Release Notes

OmniSwitch 6350/6450

Release 6.7.2.R02

These release notes accompany release 6.7.2.R02 software for the OmniSwitch 6350/6450 series of switches. The document provides important information on individual software and hardware features. Since much of the information in the release notes is not included in the hardware and software user manuals, it is important to read all sections of this document before installing new hardware or loading new software.

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

Table of Contents

Related Documentation

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

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

AOS 6.7.2.R02 Prerequisites

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
6.7.2.94.R02(GA)	6.6.3.259.R01	6

OmniSwitch 6450-24/P24/48/P48

Release	Uboot/Miniboot	CPLD
6.7.2.94.R02(GA)	6.6.3.259.R01	11

OmniSwitch 6450-U24

Release	Uboot/Miniboot	CPLD
6.7.2.94.R02(GA)	6.6.3.259.R01	6

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

Release	Uboot/Miniboot	CPLD
6.7.2.94.R02(GA)	6.6.4.54.R01	11

OmniSwitch 6450-P10S/U24S

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

OmniSwitch 6450-M/X Models

Release	Uboot/Miniboot	CPLD
6.7.2.94.R02(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
6.7.2.94.R02(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
6.7.2.94.R02(GA)	6.7.1.30.R04	4

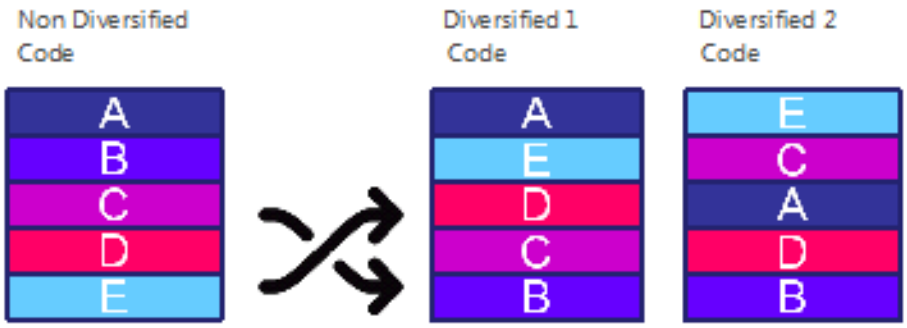
Note: Refer to the Upgrade Instructions section for upgrade instructions and additional information on Uboot/Miniboot and CPLD requirements.

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.R02	AOS 6.7.2.RX2	AOS 6.7.2.LX2

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.R02 New Hardware Supported

There is no new hardware in this release.

6.7.2.R02 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
AG Integration with UPAM for Guest Access and BYOD	OS6450	N/A
mDNS/SSDP (UPnP/DLNA) Relay Across L3 networks	OS6450	N/A
OmniAccess Stellar AP Integration with the OmniSwitch	OS6350/OS6450	N/A
AOS enhancement for dynamic WLAN vlan creation	OS6350/OS6450	N/A
LLDP for OmniAccess Stellar AP Web Management through WebView	OS6350/OS6450	N/A
LLDP AOS enhancements for Assignment of WLAN Parameters to the OmniAccess Stellar Access Points	OS6350/OS6450	N/A
OpenFlow - Packet modifcation OpenFlow - Order of actions OpenFlow - PUSH-VLAN OpenFlow - Apply actions	OS6450	N/A
Link Fault Propagation Enhancements	OS6350/OS6450	N/A
Command Implementation to Enable DDM traps	OS6350/OS6450	N/A
Control Directed Broadcasts	OS6350/OS6450	N/A
Topology Change Notice Logging	OS6350/OS6450	N/A
Clear Command for DHCP Snooping Violation Counters and Enhanced DHCP Snooping Troubleshooting	OS6350/OS6450	N/A
BYOD Enhancements for Supplicant and Non-supplicants	OS6350/OS6450	N/A
DHCP Snooping Binding Table	OS6350/OS6450	N/A

New Feature Descriptions

Access Guardian Integration with UPAM for Guest Access and BYOD
In previous releases Access Guardian worked with ClearPass for Guest Access and BYOD solutions. This enhancement integrates Access Guardian with the new Unified Policy Access Manager (UPAM) solution for Guest Access and BYOD.

mDNS/SSDP (UPnP/DLNA) Relay Across L3 Networks
The Zero configuration for mDNS and SSDP is developed to extend mDNS and SSDP across Layer 3.
The Zero configuration solution allows:

- mDNS and SSDP compatible devices to discover network services across IP subnet boundaries.
- To provide the solution that is unified across wire or wireless network.

