Release Notes

OmniSwitch 6250/6450

RELEASE 6.6.5.R02

This release notes accompany release 6.6.5.R02 software for the OmniSwitch 6250/6450 Metro, Enterprise, and Small Cell models. 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 that you read all sections of this document before installing new hardware or loading new software.

Alcatel-Lucent proprietary and confidential.
Copyright © 2015. All rights reserved.

Table of Contents

Related Documentation

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

OmniSwitch 6250 Getting Started Guide
Describes the hardware and software procedures for getting an OmniSwitch 6250 Series switch up and running.

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

OmniSwitch 6450 Getting Started Guide
Describes the hardware and software procedures for getting an OmniSwitch 6450 Series switch up and running.

OmniSwitch 6450 Hardware Users Guide
Complete technical specifications and procedures for all OmniSwitch 6450 Series chassis, power supplies, and fans.

OmniSwitch 6250/6450 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 6250/6450 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 6250/6450 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 6250/6450 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.

System Requirements

Memory Requirements

The following are the requirements for the OmniSwitch 6250/6450 Series Release 6.6.5.R02:

- OmniSwitch 6250/6450 Series Release 6.6.5.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 and OS6450 models, except where otherwise noted. Switches running the minimum versions, as listed below; do not require any miniboot or FPGA upgrade.

Switches not running the minimum version required should be upgraded to the latest Uboot/Miniboot or FPGA that is available with the 6.6.5.R02 AOS software available from Service & Support.

OmniSwitch 6250 (All Models)

Release	Uboot/Miniboot	CPLD
6.6.5.63.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
6.6.5.63.R02 (GA)	6.6.3.259.R01	6

OmniSwitch 6450-24/P24/48/P48

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

OmniSwitch 6450-U24

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

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

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

OmniSwitch 6450-P10S/U24S

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

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

6.6.5 New Hardware Supported

New Small Cell Switches

Service Providers are deploying Small Cell solutions to improve coverage and capacity beyond the macro cell towers. Small cells are being developed to be multi-standard compliant (WiFi, 3G and 4G). These new small cell OmniSwitches support the two critical requirements for Small Cells that is higher PoE capability and support of Precision Time Protocol (PTP) for 4G deployments.

OS6450-P10S
The OmniSwitch 6450-P10S is a Gigabit, Power Over Ethernet, non-stackable LAN switch with support for the following:

- 8 RJ-45 10/100/1000 BaseT PoE ports (all ports support 802.3at)
- Ports 1-4 capable of 75 watts of PoE (4 pair) – Compliant with the PoE portion of the Power over HD Base-T (PoH) standard.
- Ports 5-8 capable of 30 watts of PoE (802.3at)
- 2 fixed SFP+ ports used for uplinks
- Internal AC power supply supporting a 280W PoE power budget
- Supports IEEE 1588 v2 Precision Time Protocol (PTP) – End-to-End Transparent Clocking
- Supports all the same software features as the OS6450-P10.

OmniSwitch 6450-U24S
The OmniSwitch 6450-U24S is a 10-Gigabit, Gigabit and Fast Ethernet stackable LAN switch with support for the following:

- 22 SFP ports
- 2 SFP/RJ-45 combo ports
- 2 fixed 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 RFC 1588 v2 Precision Time Protocol (PTP) – End-to-End Transparent Clocking
- Supports all the same software features as the OS6450-U24.

Note: The SFP+ ports support 1G speed by default and can be upgraded to support 10G with the OS6450-SW-PERF Performance License. This license is not required for the optional OS6450-XNI-U2 plug-in module.

Note: The OmniSwitch 6450-U24S does not support stacking when PTP is enabled.

Transceivers

SFP-GIG-T
This transceiver now supports "triple speed" (10/100/1000Mbps) on the OS6450-U24.

6.6.5 New Software Features and Enhancements

The following software features are new with the 6.6.5.R02 release, subject to the feature exceptions and problem reports described later in these release notes:

Feature	Platform	License
Chassis / System		
6450 Fan speed	OS6450-U24	
PoE Link layer classification	OS6250/6450	
Stack Split Protection	OS6250/6450	
RFC 1588 v2 – Precision Time Protocol	OS6450 – S Models	
Layer 2		
MVRP	OS6250/6450	
Layer 3		
Increase ARP table size	OS6250/6450	
Static route to directly connected subnet	OS6250/6450	
IPv6 Phase 2 Logo	OS6250/6450	
Management		
OpenFlow	OS6250/6450	
CPU Protection	OS6250/6450	
Metro		
Non-GBPT SW mac-tunnel uni-profile	OS6250/6450	Metro
Hybrid mode with Q in Q and 802.1a VLANS on same NNI	OS6250/6450	Metro
PDUs for EVC MEG	OS6250/6450	Metro
CPE Test Head enhancements	OS6250/6450	Metro
MEF CE 2.0 Certification	OS6250/6450	Metro
QoS		
Per port rate limiting for port group	OS6250/6450	
Buffer Management Custom Profiles	OS6250/6450	
Security / BYOD		
BYOD and External Captive Portal	OS6250/6450	
mDNS relay for Apple TV/Airprint	OS6250/6450	
Console disable command	OS6250/6450	
SSH for read-only user	OS6250/6450	
AAA TACACS command authorization	OS6250/6450	
CLI for TACACS new wait time	OS6250/6450	
SSH Key Increase	OS6250/6450	
Increase Authentication and Accounting Servers	OS6250/6450	

Feature Summary Table

Chassis / System

6450 Fan Speed

Prior to AOS 6.6.5 the operation of the OmniSwitch 6450-U24 fans was they are off when the switch boots up and are only turned on if the temperature reaches the highest operating threshold. Once on, they run at 100% of the duty cycle until the temperature reaches the low threshold temperature, at which point the fans are turned off.

