Release Notes

OmniSwitch 6350/6450

Release 6.7.2.R03

These release notes accompany release 6.7.2.R03 software for the OmniSwitch 6350/6450 series of switches. The document provides important information on individual software and hardware features. Since much of the information in the release notes is not included in the hardware and software user manuals, it is important to read all sections of this document before installing new hardware or loading new software.

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

Table of Contents

Related Documentation

The release notes should be used in conjunction with the associated manuals as listed below.
User manuals can be downloaded at:

https://support.esd.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: support.esd.alcatel-lucent.com.

AOS 6.7.2 R03 Prerequisites

ERPv2 Upgrade Procedure – 672.R02 build (ERPv1) to 672.R03 build (ERPv2)

ERPv2 support is new in 6.7.2 R03. Follow the given procedure to migrate from ERPv1 to ERPv2:

1. Before reloading the switch with build 6.7.2 R03, perform the following steps:
   a. Save the existing ERP configuration in *boot.cfg* by executing "write memory" CLI command.
   b. Also, save a copy of *boot.cfg* (of release 6.7.2 R02) of ERPv1 that might be required in case of downgrade from build 6.7.2 R03 to ERPv1 6.7.2 R02 build.

Note: Only build upgrade to Release 6.7.2 R03 shall be supported through software. For downgrade of Release to any Release lower than 6.7.2 R03, user has to use the old *boot.cfg* and no automatic conversion of configuration shall be supported for Release downgrade.

2. After the upgradation is successful from 6.7.2 R02 to 6.7.2 R03, it is required to issue the following command to have the ERP version changed from ERPv1 to ERPv2. Until the command is issued, the ERP version will remain as version 1. Once the ERP ring is in IDLE state after upgrading to 6.7.2.R03, the command below has to be issued on all nodes starting from the RPL. This updates the version to ERPv2. This command is used only for upgrading AOS to ERPv2. It does not save any configuration files.

   -> erp-ring reset-version-fallback

3. To support ERP configuration interoperability between 6.7.2 R02 and 6.7.2 R03, software has been enhanced to,
   a. Automatically convert the 6.7.2 R02 configuration of ERP into its corresponding version in 6.7.2 R03. This means ERP protected-vlan CLIs shall be automatically converted to 8021q tagging CLIs on up-gradation of build to 6.7.2 R03.
   b. The configuration snapshot shall be updated to store 6.7.2 R03 based version.

Note: The 672R02 version of ERP configuration (protected VLAN CLI), shall be honored by 6.7.2 R03 ERP only from boot.cfg (not at run time configuration). Hence, it is required to do "write memory" to save the configuration in boot.cfg.

4. Find below an example of ERP configuration (in Blue) in conventional mode and E-service mode for Release 672R02 and that shall be replaced by corresponding 672R03 configuration- ERPv2 CLIs (in Pink) after up-gradation.

   Conventional Mode (Standard VLAN mode) :

   In Release 672R02

Conventional Mode

```
6450-> show configuration snapshot erp
! ERP :
erp-ring 1 port1 1/1 port2 1/2 service-vlan 700 level 1
erp-ring 1 protected-vlan 701-710
erp-ring 1 enable

6450-> show configuration snapshot vlan
! VLAN :
vlan 1 enable name "VLAN 1"
vlan 172 enable name "VLAN 172"
vlan 172 port default 2/21
vlan 172 port default 2/22
```

```
vlan 700 enable name "VLAN 700"
vlan 701 enable name "VLAN 701"
vlan 702 enable name "VLAN 702"
vlan 703 enable name "VLAN 703"
vlan 704 enable name "VLAN 704"
vlan 705 enable name "VLAN 705"
vlan 706 enable name "VLAN 706"
vlan 707 enable name "VLAN 707"
vlan 708 enable name "VLAN 708"
vlan 709 enable name "VLAN 709"
vlan 710 enable name "VLAN 710"
! VLAN SL:
! VLAN AGG:
! VLAN STACKING:

6450-> show configuration snapshot 802.1q
! 802.1Q :
```

In Release 672R03 (After Upgradation)

