Release Notes

OmniSwitch 6250/6350/6450

Release 6.7.1.R02

These release notes accompany release 6.7.1.R02 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

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.R02 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.R02:

- OmniSwitch 6250/6350/6450 Series Release 6.7.1.R02 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.R02 AOS software available from Service & Support.

OmniSwitch 6250 (All Models)

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

OmniSwitch 6450-24/P24/48/P48

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

OmniSwitch 6450-U24

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

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

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

OmniSwitch 6450-P10S/U24S

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

OmniSwitch 6450-M/X Models

Release	Uboot/Miniboot	CPLD
6.7.1.54.R02(GA)	6.6.5.137.R02	10M – 6 24X/24XM/P24X/48X/P48X – 11 U24SXM/U24X - 7

OmniSwitch 6350-24/P24/48/P48

Release	Uboot/Miniboot	CPLD
6.7.1.54.R02(GA)	6.7.1.69.R01/6.7.1.103.R01	12

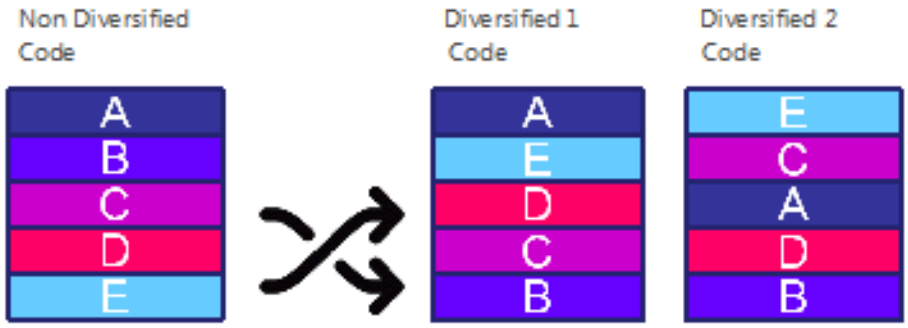
Note: Refer to the Upgrade Instructions section for upgrade instructions and additional information on Uboot/Miniboot and CPLD requirements.

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.R02	AOS 6.7.1.RX2	AOS 6.7.1.LX2

- 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.R02 New Hardware Supported

New Metro and 10-Gigabit Switches

The following new models are being introduced in this release.

- The new 'M' models support the same functionality as the non-'M' models with the addition of Metro feature support being enabled by default.
- The new 'X' models support the same functionality as the non-'X' models with the addition of 10-Gigabit capability being enabled by default.
- Please note that for stacking purposes 'M' models can be stacked with other 'M' models or with non-'M' models that have the Metro license installed.

OS6450-10M

The OS6450-10M supports the following:

- 8 RJ-45 10/100/1000 ports
- 2 SFP/RJ-45 Combo ports
- 2 non-combo SFP ports
- Internal AC power supply
- Supports the same features as the OS6450-10 plus Metro feature support enabled by default.

OmniSwitch 6450-24X

The OS6450-24X supports the following:

- 24 RJ-45 10/100/1000 ports
- 2 non-combo SFP+ ports
- 1 expansion slot for optional stacking or uplink modules
- Internal AC power supply
- Optional slide-in 90W AC or DC redundant power supply
- Supports the same features as OS6450-24 plus 10-Gigabit capability enabled by default.

OmniSwitch 6450-24XM

The OS6450-24XM supports the following:

- 24 RJ-45 10/100/1000 ports
- 2 non-combo SFP+ ports
- 1 expansion slot for optional stacking or uplink modules
- Internal AC power supply
- Optional slide-in 90W AC or DC redundant power supply
- Supports the same features as OS6450-24 plus 10-Gigabit capability and Metro feature support enabled by default.

OmniSwitch 6450-P24X
The OS6450-P24X supports the following:

- 24 RJ-45 10/100/1000 802.3at PoE ports
- 2 non-combo SFP+ ports
- 1 expansion slot for optional stacking or uplink modules
- Internal AC power supply
- Optional slide-in 550W AC power supply
- Supports the same features as OS6450-P24 plus 10-Gigabit capability enabled by default.