The mDNS or SSDP packet handling across layer 3 supports three mode of operation:

- **Aruba Mode:** Supports mDNS or SSDP compatible devices with Aruba controller with GRE tunnel protocol type 0x0. This is the default mode of operation.
- **Gateway Mode:** Supports mDNS or SSDP compatible devices to discover network services across IP subnet boundaries or VLANs.
- **Standard Mode:** Supports mDNS or SSDP compatible devices with responder with GRE tunnel protocol type 0x6558.

Note. Only MDNS/SSDP over IPv4 is supported. MDNS tunnel is not supported**.**

In this Release 6.7.2.R02, the following CLI commands are deprecated.
UDP Relay:
mdns-relay enable. Instead, use *zeroconf mdns admin-state enable*.
mdns-relay tunnel - Deprecated
show mdns-relay config - Deprecated

IP:
The following commands will be removed from *boot.cfg*.
mdns-relay tunnel
show mdns-relay config

OmniAccess Stellar AP Integration with the OmniSwitch
Access Guardian provides the framework through which OmniAccess Stellar Access Points (APs) connected to an OmniSwitch are detected, learned, and managed. Wireless client traffic is then forwarded from the AP device to the OmniSwitch and onto the wired network. This integration provides a unified wireless over wired network access solution.
The OmniSwitch boots up with specific default configuration and operational settings that trigger the following process to detect, learn, and classify connected Stellar AP devices:

The switch and any Stellar AP device that is connected to an 802.1x port initially exchange Link Layer Detection Protocol (LLDP) TLV packets. Through this exchange of LLDP packets, the switch identifies and learns the device MAC address as an AP.
The detection of an AP device on an 802.1x port triggers the following actions that will automatically change the operational status of the specified options (the operational status overrides the configured status).
The transmission of LLDP Port VLAN ID and AP Location TLVs is operationally enabled on the UNP bridge port.
The trust tag status for the 802.1x port is operationally enabled.
The global status for dynamic VLAN configuration is operationally enabled for the switch.

Once the AP MAC address is detected and learned, a built-in LLDP UNP classification rule for access points classifies the AP device into a built-in default profile (defaultWLANProfile). The profile is associated with a VLAN into which the AP device is classified. This establishes a VLAN-port association (VPA) between the 802.1x port and profile VLAN on which the AP MAC address is learned and forwarded.

After the AP device connection is established, classified, and the management VLAN assigned, any of the following actions can occur:
The AP device sends DHCP packets.
The switch transmits LLDP packets to the AP device to advertise the management VLAN and AP location information.
The AP device starts to send client-tagged traffic (tagged with the SSID VLAN). The switch will trust the VLAN tag of the AP client traffic and attempt to assign the traffic to a switch VLAN that matches the tag of the client traffic. If a matching switch VLAN does not exist, then the switch will dynamically create the necessary VLAN on which to forward the AP client traffic.

MVRP will then propagate the VLAN configuration (AP management VLAN and any static or dynamic VLAN that was automatically tagged to carry AP client traffic) to adjoining switches in the network. This process creates specific VLAN domains through which the untagged AP management traffic and tagged wireless client traffic is forwarded on the wired network. The ports where client VLAN need to be propagated should be configured as MVRP enabled ports by the administrator.

The OmniSwitch detection and integration of OmniAccess Stellar APs results in a switch configuration that includes a management VLAN for the AP device and additional VLANs for wireless client-tagged traffic that is forwarded by the AP onto the wired network.

AOS Enhancement for Dynamic WLAN VLAN Creation
When Access point is detected, this enhancement supports the creation of dynamic WLAN VLAN from the tagged client packets on a port. However, to ensure the traffic to flow across the network, the created VLAN should get propagated through the network with the help of MVRP. Since MVRP supports only in flat mode, this solution works only in flat mode. The ports where client VLAN need to be propagated should be configured as MVRP enabled ports by the administrator.

LLDP for OmniAccess Stellar AP Web Management through WebView
The Cluster Virtual IP address to access the group of APs through OmniSwitch WebView can be automatically configured. The OmniSwitch acquires the Cluster Virtual IP address from the LLDP TLV received from the access points (AP).