Conventional Mode

```
6450-> show configuration snapshot erp
! ERP :
erp-ring 1 port1 1/1 port2 1/2 service-vlan 700 level 1
erp-ring 1 enable

6450-> show configuration snapshot vlan
! VLAN :
vlan 1 enable name "VLAN 1"
vlan 172 enable name "VLAN 172"
vlan 172 port default 2/21
vlan 172 port default 2/22
vlan 700 enable name "VLAN 700"
vlan 701 enable name "VLAN 701"
vlan 702 enable name "VLAN 702"
vlan 703 enable name "VLAN 703"
vlan 704 enable name "VLAN 704"
vlan 705 enable name "VLAN 705"
vlan 706 enable name "VLAN 706"
vlan 707 enable name "VLAN 707"
vlan 708 enable name "VLAN 708"
vlan 709 enable name "VLAN 709"
vlan 710 enable name "VLAN 710"
! VLAN SL:
! VLAN AGG:
! VLAN STACKING:

6450-> show configuration snapshot 802.1q
! 802.1Q :
vlan 700 802.1q 1/15 "TAG PORT 1/15 VLAN 700"
vlan 701 802.1q 1/15 "TAG PORT 1/15 VLAN 701"
vlan 702 802.1q 1/15 "TAG PORT 1/15 VLAN 702"
vlan 703 802.1q 1/15 "TAG PORT 1/15 VLAN 703"
vlan 704 802.1q 1/15 "TAG PORT 1/15 VLAN 704"
vlan 705 802.1q 1/15 "TAG PORT 1/15 VLAN 705"
vlan 706 802.1q 1/15 "TAG PORT 1/15 VLAN 706"
vlan 707 802.1q 1/15 "TAG PORT 1/15 VLAN 707"
vlan 708 802.1q 1/15 "TAG PORT 1/15 VLAN 708"
vlan 709 802.1q 1/15 "TAG PORT 1/15 VLAN 709"
vlan 710 802.1q 1/15 "TAG PORT 1/15 VLAN 710"
vlan 700 802.1q 1/16 "TAG PORT 1/16 VLAN 700"
vlan 701 802.1q 1/16 "TAG PORT 1/16 VLAN 701"
```

```
vlan 702 802.1q 1/16 "TAG PORT 1/16 VLAN 702"
vlan 703 802.1q 1/16 "TAG PORT 1/16 VLAN 703"
vlan 704 802.1q 1/16 "TAG PORT 1/16 VLAN 704"
vlan 705 802.1q 1/16 "TAG PORT 1/16 VLAN 705"
vlan 706 802.1q 1/16 "TAG PORT 1/16 VLAN 706"
vlan 707 802.1q 1/16 "TAG PORT 1/16 VLAN 707"
vlan 708 802.1q 1/16 "TAG PORT 1/16 VLAN 708"
vlan 709 802.1q 1/16 "TAG PORT 1/16 VLAN 709"
vlan 710 802.1q 1/16 "TAG PORT 1/16 VLAN 710"
```

Ethernet Service Mode:

In Release 672R02

Ethernet Service Mode

```
6450-> show configuration snapshot erp
! ERP :
erp-ring 1 port1 1/1 port2 1/2 service-vlan 600 level 1
erp-ring 1 protected-vlan 601-611
erp-ring 1 enable

6450-> show configuration snapshot vlan
! VLAN :
vlan 1 enable name "VLAN 1"
vlan 172 enable name "VLAN 172"
vlan 172 port default 2/21
vlan 172 port default 2/22
ethernet-service svlan 600 name "VLAN 600"
ethernet-service svlan 601 name "VLAN 601"
ethernet-service svlan 602 name "VLAN 602"
ethernet-service svlan 603 name "VLAN 603"
ethernet-service svlan 604 name "VLAN 604"
ethernet-service svlan 605 name "VLAN 605"
ethernet-service svlan 606 name "VLAN 606"
ethernet-service svlan 607 name "VLAN 607"
ethernet-service svlan 608 name "VLAN 608"
ethernet-service svlan 609 name "VLAN 609"
ethernet-service svlan 610 name "VLAN 610"
ethernet-service svlan 611 name "VLAN 611"
! VLAN SL:
! VLAN AGG:
! VLAN STACKING:
ethernet-service svlan 600 nni 1/1-2 erp
ethernet-service svlan 601 nni 1/1-2 erp
ethernet-service svlan 602 nni 1/1-2 erp
ethernet-service svlan 604 nni 1/1-2 erp
ethernet-service svlan 605 nni 1/1-2 erp
ethernet-service svlan 606 nni 1/1-2 erp
ethernet-service svlan 607 nni 1/1-2 erp
ethernet-service svlan 608 nni 1/1-2 erp
ethernet-service svlan 609 nni 1/1-2 erp
ethernet-service svlan 610 nni 1/1-2 erp
ethernet-service svlan 611 nni 1/1-2 erp
```