OmniSwitch 6450-48X
The OS6450-48X supports the following:

- 48 RJ-45 10/100/1000 ports
- 2 non-combo SFP+ ports
- 1 expansion slot for optional stacking or uplink modules
- Internal AC power supply
- Optional slide-in 90W AC or DC redundant power supply
- Supports the same features as OS6450-48 plus 10-Gigabit capability enabled by default.

OmniSwitch 6450-P48X
The OS6450-P48X supports the following:

- 48 RJ-45 10/100/1000 802.3at PoE ports
- 2 non-combo SFP+ ports
- 1 expansion slot for optional stacking or uplink modules
- Internal AC power supply
- Optional slide-in 900W AC power supply
- Supports the same features as OS6450-P48 plus 10-Gigabit capability enabled by default.

OmniSwitch 6450-U24SXM
The OS6450-U24XSM supports the following:

- 22 SFP ports
- 2 SFP/RJ-45 combo ports
- 2 non-combo SFP+ ports
- 1 expansion slot for optional stacking or uplink modules
- Internal AC power supply
- Optional slide-in 90W AC or DC power supply
- RFC 1588v2 Precision Time Protocol (PTP) – End-to-end Transparent Clocking.
- Supports the same features as OS6450-U24S plus 10-Gigabit capability and Metro feature support enabled by default.

OmniSwitch 6450-U24X
The OS6450-U24XSM supports the following:

- 22 SFP ports
- 2 SFP/RJ-45 combo ports
- 2 non-combo SFP+ ports
- 1 expansion slot for optional stacking or uplink modules
- Internal AC power supply
- Optional slide-in 90W AC or DC power supply
- Supports the same features as the OS6450-U24 plus 10-Gigabit capability enabled by default.

6.7.1.R02 New Software Features and Enhancements

The following software features are new with the 6.7.1.R02 release, subject to the feature exceptions and problem reports described later in these release notes:

Feature	Platform	License
Ethernet OAM Remote Fault Propogation	OS6250/6350/6450	Metro
C-VLAN Insertion with Loopback0 Interface	OS6250/6350/6450	Metro
Multicast Dynamic Control	OS6250/6350/6450	N/A
Network Address Translation	OS6250/6350/6450	N/A
Two-Way Active Measurement Protocol (TWAMP)	OS6250/6350/6450	N/A
NIS Phase 1&2	OS6250/6350/6450	N/A
Critical voice VLAN when RADIUS down Phase 1 / Phase 2	OS6250/6350/6450	N/A
ISF – Support for exceptional Subnets	OS6250/6350/6450	N/A
Logging mechanism for traffic from ineligible clients in ISF enabled network	OS6250/6350/6450	
SSH Port	OS6250/6350/6450	N/A
BYOD Whitelist	OS6250/6350/6450	N/A
NTP Swlog Enhancement	OS6250/6350/6450	N/A
NTP Traps	OS6250/6350/6450	N/A
SNMVP3 dual password	OS6250/6350/6450	N/A
Weak Webview Session ID and the CSRF	OS6250/6350/6450	N/A
DHCP Snooping Global Mode Enhancement	OS6250/6350/6450	N/A
Increased number of Telnet, Syslog, NTP	OS6250/6350/6450	N/A
Increased number of TACACS server (4+local)	OS6250/6350/6450	N/A
DHCP snooping binding table for IP source filtering enabled ports	OS6250/6350/6450	N/A
Tri Speed (10/100/1000) SFP Support on OS6450 U24	OS6450	N/A
OS6350 Fan Speed	OS6350	N/A
Config File Management	OS6250/6350/6450	N/A
Monitoring interstack connection	OS6250/6350/6450	N/A

Feature Summary Table

Chassis / System

Ethernet OAM Remote Fault Propogation

Remote Fault propagation (RFP) propagates connectivity fault events into the interface that is attached to a MEP. Once the fault is detected for a MEP, the MEP's interface is shutdown. Unlike other violation mechanisms that keep the link up when an interface is shutdown, this fault propagation mechanism will effectively shutdown the link so that the remote end of the interface also detects a link down. The feature is configurable on per MEP basis and is supported only for UP MEPs. Remote Fault Propagation detects only loss of connectivity and remote MAC defect.

