log). Apply a policy for DHCP marking. 🔒 Click for Additional Information
Case: **00352100** **Case:** **00357129** *CRAOS6X-1733*	**Summary:** OS6450 Unable to change the default Admin Password. **Explanation:** Not able to change the default Admin password of the switch OS6450 after upgrading switch from 6.6.4. 244.R01 to 6.7.2. 191.R04. Getting error message " Password cannot be change until", even though the user password -min-age is 1 but the date is missing because it was showing “None” for default admin. 🔒 Click for Additional Information
Case: **00351969** *CRAOS6X-1700*	**Summary:** OS6450 6.7.2.R05 - Stellar AP 1201H in aaa blocking policy (not classified in built-in defaultWLANProfile policy). **Explanation:**

	Stellar AP is blocked by Access Guardian when connected to 802.1x with built-in policy “defaultWLANProfile” based on LLDP classification. Use 802.1x MAC Authentication or classification based on MAC Range instead of LLDP classification. 🔒 Click for Additional Information
Case: 00348493 *CRAOS6X-1682*	**Summary:** OS6450 switch is not sending any trap message. **Explanation:** When the fan failure occurred in Normal Temperature (device temperature lower than upper threshold temperature) no Traps were sent, Only the log got captured " info Board temp is below the threshold, Fan #3 is not running". 🔒 Click for Additional Information
Case: 00344478 *CRAOS6X-1642*	**Summary:** Unable to access SSH for end-user profile. **Explanation:** User associated with end-user profile is not able to access via SSH due to user privileges. 🔒 Click for Additional Information
Case: 00346146 *CRAOS6X-1630*	**Summary:** OV Cirrus - Device W2180194 lost its VPN connectivity during several days without do call home function. **Explanation:** Switch OS6350/0S6450 connected to OV Cirrus through the VPN link are losing the connectivity because of a TLS Handshake failure.Restarting the cloud agent will resolve the issue. 🔒Click for Additional Information
Case: 00342491 *CRAOS6X-1616*	**Summary:** OS6450 - No internet access on dot1x authenticated client on some port. **Explanation:** Client is unable to reach external site like (google.de) and PCs in the same vlan. The issue is noticed in stack. 🔒 Click for Additional Information
Case: 00339445 *CRAOS6X-1609*	**Summary:** CPE-Test on OS6450-U24SXM-10G port test not starting unless the port is physically UP. **Explanation:** CPE test does not show the statistics if the generator uses the 10G port as test-OAM port. It shows the following error when the test is started: *-> test-oam e2e start fetch-remote-stats* *FRI MAR 08 12:54:03 : INTERFACE (6) error message:*

	+++ == *HAL == hal_esm_set_phy_power_down:14139: error lport:26* There is no error and the test-OAM works if 1G port is used as test-OAM port. Run the test on a 10G port that is active. 🔒 Click for Additional Information
Case: 00335889 *CRAOS6X-1550*	**Summary:** ARP resolves to the incorrect port. **Explanation:** ARP learning caused arp packets with sender mac and ethernet source mac different. With CLI "ip dos arp-protect enable/disable", when enabled packets with different source mac and sender mac will be dropped. This feature will be disabled by default. Enabled or disabled status can be seen in "show ip dos config". This arp-protect has less precedence than arp-poison. 🔒 Click for Additional Information
Case: 00324103 *CRAOS6X-1432*	**Summary:** ip-ping SAA probe issue with no static MAC configured in the source. **Explanation:** SAA ip-ping is configured on OS6450 to sent ICMP packets with a source IP towards another destination IP. When there is no static ARP configured for the destination, packet drops will be seen from time to time while re-learning the ARP. In SAA statistics, total number of packets received will be less than the packets sent.As a workaround, configure static ARP entry for the destination IP. 🔒 Click for Additional Information
Case: 00343441 *CRAOS6X-1595*	**Summary**: Update of Switches via OV2500 fails. **Explanation**: Upgrade the OS6450 switch through OV. The issue is File transfer to the switch was timed out when choosing all files at once on OV. 🔒 Click for Additional Information
Case: 00337084 *CRAOS6X-1490*	**Summary:** SAM server keeps receiving the "Reachability test failed" Alarms for the OS6450 switches and it is completely intermittent. **Explanation:** The OS6450 switches are not responding for the “SysUptime” polling from the SAM server and issue is intermittent. 🔒 Click for Additional Information

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