In Release 672R03 (After Up gradation)

Ethernet Service Mode

```
6450-> show configuration snapshot erp
! ERP :
erp-ring 1 port1 1/1 port2 1/2 service-vlan 600 level 1
erp-ring 1 enable

6450-> show configuration snapshot vlan
! VLAN :
vlan 1 enable name "VLAN 1"
vlan 172 enable name "VLAN 172"
vlan 172 port default 2/21
vlan 172 port default 2/22
ethernet-service svlan 600 name "VLAN 600"
ethernet-service svlan 601 name "VLAN 601"
ethernet-service svlan 602 name "VLAN 602"
ethernet-service svlan 603 name "VLAN 603"
ethernet-service svlan 604 name "VLAN 604"
ethernet-service svlan 605 name "VLAN 605"
ethernet-service svlan 606 name "VLAN 606"
ethernet-service svlan 607 name "VLAN 607"
ethernet-service svlan 608 name "VLAN 608"
ethernet-service svlan 609 name "VLAN 609"
ethernet-service svlan 610 name "VLAN 610"
ethernet-service svlan 611 name "VLAN 611"
! VLAN SL:
! VLAN AGG:
! VLAN STACKING:
ethernet-service svlan 600 nni 1/1-2
ethernet-service svlan 601 nni 1/1-2
ethernet-service svlan 602 nni 1/1-2
ethernet-service svlan 604 nni 1/1-2
ethernet-service svlan 605 nni 1/1-2
ethernet-service svlan 606 nni 1/1-2
ethernet-service svlan 607 nni 1/1-2
ethernet-service svlan 608 nni 1/1-2
ethernet-service svlan 609 nni 1/1-2
ethernet-service svlan 610 nni 1/1-2
ethernet-service svlan 611 nni 1/1-2
```

Note: ERPv2 and STP shall not operate together on the same port. All the VLANs tagged to the ring port (802.1q) shall be controlled by ERP only and not by STP.

System Requirements

Memory Requirements

The following are the requirements for the OmniSwitch 6350/6450 Series Release 6.7.2.R02:

OmniSwitch 6350/6450 Series requires 256 MB of SDRAM and 128MB of flash memory. This is the standard configuration shipped.

Configuration files and the compressed software images—including web management software (WebView) images—are stored in the flash memory. Use the **show hardware info** command to determine your SDRAM and flash memory.

Miniboot and FPGA Requirements for Existing Hardware

The software versions listed below are the minimum required version for existing models, except where otherwise noted. Switches running the minimum versions, as listed below; do not require any miniboot or CPLD upgrade.

Switches not running the minimum version required should be upgraded to the latest Uboot/Miniboot or CPLD that is available with the 6.7.2.R01 AOS software available from Service & Support.

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

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

OmniSwitch 6450-24/P24/48/P48

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

OmniSwitch 6450-U24

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

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

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

OmniSwitch 6450-P10S/U24S

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

OmniSwitch 6450-M/X Models

Release	Uboot/Miniboot	CPLD
6.7.2.107.R03(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
6.7.2.107.R03(GA)	6.7.1.69.R01/6.7.1.103.R01 6.7.1.30.R04 (optional)	12 (minimum) 16 (optional)
Note: The optional uboot/miniboot and CPLD is only needed for stacking support. Standalone units can remain at the previous versions.		