CVLAN Insertion with Loopback0 Interface

This feature converts the untagged frames into double tagged frames in the provider network so as to make ICMP between the endpoints work. The frames should always be untagged on the customer network. This will be ensured using double push and double pop operations. The double push will happen on the UNI port in order to push the configured CVLAN as well as the SVLAN in the egressing packet. The double pop must be applied on the NNI port in order to remove both the tags when the packet is egressed from the UNI.

Multicast Dynamic Control

In AOS, IPv4 and IPv6 multicast protocols are by default always copied to the CPU. The high CPU usually impacts the normal operations of the OmniSwitch protocols such as LACP, ERP.

In order to resolve this high CPU issue, this feature is introduced to control the processing of the IPv4 multicast protocols. The processing of all IPv6 multicast protocols is globally controlled by the presence of an IPv6 Interface.

- No IPv6 interface configured - All protocols in the ff02:0::/32 range are transparently forwarded and not copied to CPU.
- At least one IPv6 interface configured - All protocol packets in the ff02:0::/32 range are copied to CPU on all vlans irrespective on which vlan IPV6 interface is enabled.

MLD packets are copied to CPU based on the global ipms status. When IPMS is globally enabled, MLD packets are copied to CPU. When IPMS is globally disabled, MLD packets are not copied to CPU.

Network Address Translation

Network Address Translation (NAT) is a feature that allows an organization's IP network to appear from the outside to use different IP address space than what it is actually using. Thus, NAT allows an organization which uses private addresses (local addresses), and therefore not accessible through the Internet routing tables, to connect to the Internet by translating those addresses into globally routable address space (public addresses) which are accessible from Internet. NAT also allows organizations to launch readdressing strategies where the changes in the local IP networks are minimal. NAT is described in RFC 1631.

Network Address Translation (NAT) is used for rewriting a source or destination IP address to another address. A single address may be rewritten, or an entire subnet or list of IP addresses may be rewritten to a group of addresses.

TWAMP

The Two-Way Active Measurement Protocol (TWAMP) is an open protocol for measurement of two-way metrics between any two network devices which supports the TWAMP protocol. TWAMP provides a standard technique to measure network performance metrics. Unlike ICMP Ping, TWAMP also measures round trip delay/Jitter apart from the RTT. TWAMP does not require clock synchronization between the two devices.

Following are the functionality provided by the feature.

AOS software implements TWAMP server/reflector functionality specified in RFC 5357. Supports establishing TCP control session between TWAMP client/controller and the AOS switch that would function as TWAMP Server/Reflector Supports SERVWAIT functionality in case of TCP control session failure. The SERVWAIT time value can be configured by the user. Supports the following commands from the TWAMP client:

a) Request-TW-Session
b) Start-Sessions
c) Stop-Sessions

TWAMP server transmits a test packet to the Session-Sender in response to every received packet. AOS software also implements a REFWAIT timer functionality to monitor inactivity in test sessions. Loopback0 IP address configured on the switch will be taken as the IP address of the TWAMP Server.

Authenticated Switch Access – Enhanced Mode (NIS-Phase2)

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.
- Saves SNMP 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, aligns IP services dynamically with AAA authentication configuration.
- Restricts reload and firmware update only to console.
- 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.

Critical Voice VLAN Phase 1 & 2

Existing behavior is when the radius server becomes unresponsive or unreachable an IP phone getting authenticated will be moved to default vlan, which need not be the Voice vlan. This may cause phones to not connect. As an enhancement, current auth-server down feature is leveraged to support the critical voice vlan. A new policy is introduced to support one “Voice” User Network-Profile.
With this enhancement, when RADIUS authentication fails for server not responsive, the device mac-address is checked against the LLDP database. If it is deemed to be an IP Phone, mac-address is learned and classified in the configured “Voice-user-network-profile”. If no such voice profile is configured, then it is classified as that of a non-IP phone device as below.
If the mac-address is not an IP Phone, the normal policy is enforced. In the normal policy, if user-network profile is configured, mac-address is learned and classified in the respective profile. If user-network profile is not configured, mac-address is blocked and learned as filtering

Phase 2 - The feature provides the functionality to test the reachability of RADIUS server from the AOS Switch by enabling server polling, which polls all the configured RADIUS servers periodically to obtain the server status (Up/Down).

