Release Notes

OmniSwitch 6250/6350/6450

Release 6.7.1.R04

These release notes accompany release 6.7.1.R04 software for the OmniSwitch 6250/6350/6450 series of switches. The document provides important information on individual software and hardware features. Since much of the information in the release notes is not included in the hardware and software user manuals, it is important to read all sections of this document before installing new hardware or loading new software.

Table of Contents

Related Documentation **3**
AOS 6.7.1.R04 Prerequisites **4**
System Requirements **4**
Memory Requirements 4
Miniboot and FPGA Requirements for Existing Hardware 4
CodeGuardian **6**
6.7.1.R04 New Hardware Supported **7**
6.7.1.R04 New Software Features and Enhancements **8**
New Feature Descriptions 9
Unsupported Software Features **11**
Unsupported CLI Commands **11**
Open Problem Reports and Feature Exceptions **13**
Fixed Problem Reports **13**
Redundancy/ Hot Swap **16**
CMM (Primary Stack Module) and Power Redundancy Feature Exceptions 16
Stack Element Insert/Removal Exceptions 16
Hot Swap / Insert of 1G/10G Modules on OS6450 16
Technical Support **17**
Appendix A: AOS 6.7.1.R04 Upgrade Instructions **18**
OmniSwitch Upgrade Overview 18
Prerequisites 18
OmniSwitch Upgrade Requirements 18
Upgrading to AOS Release 6.7.1.R04 19
Summary of Upgrade Steps 19
Verifying the Upgrade 23
Remove the CPLD and Uboot/Miniboot Upgrade Files 24
Appendix B: AOS 6.7.1.R04 Downgrade Instructions **25**
OmniSwitch Downgrade Overview 25
Prerequisites 25
OmniSwitch Downgrade Requirements 25
Summary of Downgrade Steps 25
Verifying the Downgrade 26

Related Documentation

The release notes should be used in conjunction with the associated manuals as listed below.
User manuals can be downloaded at:
http://enterprise.alcatel-lucent.com/?dept=UserGuides&page=Portal

OmniSwitch 6250 Hardware Users Guide
Complete technical specifications and procedures for all OmniSwitch 6250 Series chassis, power supplies, and fans.

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 6250/6350/6450 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 6250/6350/6450 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 6250/6350/6450 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 6250/6350/6450 Transceivers Guide
Includes transceiver specifications and product compatibility information.

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

AOS 6.7.1.R04 Prerequisites

Please note the following important release specific information prior to upgrading or deploying this release. The information below covers important upgrade requirements, changes in AOS default behavior, and the deprecation of features.

- For a few seconds at the beginning of the boot up process random characters may be briefly displayed on the console of an OS6350. This is due to an initial baud rate mismatch. As soon as the bootrom is initialized the issue is automatically resolved.

System Requirements

Memory Requirements

The following are the requirements for the OmniSwitch 6250/6350/6450 Series Release 6.7.1.R04:

- OmniSwitch 6250/6350/6450 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 OS6250/6350/6450 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 6.7.1.R04 AOS software available from Service & Support.

OmniSwitch 6250 (All Models)

Release	Uboot/Miniboot	CPLD
6.7.1.76.R04(GA)	6.6.3.259.R01 6.6.4.158.R01 (optional – ships on all factory units)	12 14 (optional – ships on all factory units)
Note: The optional uboot/miniboot and CPLD upgrade fixes a known push button and LED issue and applies to existing OS6250 units, these versions will ship on all units from the factory. Refer to the Upgrade Instructions for additional information.		

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

Release	Uboot/Miniboot	CPLD
6.7.1.76.R04(GA)	6.6.3.259.R01	6

OmniSwitch 6450-24/P24/48/P48

Release	Uboot/Miniboot	CPLD
6.7.1.76.R04(GA)	6.6.3.259.R01	11

OmniSwitch 6450-U24

Release	Uboot/Miniboot	CPLD
6.7.1.76.R04(GA)	6.6.3.259.R01	6

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

Release	Uboot/Miniboot	CPLD
6.7.1.76.R04(GA)	6.6.4.54.R01	11

OmniSwitch 6450-P10S/U24S

Release	Uboot/Miniboot	CPLD
6.7.1.76.R04(GA)	6.6.5.41.R02	P10S - 4 U24S – 7

OmniSwitch 6450-M/X Models

Release	Uboot/Miniboot	CPLD
6.7.1.76.R04(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
6.7.1.76.R04(GA)	6.7.1.69.R01/6.7.1.103.R01 6.7.1.73.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
6.7.1.76.R04(GA)	6.7.1.73.R04	4