OmniSwitch 6350-10/P10

Release	Uboot/Miniboot	CPLD
6.7.2.107.R03(GA)	6.7.1.30.R04	4

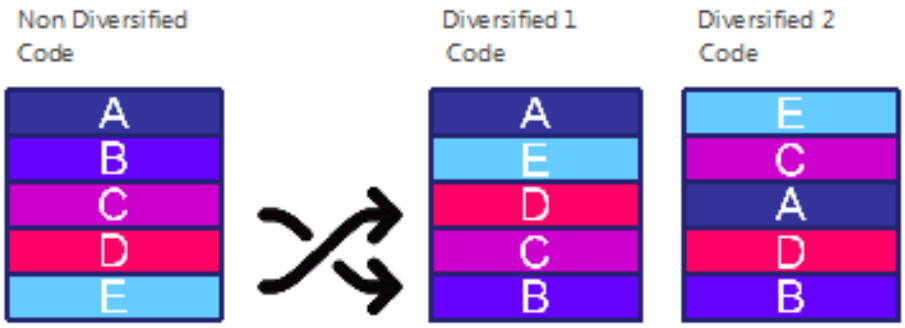
Note: Refer to the Upgrade Instructions section for upgrade instructions and additional information on Uboot/Miniboot and CPLD requirements.

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.R03	AOS 6.7.2.RX	AOS 6.7.2.LX

X=Diversified image 1-3
ALE will have 3 different diversified images per AOS release (R12 through R32)
Our partner LGS will have 3 different diversified images per AOS release (L12 through L32)

6.7.2.R03 New Hardware Supported

OS6450-XNI-U2X - 10G Uplink Port
New module that upon insertion sets the switch to Standalone mode and the two 10G ports act as uplink ports.
Note: The current OS6450-XNI-U2 module supports stacking mode only.

OS6450-24 SXM supports XNI-U2X expansion module in standalone mode.
Other OS6450 24/48 port variants with compatible expansion module slot will also support XNI-U2X expansion slot in standalone mode.
XNI-U2X ports will have assigned port numbers 27,28 in 24-port variant and in 48-port variant this will have assigned port numbers 51,52.

This expansion module 2 * 10G uplink ports does not require METRO/10G license to operate in 10G mode.

XNI-U2X hot swap configuration with various other Expansion modules is listed below.

Expansion Module Being Installed	Expansion Module Being Replaced	Reboot Required?	Mode Following Installation	Actual Mode following Installation.
10G (OS6450-XNI-U2X)	None (empty slot)	Yes	Stackable	Standalone
10G (OS6450-XNI-U2X)	10G (OS6450-XNI-U2)	Yes	Stackable	Standalone
10G (OS6450-XNI-U2)	10G (OS6450-XNI-U2X)	Yes	Standalone	Stackable
10G (OS6450-XNI-U2X)	10G (OS6450-XNI-U2X)	No	Standalone	Standalone
10G (OS6450-XNI-U2X)	1G (OS6450-GNI-C2/U2)	Yes	Standalone	Standalone
1G (OS6450-GNI-C2/U2)	10G (OS6450-XNI-U2X)	Yes	Standalone	Stackable

6.7.2.R03 New Software Features and Enhancements

The following software features are new with this release, subject to the feature exceptions and problem reports described later in these release notes:

Feature	Platform	License
Two Port PoE Support	OS6350/OS6450	N/A
RADIUS Stats	OS6350/OS6450	N/A
OV Cloud Agent	OS6350/OS6450	N/A
Add "hash-key" keyword in aaa configuration CLI	OS6350/OS6450	N/A
Admin Password in SHA2	OS6350/OS6450	N/A
Increase RADIUS Server Re-Authentication Time	OS6350/OS6450	N/A
ERPv2 support on 6450	OS6450 [Metro licence is required]	N/A

Feature Summary Table

New Feature Descriptions

Two Port PoE Support
The requirement is to support the active/standby ports of the ARUBA APs (AP 135, AP 224, AP 225, AP 325) in scenarios where both of the ports are connected to the OmniSwitch. This feature will work as an active/standby configuration. It is advisable to enable this feature only when Two Port PD is used.