An SNMP trap would be raised on the first polling cycle for the RADIUS servers configured. And on the subsequent polling cycles, an SNMP trap would be raised only if the server status gets changed from up to down and from down to up. Events would be logged in both these scenarios. If there are four radius servers configured, only four SNMP trap and SWlogs entries are generated, until the status of the server is changed. When the switch detects that server is unreachable during authentication, server status would be updated and SNMP trap generated only after the interval period. ‘show aaa server’ is enhanced to verify the reachability of the configured radius server.

ISF – Support for exceptional subnets

IP Source Filtering Drop-Log (ISF) feature enables the user to see the packets getting dropped by IP Source Filter entries. When ISF (ip helper dhcp-snooping ip-source-filter) is enabled on a port or VLAN, it restricts all

the IP traffic on that port except the DHCP traffic and the traffic from the client, whose binding entry exists on that port. With ISF drop log feature, whenever a packet is dropped by ISF drop entry in the hardware, drops are logged in QoS log, which are displayed in 'show qos log' command. This will enable the user to know which port/MAC/IP was dropped.

ISF drop logging is enabled by default. Hence, the packets that are getting dropped due to ISF drop rule are logged. 64 packets are logged per second.

Logging Mechanism for traffic from in-eligible clients in ISF enabled network
This feature enables the user to see the packets getting dropped by IP-source-filter entries. Currently when ISF(ip-source-filter) is enabled on a port, it restricts all the IP-traffic on that port except the Dhcp traffic & the traffic from the client, whose binding entry exists on that port. But there is no way a customer/user can come to know which port/MAC/IP was dropped. This might help them in isolating the problem area/spoof attacks etc.
ISF Drop Log feature works in such a way that whenever a packet is dropped by ISF drop entry in hardware, drops will be logged in qos log which can be seen via "show qos log" command

SSH port
In the existing implementation, AOS uses the default SSH TCP port (port 22) to establish an SSH session.
With the new implementation, the user can specify the TCP port number to be used for SSH session. The TCP port numbers can be either default port 22 or port numbers in the range 1025 - 65535. The configured TCP port number will be saved in the switch file /flash/network/sshConfig.cfg. In order to use the configured port number while establishing the SSH session, the switch must be rebooted. While the switch boots up, if the file "/flash/network/sshConfig.cfg" exists, it will be parsed to read the TCP port number that should be used to establish the SSH session, otherwise the default SSH TCP port shall be used.

Well-known reserved TCP port numbers (1-1024) and the IP ports which are internally used cannot be configured for the SSH TCP port.

BYOD Whitelist
Implementation of BYOD White-list IP address to bypass the redirect server which was provided by CPPM server. Maximum of 8 IP addresses can be configured to be redirected.

NTP SWLOG Enhancement

An swlog appid has been added for NTP.

NTP Traps Enhancement

AOS provides support for configuring NTP in client mode. NTP client will select a synchronization peer from among the configured NTP servers for performing clock synchronization. This enhancement will send an SNMP trap for the two scenarios below:

- The active NTP synchronization peer server changes.

- No active/reachable NTP server from among the configured NTP servers

SNMPv3 Dual Password

The existing AOS implementation supports SNMPv3 users with both hashing and encryption such as SHA+DES/MD5+DES/SHA+AES. However, in the existing implementation only one password is supported which is used for both authentication and encryption. This enhancement is to provide support for separate Auth Key and Priv Key. To support two different passwords, a new option priv-password has been added to the existing user creation CLI.

Weak Webview Session ID
Increased Session ID strength in web Interface to prevent session guessing attacks to address CVE-2015-2804.