All APs belonging to the same L2 domain and having the same cluster-ID are grouped into a single cluster. Each of these APs have their own unique IP address and the cluster is associated with a single virtual IP address for management. The cluster can be configured or managed through a Web interface by connecting to the cluster virtual IP address. The cluster virtual IP address is associated with the primary AP of the cluster. The OmniSwitch automatically configures the cluster virtual IP address from the received LLDP packets from the APs.

LLDP AOS Enhancements for Assignment of WLAN Parameters to OmniAccess Stellar APs
The OmniSwitch can advertise the WLAN management VLAN information and Access Point Location information of the APs connected to it using the LLDP TLVs.
The WLAN Management VLAN is transmitted to AP through LLDP using existing Port VLAN TLV. The WLAN management VLAN is locally maintained for each port on the switch.
The respective TLV must be enabled to advertise the information.

OpenFlow - Packet Modification
The concept of Groups and Buckets are used in OpenFlow in order to support a flow, which can execute more than one set of actions for a particular condition. This feature implementation enables the support of packet modification action for group type ALL. ‘debug openflow flow-id all’ displays the group flow in the form of buckets.

- This support is limited to OpenFlow 1.3.1 as Openflow 1.0 does not support groups.
- Group type ALL does not work when the packets are sent to non-primary Nis.

OpenFlow - Order of Actions
Multipart flow statistics messages and Multipart group descriptor messages show the list of actions associated with the flow and group respectively. This feature supports the actions in the multipart flow statistics reply messages and multipart group descriptor messages to be filled in the same order the actions were received in the flow mod message from the Openflow controller Management. This is applicable only to OpenFlow 1.3.1 version.

OpenFlow - PUSH-VLAN
This feature supports PUSH_VLAN action from Openflow controller. Newly pushed tags are always inserted as the outermost tag in the outermost valid location for that tag. When a new VLAN tag is pushed, it will be the outermost tag inserted, immediately after the Ethernet header and before other tags. This is applicable only to OpenFlow 1.3.1 version.

OpenFlow – Apply+ Actions
This feature supports APPLY_ACTION action from the Openflow controller. Instructions of type Apply-Actions applies the specific actions immediately, without any change to the Action Set. The actions are specified as an action list. The actions of an action list are executed in the order specified by the list, and are applied immediately to the packet.

- The execution of an action list starts with the first action in the list and each action is executed on the packet in sequence. The effect of those actions is cumulative, if the action list contains two Push VLAN actions, two VLAN headers are added to the packet.
- If the action list contains an output action, a copy of the packet is forwarded in its current state to the desired port.
- If an action list contains a sequence of actions that the switch cannot support in the specified order, the switch returns an error message.
- ‘debug openflow flow-id all’ displays the Apply-Action.
- Apply Actions with ACTION type GROUP is not supported.
- When there are more than one output port across stacks, packets destined to the ports in another stack will be dropped.
- This is applicable only to OpenFlow 1.3.1 version.

Link Fault Propagation Enhancement
The Link Fault Propagation (LFP) feature provides a mechanism to propagate a local interface failure into another local interface. In many scenarios, a set of ports provide connectivity to the network. If all these ports go down, the connectivity to the network is lost. However, the remote end remains unaware of this loss of connectivity and continues to send traffic that is unable to reach the network. To solve this problem, LFP does the following:
Monitors a group of interfaces (configured as source ports).
If all the source ports in the group go down, LFP waits a configured amount of time then shuts down another set of interfaces (configured as destination ports) that are associated with the same group.
When any one of the source ports comes back up, all of the destination ports are brought back up and network connectivity is restored.

Command Implementation to Enable DDM Traps
Digital Diagnostics Monitoring (DDM) allows the switch to monitor the status of a transceiver by reading the information contained on the transceiver's EEPROM. The transceiver can display Actual, Warning-Low, Warning-High, Alarm-Low and Alarm-High for the following:

- Temperature
- Supply Voltage

- Current
- Output Power
- Input Power

The transceiver is programmed with warning and alarm thresholds for predefined low and high conditions that can generate system events. If the actual value crosses the threshold value, trap can be generated. DDM trap can be enabled globally for DDM warning/alarm threshold violation using the ‘interfaces transceiver ddm trap enable’ command.