RADIUS Stats
The statistics for every RADIUS server configured on the OmniSwitch can be viewed. This allows to understand the transactions between switch and configured RADIUS server. The following statistics per RADIUS server is displayed:

- Global Information
- Authorization Statistics
- Authentication Statistics
- Accounting Statistics
- BYOD Statistics

OmniVista Cirrus
The OmniVista Cirrus (OV Cirrus) is an alternative to the current on premise version of OmniVista. The major objectives of the Cloud-based network management system are:

- Reduce the cost of IT for the Customer
- Management from anywhere and ability to manage the network using device ranging from top end workstations to smart phones.
- Simpler network setup
- Easier to use management and monitoring tools.
- Unified wired/wireless management from the cloud.

This feature allows the OmniSwitches to be managed remotely from OV Cirrus without any manual intervention.

Add "hash-key" keyword in aaa configuration CLI
The RADIUS server configuration now allows the user to provide the shared secret in encrypted form using keyword "hash-key". The hash-key secret will be used for transactions between Switch and RADIUS server. The hash-key input is based on MD5 hashing.

Shared secret configured either through Key or hash-key keyword will be displayed in encrypted form with keyword “hash-key” in show configuration snapshot aaa.
Since we do not support parameter “hash-key” in older builds, backward compatibility is not supported for this feature.

Admin Password in SHA2
The release adds support for SHA2 hashing for the user admin account. Currently this capability is only supported for users created with SNMP privileges. The support is now being extended to the user admin account.

Increase Auth-Server down Reauth Period
The maximum configurable range for re-auth timer value is increased from 9999 to 43200 seconds.

ERPv2 support on 6450
Ethernet Ring Protection (ERP) switching is a self-configuring algorithm that maintains a loop-free topology while providing data path redundancy and network scalability. ERP provides fast recovery times for Ethernet ring topologies by utilizing traditional Ethernet MAC and bridge functions.

Alcatel-Lucent OmniSwitch supports ERPv2 according to the ITU-T recommendation. G.8032 03/2010 in the current AOS version. The previous AOS versions support ERPv1.

The ERPv2 implementation helps maintain a loop-free topology in multi-ring and ladder networks that contain interconnection nodes, interconnected shared links, master rings and sub-rings.

With the introduction of Version 2, OmniSwitch supports the following:
- Backward compatibility with ERPv1
- Multi-ring and ladder networks
- Interconnection nodes
- Interconnected shared links
- Master rings
- Sub-rings
- Revertive and non-revertive mode

Unsupported Software Features

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

Feature	Platform
BGP	6350/6450
DVMRP	6350/6450
IS-IS	6350/6450
Multicast Routing	6350/6450
OSPF, OSPFv3	6350/6450
PIM	6350/6450
Traffic Anomaly Detection	6350/6450
IPv6 Sec	6350/6450
IP Tunnels (IPIP, GRE, IPv6)	6350/6450
Server Load Balancing	6350/6450
VLAN Stacking / Ethernet Services	OS6350
Ethernet/Link/Test OAM	OS6350
PPPoE	OS6350
ERP	OS6350
GVRP	OS6350
IPv4/ IPv6 RIP	OS6350
VRRP	OS6350
HIC/ BYOD / Captive Portal	OS6350
mDNS Relay	OS6350
IPMVLAN (VLAN Stacking Mode)	OS6350
IPMC Receiver VLAN	OS6350
OpenFlow	OS6350
License Management	OS6350
Loopback Detection	OS6350
SAA	OS6350
Ethernet Wire-rate Loopback Test	OS6350
Dying Gasp	OS6350

Unsupported CLI Commands

The following CLI commands are not supported in this release of the software:

Software Feature	Unsupported CLI Commands
AAA	aaa authentication vlan single-mode aaa authentication vlan multiple-mode

Software Feature	Unsupported CLI Commands
	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.