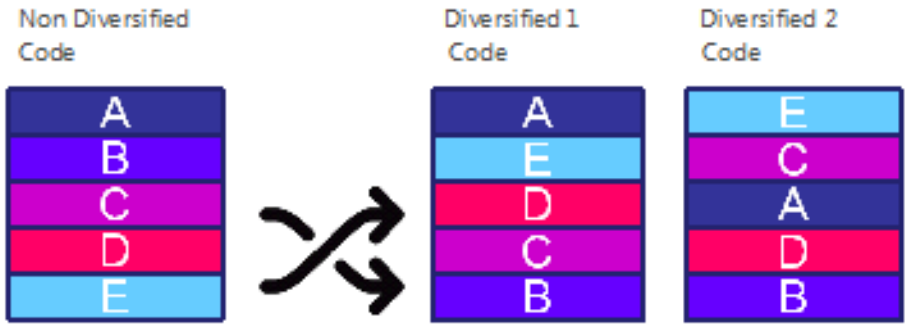
Note: Refer to the Upgrade Instructions section for upgrade instructions and additional information on Uboot/Miniboot and CPLD requirements.

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 5 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 6.7.1.R04	AOS 6.7.1.RX4	AOS 6.7.1.LX4

- X=Diversified image 1-5
- ALE will have 5 different diversified images per AOS release (R11 through R51)
- Our partner LGS will have 5 different diversified images per AOS release (L11 through L51)

6.7.1.R04 New Hardware Supported

OmniSwitch 6350-10

- Non-stackable
- 8 ports of 10/100/1000BaseT Ethernet
- 2 RJ-45/SFP combo interfaces supporting gigabit transceivers
- Fixed internal primary power supply
- No redundant power supply option

OmniSwitch 6350-P10

- Non-stackable
- 8 ports PoE+ (802.3af/at) 10/100/1000BaseT Ethernet
- 2 RJ-45/SFP combo interfaces supporting gigabit transceivers
- Fixed internal primary power supply
- No redundant power supply option
- 120W PoE power budget

SFP-10G-T
10-Gigabit copper transceiver supporting 10GBaseT with Cat 6a/7 cabling.

6.7.1.R04 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
6350 stacking support	OS6350-24/48 models	N/A
Common Criteria	All	N/A
CPE testhead accuracy	All	N/A
Writing directly to Certified directory	All	N/A
CLI Auto-completion	All	N/A
Oxo integration of 6350-10/P10	6350-10/P10	N/A
OAW-AP web management via WebView	All	N/A
NIS Enhancements - Masquerade RADIUS PSK - Password stored with SHA-224/256 or SHA-2 AES - SSH/SSL public and private key hashing with SHA-2 - DSA and RSA key over 2048 bits - AOS image integrity check function with SHA-2 - TLS 1.2 support - Manager only for log access/re-authentication needed - Process Self-Test Function	All	N/A

Feature Summary Table

New Feature Descriptions

OmniSwitch 6350 Stacking Support

Stacking of up to 4 units for 6350-24/48 models. The OS6350-24/48/P24/P48 models are designed to be stackable. These models have 4x1G uplink ports, two of which are capable of 5Gbps stacking. For OS6350-24/P24, ports 27 and 28 and for OS6350-48/P48, ports 49 and 50 are both uplink (1Gbps) and stacking capable (5Gbps) ports.

Common Criteria

The Common Criteria for Information Technology Security Evaluation (CC), and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Arrangement (CCRA), which ensures that:

- Products can be evaluated by competent and independent licensed laboratories so as to determine the fulfillment of particular security properties, to a certain extent or assurance
- Supporting documents, are used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying specific technologies.
- The certification of the security properties of an evaluated product can be issued by a number of Certificate Authorizing Schemes, with this certification being based on the result of their evaluation;

These certificates are recognized by all the signatories of the CCRA. The CC is the driving force for the widest available mutual recognition of secure IT products.

CPE Testhead Accuracy
In order to get more accurate throughput results for the CPE tests, work around (WA) timers is introduced to begin the packet count when the packet transfer reach the configured test rate.
WA timer drops the packets for the first 5 seconds as the initial packets would not have reached the configured rate. The actual test duration will be started on expiration of this WA timer. Hence the CPE tests provides the actual throughput value.

The WA timer is introduced for all the CPE test types – unidirectional, bidirectional, single test and group test.