DHCP Snooping Global Mode Enhancement
When DHCP snooping is globally enabled, the DHCP packets with unicast MAC and unicast IP are forwarded based on the MAC entry information previously cached. Hence, the packets that are received on the DHCP snooping switch in client VLAN will not be dropped as there is a MAC present in the DHCP snooping table.

Hence, when globaluturn is enabled on the switch the binding table will not be built for the unicast BOOTP packets sent on the trusted ports. So the binding table entry is not modified when the DHCP packet is relayed to the switch from the relay agent and the DHCP server packets are not dropped when received on the client VLAN.

There are four setting option for the global mode:

- **default**: Default DHCP snooping functionality is followed. Only the source packets are trapped to the CPU.
- **globaluturn**: Disable DHCP binding entry on a trusted port. The binding table will not be built for the unicast BOOTP packets sent on the trusted ports.
- **hardware**: The packets sent with source port 67 and destination port 67 will not be trapped to the CPU during DHCP snooping.
- **software**: The DHCP packets with 67/67 pair is trapped to the CPU in addition to 67/68 and 68/67.

Increased number of Telnet/ Syslog & NTP
This enhancement has increased the number increased of telnet sessions from 4 to 6, no of syslog servers increased from 3 to 12 and no of NTP servers increased from 3 to 12

Increased number of TACACs Servers
A maximum of up to 5 servers can be specified for authentication and accounting. The total number of servers that can be configured on the switch would remain the same (30).

DHCP snooping binding table for IP source filtering enabled ports
The feature enhances the current show CLI “show ip helper dhcp-snooping ip-source-filter” to display the binding table entry for the ip-source filtering enabled ports. An additional option “binding” parameter is introduced in the show command to display the binding table in the show output.

Tri Speed (10/100/1000) SFP Support on OS6450 U24
The 6450-U24(S) now supports 10/100/1000 mbps on user ports (1-22), SFP+ ports support 1G only. Not supported on combo ports.

OmniSwitch 6350 Fan Speed
Modified default ambient fan speed settings and a modified fan frequency have been implemented in this release to help reduce fan noise and eliminate the high pitch sound on the OS6350-P24/48/P48 models.

Config File Management

The configuration file management feature modifies the configuration file label corresponding to the directory it resides, without affecting any functionality. Earlier when configuration file was retrieved either from the working or certified directories of OmniSwitch, the file had the same label as in old directory in the beginning of file. So after retrieval, it was difficult to find the source directory of the configuration file.

The mechanism of existing configuration file management system:
1. While performing certify and/or synchronization or restoration process in OmniSwitch, the configuration file of the source directory will be copied to the destination directory based on the below conditions.
a) If the configuration file does not exist in the destination directory.
b) The file exists, but differs in size and/or time stamp.

2. If any of the above condition is true, the configuration file will be copied to the destination directory and the timestamp of source directory configuration file will be re-applied on the copied configuration file in destination directory.

After the source configuration file contents are copied to destination configuration file, the label in destination configuration file will be modified and the time stamp of the source configuration file will be reapplied.

Monitoring interstack connection
This function provides the ability for the user to monitor the status, statistics, and counters of the stacking links (if the product is stackable) in addition to normal user interfaces using the below CLI Commands:

- show stacking interfaces
- show stacking interfaces status
- show stacking interfaces counters
- show stacking interfaces counters errors

A CLI command to clear the L2 statistics for the stacking ports is also introduced.
- stacking interfaces <slot|slot/port> no l2 statistics

Dying Gasp Enhancment
The Power Supply Type field in the Dying Gasp trap has been updated to add an additional value (3). This value indicates that the switch has rebooted due to a software reload.

Warm/Cold Start Indication
The Warm / Cold Start traps have been enhanced so that a Warm start trap will be sent for all cases where the reboot was initiated by the AOS software, other types of reboots such as a power cycle will be considered Cold starts. Additionally, a trap will be sent for a reboot of any unit in a stack with the exception of unit(s) in pass-through mode.

PoE Monitoring and Reset
An AOS update has been incorporated to automatically reset the PoE functionality after it has been shutdown due to an in rush current. This removes the need for a manual PoE reset or a system reboot. The PoE reset will reboot all the PDs connected to the switch. A log message will be displayed on the console as well as the switch logs stating that a PoE reset has occurred.