PR	Description	Workaround
228221	When Guest user logins , 1st level of authentication happens and HTTP traffic from user is redirected to guest web login page. Once the user enters valid username/password , COA is successful and guest user is placed in new VLAN. But the guest user logout page is not displayed.Due to this user will not be able to disconnect from the session.	There is no known workaround at this time.
230517	Star symbol is missing in *show erp* command output, when ERP member port NI is not present in stack.	There is no known workaround at this time.
229431	When the new OS6450-XNI-U2X expansion module is removed from OS6450 slot, a HAL error message may be observed. This occurrence is intermittent and has no functional impact. Similarly when a 1G SFP is removed from the new XNI-U2X module, an error message is seen. This also has no functional impact.	There is no known workaround at this time.
229694	Class classification issue when powering up the stellar AP 1251 powered device. When PoE high-resistance is enabled, 2-port APs PD classification(PoE Class value) may not be accurate.	There is no known workaround at this time.

Redundancy/ Hot Swap

CMM (Primary Stack Module) and Power Redundancy Feature Exceptions

Manual invocation of failover (by user command or Primary pull) must be done when traffic loads are minimal.
Hot standby redundancy or failover to a secondary CMM without significant loss of traffic is only supported if the secondary is fully flash synchronized with the contents of the primary's flash.
Failover/Redundancy is not supported when the primary and secondary CMMs are not synchronized (i.e., unsaved configs, different images etc.).
When removing modules from the stack (powering off the module and/or pulling out its stacking cables), the loop back stacking cable must be present at all times to guarantee redundancy. If a module is removed from the stack, rearrange the stacking cables to establish the loopback before attempting to remove a second unit.
When inserting a new module in the stack, the loopback has to be broken. Full redundancy is not guaranteed until the loopback is restored.

Stack Element Insert/Removal Exceptions

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

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

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

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

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

Technical Support

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

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

Email: ebg_global_supportcenter@al-enterprise.com

Internet: Customers with Alcatel-Lucent service agreements may open cases 24 hours a day via Alcatel-Lucent's support web page at: support.esd.alcatel-lucent.com.

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

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

Appendix A: AOS 6.7.2.R03 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.R03.
OmniSwitch 6350 models being upgraded to AOS 6.7.2.R03.

Prerequisites

This instruction sheet requires that the following conditions are understood and performed, BEFORE upgrading:
Read and understand the entire Upgrade procedure before performing any steps.
The person performing the upgrade must:
- Be the responsible party for maintaining the switch's configuration.
- Be aware of any issues that may arise from a network outage caused by improperly loading this code.
- Understand that the switch must be rebooted and network users will be affected by this procedure.
- Have a working knowledge of the switch to configure it to accept an FTP connection through the Network Interface (NI) Ethernet port.

Read the Release Notes prior to performing any upgrade for information specific to this release.
All FTP transfers MUST be done in binary mode.

WARNING: Do not proceed until all the above prerequisites have been met and understood. Any deviation from these upgrade procedures could result in the malfunctioning of the switch. All steps in these procedures should be reviewed before beginning.

OmniSwitch Upgrade Requirements

These tables list the required Uboot/Miniboot, CPLD and AOS combinations for upgrading an OmniSwitch. The Uboot/Miniboot and CPLD may need to be upgraded to the versions listed below to support AOS Release 6.7.2.R03.

Version Requirements – Upgrading to AOS Release 6.7.2.R03

Version Requirements to Upgrade to AOS Release 6.7.2.R03			
	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,	6.7.2.107.R03(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	6.7.2.107.R03(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.R03

Upgrading consists of the following steps. The steps must be performed in order. Observe the following prerequisites before performing the steps as described below:

Upgrading an OmniSwitch to AOS Release 6.7.2.R03 may require two reboots of the switch or stack being upgraded. One reboot for the Uboot/Miniboot or AOS and a second reboot for the CPLD.
Refer to the Version Requirements table to determine the proper code versions.
Download the appropriate AOS images, Uboot/Miniboot, and CPLD files from the Service & Support website.