Writing directory to Certified directory
In this new implementation, the upgrade procedure works in the "Certified" directly and modification of the configuration is reflected correctly in the configuration files.
When you upload a new image into the "Certified" directory and issue a "copy certified working" command, the system is fully synchronized including the running configuration.

CLI Auto completion
In this new implementation, the space key can be used for auto completion of the CLI command similar to the TAB key. If the space key is pressed auto-completion will complete the keyword. If an incorrect keyword is entered, pressing the space key will not remove the keyword whereas pressing the TAB key will remove the keyword while attempting auto-completion.

To enable CLI Auto completion, a new CLI is introduced; **session cli-auto-complete-space enable**.

Oxo Integration of 6350-10/P10
During the remote configuration download procedure the OmniSwitch sends the Vendor Class Identifier (VCI) in the DHCP discover/request packets. The VCI is sent as part of option-60 in "OmniSwitch-<moduleType>" format and is used by the OXO server to identify OmniSwitch DHCP requests. The following VCIs have been added to provide support for the OS6350-10/P10 models.

- OS6350-P10: OmniSwitch-OS6350-P10
- OS6350-C10: OmniSwitch-OS6350-10

OAW-AP web management integration with WebView

The OAW-APs can be managed from the OAW-AP web interface. The cluster of APs can be configured through a single interface.

The OAW-AP web interface can be accessed from the OmniSwitch web view page by clicking on the WLAN button under the Physical group. The WebView server on the switch redirects the URL to the AP (Virtual IP Address) URL on port 8080 from where the OAW-APs can be managed.

WebView on the switch must be aware of the Virtual Cluster IP and the IP addresses of the APs in order to re-direct to the OAW-AP web interface. To configure the virtual cluster IP address of the OAW- APs, a new CLI is introduced; **webview wlan cluster-virtual-ip** {virtual-ip-address-of-wlan-cluster}.

Authenticated Switch Access – Enhanced Mode (NIS-Phase2 and Phase3)

ASA Enhanced mode feature allows configuration of enhanced security restrictions to the OmniSwitch. This feature provides the following functionality:

- Improved password policies and lockout setting for the user.
- Option to configure user passwords with SHA1/SHA2 hash and AES encryption, saves the secret keys for external server authentication with AES encryption.
- Restricts access to the switch only for certain IP (configured as management station), bans the IPs permanently from accessing the switch on invalid authentication attempts for threshold number of times.
- Provides option to configure privileges for all access types.
- IP services will be aligned dynamically with AAA authentication configuration.
- Mandates authentication for viewing SWLOG data and accessing DSHELL with password protection.
- Provides option to verify the integrity of the images present in the switch.
- Restricts only one session per user.
- Self test performed during startup.

In 671 R04 release, the following additional support is provided in ASA enhanced mode:

- Option for password masking function to prohibit the disclosure while configuring user password, snmpv3 privacy password and AAA external server shared secret/password.
- Viewing of SSH public and SSH private key files on the terminal using ‘vi’ or ‘more’ commands is not allowed in the enhanced mode.
- RSA 2048 bit public key algorithm will be supported in enhanced mode in addition to existing DSA 1024 algorithm.
- AOS image integrity check function with SHA-2 (SHA256).
- Process Self-Test functional commands to view the major hardware and software process status.
- Support of TLS 1.2 version for only TLS connections.
- SWLOG data access is restricted through re-authentication, valid ASA credentials need to be provided to access SWLog content.

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	OS6250/6350/6450
DVMRP	OS6250/6350/6450
IS-IS	OS6250/6350/6450
Multicast Routing	OS6250/6350/6450
OSPF, OSPFv3	OS6250/6350/6450
PIM	OS6250/6350/6450
Traffic Anomaly Detection	OS6250/6350/6450
IPv6 Sec	OS6250/6350/6450
IP Tunnels (IPIP, GRE, IPv6)	OS6250/6350/6450
Server Load Balancing	OS6250/6350/6450
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

Software Feature	Unsupported CLI Commands
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.

QoS

PR	Description	Workaround
214111	TCAM entry allocation is not reflected in "show qos slice" output after configuring dynamic QoS applications. TCAM entries are not getting free after unconfiguring dynamic QoS applications, "show qos slice ingress".	There is no known workaround at this time.

System

PR	Description	Workaround
219745	IP phone sometimes reboots when enabling/disabling EEE on an IP phone connected interface.	There is no known workaround at this time.