Control Directed Broadcasts
An IP directed broadcast is an IP datagram that has all zeros or all 1 in the host portion of the destination IP address. The Control Directed Broadcast supports subnet-directed broadcast, which is allowed only for a given/trusted set of source IP address and VLANs. This can be configured using ‘ip directed-broadcast controlled’ command. User needs to mention the trusted information such as source IP address, destination IP address, and VLAN information to broadcast the packets in a controlled manner. The specified information is considered as the trusted information to broadcast the packets received only from the defined source, and the remaining broadcast packets are dropped.

Topology Change Notice Logging
New ‘Last TC Rcvd Port’ field in the ‘show spantree’ command indicates the port or link aggregate that received the topology change for RSTP and MSTP protocols. This information is available on each switch and can be used to track down the source of the topology change within the network.

Additionally, this feature provides additional debugging information to help the customers to know the frequency and the magnitude of topology changes, which is happening in the ports for a given instance in the switch.

‘debug show spantree’ command can be used to view the STP BPDU statistics of all the available instances in the switch, or aggregated STP BPDU information and relative counter information for a particular instance. ‘debug stp reset cumulative-stats’ command can be used to the BPDU stats globally and based on the STP ID as well.

Clear Command for DHCP Snooping Violation Counters and Enhanced DHCP Snooping Troubleshooting
This enhancement can help with the troubleshooting for IPv4 DHCP snooping. The current debug logs available with swlog print many logs and are not always easy to interpret. This enhancement focuses on providing new CLI debug and show commands that can help troubleshoot the DHCP snooping feature more easily. There is also a clear command provided for DHCP snooping violation counters. The violation counters are existing from earlier releases.

BYOD Enhancements for Supplicant and Non-supplicants
The current BYOD solution uses the RADIUS attribute’s "session-timeout" for both supplicant and non supplicants. In this release, this functionality has been enhanced to be supported for supplicants. The user-name attribute from the radius server is already available for supplicants. In this release, this functionality has been enhanced to re-authenticate both supplicant and non-supplicant clients based on the session-timeout attribute from the authentication server. In case authentication server does not return session timeout attribute, Port level re-authentication will already happen for supplicants, this has been introduced for non-supplicants.
Show commands of 802.1x and aaa device have been enhanced to display the "username" information for non-supplicants clients. This already exist for supplicant clients in previous releases.

DHCP Snooping Binding Table

DHCP Snooping binding entries are stored in a file and displayed only in a table format.
In this release, a new command is added to display the binding table with option to filter static and dynamic entries. The DHCP Snooping binding entries can now be displayed in the snapshot format, so that the contents can be copied and pasted for reconfiguration as and when needed.

Unsupported Software Features

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

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

Unsupported CLI Commands

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

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

Software Feature	Unsupported CLI Commands
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]
UDP Relay	mdns-relay enable mdns-relay tunnel show mdns-relay config
IP	ip interface tunnel protocol gre

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	Webpage (displaying login confirmation and an option to logout) sent by UPAM radius server is not received by client, during BYOD non-supplicant CoA (change of authorization) operation. Client is first placed in an initial VLAN, as part of MAC authentication and is then redirected to a web portal hosted on UPAM radius server. Once the client is authenticated in redirect web portal, the following two actions happen: UPAM server sends a webpage confirming the login success along with an option to logout when user wants to. In OmniSwitch, client is moved to the new VLAN received as part of CoA and the client connected interface is toggled/reset to enable the client to get a new IP via DHCP in the new VLAN. Here, since the port reset happens quickly, client could not receive the URL page containing the logout option in time. This issue could be intermittent in some cases as its timing dependent. There is no impact on functional client traffic usage post login phase.However, the user would not be able to explicitly communicate the logout of BYOD session to UPAM server.	Client can either be removed manually removed by the administrator from "Remembered Devices" section in UPAM server or would be automatically removed post a timer expiry at UPAM server that can be configured.

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: http://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.R02 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.R02.
OmniSwitch 6350 models being upgraded to AOS 6.7.2.R02.

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.R02.

Version Requirements - Upgrading to AOS Release 6.7.2.R02

Version Requirements to Upgrade to AOS Release 6.7.2.R02			
	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,	6.7.2.94.R02 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	6.7.2.94.R02 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.R02

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.R02 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.R02 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.R02.