Summary of Upgrade Steps

1. FTP all the required files to the switch
2. Upgrade the Uboot/Miniboot and AOS images as required. (A reboot is required).
3. Upgrade the CPLD as required. (Switch automatically reboots).
4. Verify the upgrade and remove the upgrade files from the switch.

Upgrading - Step 1. FTP the 6.7.2.R03 Files to the Switch

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

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

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

Upgrading - Step 2. Upgrade Uboot/Miniboot and AOS

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

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

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

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

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

Upgrading - Step 3. Upgrade the CPLD

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

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

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

Single Switch Procedure

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

The switch will upgrade the CPLD and reboot.

Stack Procedure

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

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

The stack will upgrade the CPLD and reboot.

Proceed to Verifying the Upgrade to verify the upgrade procedure.

Verifying the Upgrade

The following examples show what the code versions should be after upgrading to AOS Release 6.7.2.R03.

Note: These examples may be different depending on the OmniSwitch model upgraded. Refer to the Version Requirements tables to determine what the actual versions should be.

Verifying the Software Upgrade

To verify that the AOS software was successfully upgraded, use the show microcode command as shown below. The display below shows a successful image file upgrade.

```
-> show microcode

Package         Release       Size       Description
----------------+--------------+----------+-----------------------------------------
KFbase.img       6.7.2.R03    15510736   Alcatel-Lucent Base Software
KFos.img         6.7.2.R03    2511585     Alcatel-Lucent OS
KFeni.img        6.7.2.R03    5083931    Alcatel-Lucent NI software
KFsecu.img       6.7.2.R03    597382      Alcatel-Lucent Security Management
```

Verifying the U-Boot/Miniboot and CPLD Upgrade

To verify that the CPLD was successfully upgraded on a CMM, use the show hardware info command as shown below.

```
-> show hardware info

CPU Type                    : Marvell Feroceon,
Flash Manufacturer          : Numonyx, Inc.,
Flash size                  : 134217728 bytes (128 MB),
RAM Manufacturer            : Samsung,
RAM size                    : 268435456 bytes (256 MB),
Miniboot Version            : 6.6.4.158.R01,
Product ID Register         : 05
Hardware Revision Register  : 30
FPGA Revision Register      : 014
```

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

```
-> show ni
Module in slot 1
Model Name:                 OS6450-24,
Description:                24 10/100 + 4 G,
Part Number:                902736-90,
Hardware Revision:          05,
Serial Number:              K2980167,
Manufacture Date:           JUL 30 2009,
Firmware Version: ,
Admin Status:               POWER ON,
Operational Status:         UP,
Power Consumption:          30,
Power Control Checksum:     0xed73,
CPU Model Type :            ARM926 (Rev 1),
MAC Address:                00:e0:b1:c6:b9:e7,
ASIC - Physical 1:          MV88F6281 Rev 2,
FPGA - Physical 1:          0014/00,
UBOOT Version :             n/a,
UBOOT-miniboot Version :    6.6.4.158.
```

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

Remove the CPLD and Uboot/Miniboot Upgrade Files

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

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

Appendix B: AOS 6.7.2.R03 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.R03.
OmniSwitch 6350 models being downgraded from AOS 6.7.2.R03.

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

Note: The OmniSwitch PoE models with the new PoE controller require a minimum of AOS Release 6.7.2.R01 and cannot be downgraded to any other release.
OS6350-P10 (903966-90)
OS6350-P24 (903967-90)
OS6350-P48 (903968-90)

Prerequisites

This instruction sheet requires that the following conditions are understood and performed, BEFORE downgrading:

Read and understand the entire downgrade procedure before performing any steps.
The person performing the downgrade must:

- Be the responsible party for maintaining the switch's configuration.
- Be aware of any issues that may arise from a network outage caused by improperly loading this code.
- Understand that the switch must be rebooted and network users will be affected by this procedure.
- Have a working knowledge of the switch to configure it to accept an FTP connection through the Network Interface (NI) Ethernet port.

Read the Release Notes prior to performing any downgrade for information specific to this release.
All FTP transfers MUST be done in binary mode.