Fixed Problem Reports

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

170696	SSH password attack using Hydra causes memory leak in AOS 6x
202984	Total number fans in OS6450 switches are mentioned incorrect in the Guide.
203985	FREAK vulnerability in Open SSL CVE-2015-0204
206331	CERT-IST/AV-2015.0452 Logjam vulnerability in Diffie-Hellman CVE-2015-4000
209959	CERT-IST/AV-2015.0793 Vulnerability in Open LDAP on Linux/Unix CVE-2015-6908
214062	6850E - DHCP issue during lease refresh with Wyse thin client
214423	Ipc pool depletion seen due to continuous ?show configuration snapshot? command and randomly show co
214774	Clients (switch) connected to Dlink router (DHCP server) does not get IP address
214818	6850E - inconsistent DHCP issue during lease refresh with Wyse thin client
215006	OS6450-P24 no response in SSH session
215547	6450-U24 - Crash of both unit of the stack
215720	OS6450: LAN power Stop command Cosmetic Issue
215927	6450 - packets looping on LACP ports during few seconds after rebooting 6450, causing loop detection
216226	6450 system uptime reset after 828.5 days
216595	SNMP walk skips the ports information from 32 to 48 on a OS6450P48 switch
216933	SNMP walk not working on 6450 with Error: OID not increasing
217490	Security advisory CERT-IST/AV-2016.0382 Vulnerabilities in Open SSL CVE-2016-2105, CVE-2016-2106, CVE
217750	Received packets are dropped when 2 instances of SAAs are running.
217769	Incorrect Mac movement display on OS6450.
217873	On verifying that when active route goes down and the next best in line route takes the place of the
217874	Crash.pmd got generated in NI-1 of OS6250 while running cvlan_insertion.mnl
217943	ARP Packets dropped by IPSF after MAC movement
218040	PoE Stopped working on some ports of OS6450-P10S
218085	OS6450: If Openflow action configured as NORMAL, switch is not working as expected.

218418	Logging in DUT failed on instances of multispawn telnet with access type console
218485	MemMon000.dmp file got generated in NI-2 of OS6250 while running rip.mnl
218589	OS6350 - stack of 3 (C48-C24-C24) got split while running ipms.mnl
218661	Ktrace, Crash & multiple MemMon.dmp is generated while takeover is performed in userprofile mnl &
218783	Continuous ?+++ hal_fdb_delete_shadow? messages seen in OS6450-U24 console.
218869	Stack Split without any external events
218877	OS6450 switch crash with PMD file and QoS task suspended.
218881	SAA Jitter/ RTT values & packet drop issue.
218889	Lack of entry in show ip helper dhcp-snooping port.
218988	OS6450: Query on SNMP
219049	[TYPE1] Match count is not getting incremented after takeover while setting LDAP application to Loop
219120	Unable to get the serial number of DAC/Optical fiber cable in the OS6450-P10
219212	NTP broadcast (255.255.255.255) are not flooded when NTP broadcast client is enabled
219370	NTP server config entry is sometimes not created while an entry is present in "show client ntp serve
219377	NTP broadcast client doesn't work on OS6450 ports 1/25-48
219462	4XOS6250 - Receiving power supply removed/inserted messages in switch logs
219547	3xOS6250 - primary unit crashed with following task suspended tCsCSMtask2, tCS_PRB, Vrrp.
219550	Clock is updated even if NTP client status is disabled
219551	Running configuration is not updated after "ntp client disable" is executed
219957	6450 NTP issue - Date is not updated
219978	Log missing when radius health check is enabled /disabled
220321	Flash synchronization failed on "reload working no rollback-timeout" in Stack of 8 OS6250 on running
220333	The switch displays error "?zBuffer too small-29 (CLI-mip_write_table)? when tried to apply a default
220346	IP phone which are classified in VOICE VLAN (By auth-server down policy) are getting changed to DATA
220352	Getting the message "NI out of resource unable to learn non supp 38:ea:a7:87:04:ec on ifIndex 3020"
220380	OS6450 got crashed after the telnet or ssh scripting
220393	Difference in the CPU reading between ?show health? and ?show health all cpu? outputs
220414	After reloading dut with default configurations ,DUT is not reachable and NI-2 in a stack of two is
220422	"show qos slice ingress" output show the negative value.
220440	OS6450 - SAA packet drop issue.
220466	Switch unable to synchronize with NTP server and getting the error "peer access denied, peer authentication.
220505	Scripts are getting timeout message while sending " bridge 10 protocol rstp" and hence DUT is not re
220588	?cli timed out ? Error is thrown while trying to view ?Show Configuration snapshot? through read-onl
220597	"reload all" CLI failed after "copy working certified flash-synchro" in Stack of 8 OS6450.
220600	ip service network-time is disabled while in "Authenticated Switch Access - Switch Mode Enhanced" is
220610	Ports are not going to the permanent shutdown state
220620	In OS6350 stack of 4, Boot.slot.cfg file is being modified/swapped between NIs
220622	Redundant whitespace in configuration of Radius Health Check between the status and enable
220630	Traffic drop is seen while testing RFC 2544 for Copper and fiber ports across NI