NTP – DNS Lookup (PR 203888/188377)
When the switch reboots, the DNS resolution fails since the interfaces of the switch are not yet up causing the DNS server to be unreachable. A workaround is provided which bypasses the host name look up and instead writes the host IP address itself to the boot.cfg file. There is then no need to look up the IP address of the NTP server during the next reload of the switch. To enable this workaround the flag "ntpSkipDNSLookUp" should be set to "1". This can be done for subsequent reboots by adding the line "debug set ntpSkipDNSLookUp 1" to the AlcatelDebug.cfg file.

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
CPE Testhead	OS6350
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
Stacking	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

Software Feature	Unsupported CLI Commands
	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 Alcatel-Lucent Technical 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
213546	TCAM entry is not getting freed after removing policy rules. When removing the last added policy rule it does not reflect in the 'show qos slice ingress' command.	Remove the policy rule along with another rule and add the rule back again. It will update properly in the show command.
214554	Error message: "+++ *hal_qos_setup_antispoofing 731: bad ifindex 5*" is displayed on the console after a takeover. This issue occurs during takeover,when IP spoofing is enabled and multiple interfaces are configured across NI.	There is no known workaround. This is a display issue only and has no functional impact.
214693 215038	An error similar to "+++ hal_pcl_alloc_entry" or "+++ hal_qos_install_list" may be displayed when Tcam is oversubscribed.	There is no known workaround at this time.

Security

PR	Description	Workaround
215147	All switch-access management-stations in Network Information Service (NIS) are not shown in session configuration webpage.	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.

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: esd.support@alcatel-lucent.com

Internet: Customers with Alcatel-Lucent service agreements may open cases 24 hours a day via Alcatel-Lucent's support web page at: service.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.R02 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.R02.
- OmniSwitch 6450 models being upgraded to AOS 6.7.1.R02.
- OmniSwitch 6350 models being upgraded to AOS 6.7.1.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 6.7.1.R02.

Version Requirements – Upgrading to AOS Release 6.7.1.R02

Version Requirements to Upgrade to AOS Release 6.7.1.R02			
	AOS	**Uboot/Miniboot**	**CPLD**
6250-24/P24/8M/24M	6.7.1.54 R02 GA	6.6.3.259.R01 (minimum) 6.6.4.158.R01 (optional)	12 (minimum) 14 (optional)
6450-10/10L/P10/P10L 6450-24/P24/48/P48 6450-U24 6450-24L/P24L/48L/P48L	6.7.1.54.R02 GA 6.7.1.54.R02 GA 6.7.1.54.R02 GA 6.7.1.54.R02 GA	6.6.3.259.R01 6.6.3.259.R01 6.6.3.259.R01 6.6.4.54.R01	6 11 6 11
6350-24/P24/48/P48	6.7.1.54.R02 GA	6.7.1.69.R01 6.7.1.103.R01	12
• 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.

Upgrading to AOS Release 6.7.1.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 6.7.1.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 6.7.1.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 6.7.1.R02 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 6.7.1.R02 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 6.7.1.R02 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.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 to 6.7.1.R02, 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.R02    15510736  Alcatel-Lucent Base Software
KFos.img         6.7.1.R02    2511585   Alcatel-Lucent OS
KFeni.img        6.7.1.R02     5083931  Alcatel-Lucent NI software
KFsecu.img       6.7.1.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          : 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.R01,
  POE SW Version :            n/a
```

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.R02 Downgrade Instructions

OmniSwitch Downgrade Overview

This section documents the downgrade requirements for OmniSwitch 6250 and OmniSwitch 6450 Models. These instructions apply to the following:

- OmniSwitch 6250 models being downgraded from AOS 6.7.1.R02.
- OmniSwitch 6450 models being downgraded from AOS 6.7.1.R02.
  OmniSwitch 6350 models being downgraded from AOS 6.7.1.R02.

Note: The OmniSwitch 6350 requires a minimum of AOS Release 6.7.1.R01 and cannot be downgraded to any 6.6.X 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 6.7.1.R02 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.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
```