WARNING: Do not proceed until all the above prerequisites have been met and understood. Any deviation from these procedures could result in the malfunctioning of the switch. All steps in these procedures should be reviewed before beginning.

OmniSwitch Downgrade Requirements

Downgrading the Uboot/Miniboot or CPLD is not required when downgrading AOS from 6.7.2.R03. Previous AOS releases are compatible with the Uboot/Miniboot and CPLD versions shipping from the factory.

Summary of Downgrade Steps

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

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

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

1. Download and extract the appropriate archive from the Service & Support website. The archive will contain the following files to be used for the downgrade:
   - AOS Files – KFbase.img, KFeni.img, KFos.img, KFsecu.img
   - AOS Files (6350) – KF3base.img, KF3eni.img, KF3os.img, KF3secu.img

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

3. Proceed to Step 2.

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

Downgrading - Step 2. Downgrade the AOS

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

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

2. Once the switch reboots, certify the downgrade:
   - If you have **a single CMM** enter:

   -> copy working certified
   - If you have **redundant CMMs** enter:

   -> copy working certified flash-synchro

Proceed to Verifying the Downgrade.

Verifying the Downgrade

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

```
-> show microcode

Package         Release        Size       Description
----------------+--------------+----------+-----------------------------------------
KFbase.img       6.6.5.R02   15510736  Alcatel-Lucent Base Software
KFos.img         6.6.5.R02    2511585  Alcatel-Lucent OS
KFeni.img        6.6.5.R02    5083931  Alcatel-Lucent NI software
KFsecu.img       6.6.5.R02     597382  Alcatel-Lucent Security Management
```

Appendix C: Fixed Problem Reports

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

PR NUMBER	SUMMARY
207510	Different AAA key are noticed while applying configuration.
227217	DDM values (Alert-Low) of SFP is wrong - raising alarms to NMS. Actual Low not following data-sheets
227680	OS6450: show power output displaying incorrect power supply type(showing as AC instead of DC)
227719	Packet drop noticed in ip-ping SAA probes (Ref: PR# 220514)
227804	6450 stopped DHCP client process
228113	Following the KCS article (000011607), the solution provided to add a hostname NTP server on the 645
228175	OS6450: Switch crashed while displaying "aaa" configuration
228269	OS6450 - Issue while exiting from the session after entering a certain command
228373	Port is not shutdown by qos when receiving the amap packet
228612	3XOS6450: After the reload “show running-directory" command shows stack is not synchronized
228613	OS6450: Clarification about the “I2C_do_transaction: i2cread get fail!” messages seen on the swlogs
228727	Duplicate RTP sequence number in the OS6450
229097	OS6450- static ARP enteries getting generated in boot.cfg. Ref PR#223261.
229131	Multicast entries not found in “show ip multicast group”, after sending multicast traffic flow in IP
229224	Seeing long convergence (>5 sec) for multicast traffic over ERP when ring is broken and/or restored,
229392	"stpCMM_linkAggVpaUpdate Wrong Symbol" Error message seen in swlog
229393	After configuring linkagg, ports are going in blocking state instead of forwarding.
229421	Maximum valid detection signature resistance in PSE conformance exceeds the acceptable range(26 to 3
229509	Missing multicast flows after ERP ring recovery and WTR expire
229680	Able to configure erp-ring in a non-metro device
229682	Expected Error is not thrown while configuring erp ring in non-metro device.
229705	DHCP issue FFP Resource exhaustion
229807	Not able to unconfigure ipv6 name server (dns6) .
230128	Traffic doesn’t egress through ERP ports, when the ingress port is associated to a default Vlan which
230173	Fan status is not shown properly while doing snmpget operation in "alaChasEntPhysFanTable" mib objec
230329	Unable to remove NNI association on the ports for a particular Ethernet-service svlan though that sv
230371	Error message thrown while configuring force yellow 802.1p.

230407	AOS generates the error message "Err inserting to Rules4" when apply the qos configuration.
230478	Error is not thrown when loopback-test is configured with invalid ports