220698	Documentation change for qos default multicast disposition
220700	AOS 6.7.1.86.R03 - Certain CLI commands don't change "Running Configuration" synchronization state
220727	In OS6350 DUT reachability fails on enabling "bridge mode flat"
220824	Switch unable to synchronize with NTP server and getting the error "peer access denied, peer authentication.
220995	Configure DHCP Server Options 176 and 242 for VOIP Phones.
221002	Crash.pmd and Dmp files got generated in NI-2 of OS6350 while issuing takeover in NI-1

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.

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: 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 6.7.1.R04 Upgrade Instructions

OmniSwitch Upgrade Overview

This section documents the upgrade requirements for an OmniSwitch. These instructions apply to the following:

- OmniSwitch 6250 models being upgraded to AOS 6.7.1.R04.
- OmniSwitch 6450 models being upgraded to AOS 6.7.1.R04.
- OmniSwitch 6350 models being upgraded to AOS 6.7.1.R04.

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 6.7.1.R04.

Version Requirements – Upgrading to AOS Release 6.7.1.R04

Version Requirements to Upgrade to AOS Release 6.7.1.R04			
	AOS	**Uboot/Miniboot**	**CPLD**
6250-24/P24/8M/24M	6.7.1.76.R04 GA	6.6.3.259.R01 (minimum) 6.6.4.158.R01 (optional)	12 (minimum) 14 (optional)
6450-10/10L/P10/P10L	6.7.1.76.R04 GA	6.6.3.259.R01	6
6450-24/P24/48/P48	6.7.1.76.R04 GA	6.6.3.259.R01	11
6450-U24	6.7.1.76.R04 GA	6.6.3.259.R01	6
6450-24L/P24L/48L/P48L	6.7.1.76.R04 GA	6.6.4.54.R01	11
6450-P10S	6.7.1.76.R04 GA	6.6.5.41.R02	4
6450-U24S	6.7.1.76.R04 GA	6.6.5.41.R02	7
6450-10M	6.7.1.76.R04 GA	6.7.1.54.R02	6
6450-24X	6.7.1.76.R04 GA	6.7.1.54.R02	7
6450- 24XM,24X,P24X,P48X,	6.7.1.76.R04 GA	6.7.1.54.R02	11
6350-24/P24/48/P48	6.7.1.76.R04 GA	6.7.1.69.R01/6.7.1.103.R01 (minimum) 6.7.1.73.R04 (optional)	12 (minimum) 16 (optional)
6350-10/P10	6.7.1.76.R04 GA	6.7.1.73.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.

- If an OS6250 is currently running the minimum versions listed above, then Uboot/Miniboot and CPLD upgrades are not required. However, CPLD 14 and Uboot/Miniboot 6.6.4.158.R01 fixed a known push button and LED issue (PR 176235). If you have an OS6250 that requires these fixes then upgrading both the Uboot/Miniboot and CPLD to the versions listed is required.
- If an OS6250 is already running AOS Release 6.6.3.R01 then the Uboot/Miniboot and CPLD versions should already be at the minimum versions listed above.
- If an OS6250 is running an AOS Release prior to 6.6.3.R01 the Uboot/Miniboot and CPLD will need to be upgraded. If an upgrade is required it is recommended to upgrade to the latest available versions.
- The 6.7.1.73.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 6.7.1.R04

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 6.7.1.R04 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 6.7.1.R04 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
   - AOS Files (6250/6450) – 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 6.7.1.R04.

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      6.7.1.R04     15510736   Alcatel-Lucent Base Software
KFos.img        6.7.1.R04     2511585    Alcatel-Lucent OS
KFeni.img       6.7.1.R04     5083931    Alcatel-Lucent NI software
KFsecu.img      6.7.1.R04     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:                 OS6250-24,
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 6.7.1.R04 Downgrade Instructions

OmniSwitch Downgrade Overview

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

- OmniSwitch 6250 models being downgraded from AOS 6.7.1.R04.
- OmniSwitch 6450 models being downgraded from AOS 6.7.1.R04.
  OmniSwitch 6350 models being downgraded from AOS 6.7.1.R04.

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

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 6.7.1.R04. 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
```