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.R02    15510736   Alcatel-Lucent Base Software
KFos.img         6.7.2.R02     2511585   Alcatel-Lucent OS
KFeni.img        6.7.2.R02     5083931   Alcatel-Lucent NI software
KFsecu.img       6.7.2.R02     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                : Micron Technology, Inc.,
Flash size                        : 134217728 bytes (128 MB),
RAM Manufacturer                  : Nanya Technology,
RAM size                          : 268435456 bytes (256 MB),
Miniboot Version                  : 6.6.4.157.R01,
Product ID Register               : 07
Hardware Revision Register        : 41
FPGA Revision Register            : 11
```

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 :      6.6.4.157.
```

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.R02 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.R02.
OmniSwitch 6350 models being downgraded from AOS 6.7.2.R02.

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.R02. 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
223191	Dying Gasp trap not seen randomly after the cold reboot
224568	Packet loss in adjacent switch (OS6450) connected to slave unit when the slave unit is powered OFF electrically.
225348	In OS6350, 100% CPU utilisation is seen, when accessing the switch via HTTP.
224136	In OS6450 stack, the serial number of backup power supply of secondary is not detected by OV2500.
226162	In OS6450, Stack unit hung and reboots after upgrading to 6.7.2.R01
228104	Issue on port 1/1 after upgrade to 6.7.2.R02. Issue identified as that port 1/1 is not programmed in VLAN bitmap. The port 1/1 is up and the PC connected to the device is not up and showing down. Interface is up. When the PC is connected to the other ports working fine.
226666	Samsung IP phone(SMT-i2205) connected to PoE port not working in OS6350.
203334	VLAN Stacking CPU is 100% in after a few NI takeover(s). The high CPU of NI1 is causing the other NI not be able to come up and join the stack.
223773	In OS6250-24, switch rebooted with boot type cold and Dying Gasp trap was not sent.
225264	OS6350 got crashed while setting temperature threshold in non-primary unit.
224568	2xOS6900 - packet loss in adjacent switch (OS6450) connected to slave unit when the slave unit is powered OFF electrically.
226230	“memPartAlloc: block too big - 13979 in partition 0x83b394." error is reported when issued "show ip helper dhcp-snooping binding".
225347	OS6450- Crashed with PMD relating to SSH
224923	UNP with number for auth-server-down policy creating boot.cfg.err
225421	"show stack split-protection helper status" show enabled in case helper status is disabled
215927	OS6450 - packets looping on LACP ports during few seconds after rebooting 6450, causing loop detection
226286	OS6450 crashed when executing aaa test-radius-server command
226302	In OS6450, "show aaa redirect-sever” displays an error.
226162	In OS6450, stack reboots after upgraded to 6.7.2.R01
226070	While configuring DNS through webview, following error is thrown “ Submission failed : Access denied! Authorization failed!.” But when the same is configured through CLI, it is getting reflected in WebView.
226041	After installing KB3212646 in Windows 2012 Radius server, fragmented EAP-TLS header are stripped by the switch to the client.
203334	In OS6450, vstkcmm CPU is 100% after a few NI takeover(s).
225974	802.1x mobile port display issue in OS6450.
223256	ip-ping SAA probe got stuck on OS6450
227304	Update Tx and Rx value for the CLI "show ip udp relay statistics" in documentation.
225411	OS6350-P24 POE issue on 1/9-16 ports
227498	"show ip interface dhcp-client" shows admin down while it should show admin up while no response from DHCP Server.
227228	OS6450 stacking module XNI-U2 is not hot swappable.
228027	Crash.pmd generated in NI-2 of OS6450 (stack of 3) and stack got split.
214831	Unable to reach the management IP address of OS6450 switches running 6.6.5.63.R02.
228091	Class 4 PD device does not receive the power as requested from the switch after enabling

	power-via-mdi tlv.
227556	SSP helper error message seen in NI-2 swlog after takeover
228223	Switch is not responding after executing the command “stacking interfaces 1/51 no l2 statistics".
228104	Issue on port 1/1 after upgrade to 6.7.2.80.R01
228300	MIB walk failing in snmpV1 & snmpV3.
226666	OS6350 PoE function is not working with Samsung IP phone(SMT-i2205)
228314	Modification to be done on our NT guide for OS6350 - Maximum number of clients per switching ASIC when IP source filtering is enabled.