The new operation of the OmniSwitch 6450-U24 fans introduced in AOS 6.6.5 is they are on when the switch boots up and run at 25% of the duty cycle. If the temperature reaches the highest operating threshold they run at 100% of the duty cycle until the temperature reaches the low threshold temperature, at which point the fans return to 25% of the duty cycle.

PoE Link layer classification

With power-via-mdi configured the power for the powered device is negotiated using the optional power via MDI TLV in the LLDPDU. The powered device can request additional power using the power via MDI TLV. The switch will check the current PoE budget and if power is available the switch will provide the requested power to the powered device. If power is unavailable, the switch will respond with the existing maximum power information.

- Power negotiation is supported for Class 4 powered devices.
- The maximum power a powered device can request cannot exceed the maximum power allowed for the PoE class in which the powered device is detected.
- If the port is manually configured with a maximum power value, the powered device cannot receive more power than the maximum configured value.

Stack Split Protection

In the case of a stack with mac-retention enabled, splitting into disjoint sub-stacks due to the failure of one or more stacking links / stack elements, both of the resulting stacks could end up having the same system MAC and IP addresses. Since there is no communication between these individual stacks due to the stacking link failure they end up communicating with the rest of the network devices using the same MAC and IP addresses. This stack split scenario is disruptive to the network as the conflicting MAC and IP addresses can lead to layer 2 loops and layer 3 traffic disruption.

Stack Split Protection provides the following benefits:

- Avoid network disruptions by preventing duplicate MAC and IP addresses on the network.
- The sub-stack that forms out of the stack split is able to detect that a stack split has occurred by use of a helper switch.
- Once the stack split condition has been determined, the protected sub-stack will put its front-panel ports into an operationally down state preventing traffic forwarding and avoiding loops and possible traffic disruption.
- A trap can be sent by the active-stack indicating the stack split state. The trap indicates that the stack split has occured and which elements are in the operationally down sub-stack.
- The entire stack will automatically recover when the sub-stacks rejoin the stack. The front panel ports on the protected sub-stack take 60 seconds to become operationally up.
- With the 665R02 release the device on which SSP is enabled can also act as a helper device.

This feature can also be leveraged for detecting a stack split in a remote stacking topology where the stack may consist of elements located in different physical locations such as a remote site, or multiple floors of a building.

Note: A redundant stacking cable should be used for best traffic convergence in the event of failure.

RFC 1588 v2 – Precision Time Protocol

OmniSwitch 6450-P10S and OmniSwitch 6450-U24S models provide support for IEEE 1588 Version 2 end-to-end transparent clocking. IEEE 1588 Precision Time Protocol (PTP) is used to synchronize clocks throughout a network. On a local area network, it achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control systems.

Note: PTP is not supported in stacking mode.

Layer 2

Multiple VLAN Registration Protocol (MVRP)

Multiple VLAN Registration Protocol as defined in IEEE 802.1ak is intended as a replacement to GVRP by offering more scalable capabilities for large bridged networks. MVRP's general operation is similar to GVRP in that it controls and signals dynamic VLAN registration entries across the bridged network. MVRP addresses these major areas for improvements over GVRP:

- Improved PDU format to fit all 4094 VLANs in a single PDU.
- Reduced unnecessary flushing from STP topology changes that do not impact the Dynamic VLAN topology

Layer 3

Increase ARP Table size

At run time, AOS has increased and also checks that the following objects stay below the system limit

- ARP/NDP. Unknown IP Host flows are discarded in software when the new host system limit is reached (1024 for ARP, 128 for NDP). When in this condition the switch will not generate any ARP requests or NDP solicitation messages.
- When the system is learning hosts or routes above the system limits, a swlog message and a SNMP trap may be generated to indicate to the network administrator that the switch is running above the system limits.

Static routes to directly connected subnet

Multiple static routes can be added to a subnet of a directly connected network. Use "show ip route" command to view the configured static routes.

IPv6 Phase 2 Logo

The OmniSwitch 6250/6450 has passed the conformance and interoperability testing required to obtain the IPv6 Forum IPv6 Ready Logo.

Management

OpenFlow

OpenFlow is a communications interface defined between the control and forwarding layers that is used in a Software Defined Network (SDN). OpenFlow separates the control plane and the data plane in the switch. Traditionally, switches and routers have made decisions on where packets should travel based on rules local to the device. With OpenFlow, only the data plane exists on the switch itself, and all control decisions are communicated to the switch from a central Controller. If the device receives a packet for which it has no flow information, it sends the packet to the Controller for inspection, and the Controller determines where that packet should be sent based on QoS-type rules configured by the user (drop the packets to create a firewall, pass the packets to a specific port to perform load balancing, prioritize packets, etc).

The OmniSwitch can operate in AOS or OpenFlow mode, including a modified OpenFlow mode known as Hybrid mode. AOS will designate the ports managed/controlled by AOS or by OpenFlow on a per-port basis. By default, ports are managed/controlled by AOS. OpenFlow 1.0 and 1.3.1 are supported. The following are the key components available for OpenFlow support.

OpenFlow Logical Switch - An OpenFlow logical switch consists of a portion of the switch's resources that are managed by an OpenFlow Controller (or set of Controllers) via the OpenFlow Agent. Up to 3

logical switches can be configured with each switch supporting up to three controllers. A logical switch has a VLAN, physical ports, and/or link aggregate ports assigned to it. All packets received on these ports are forwarded directly to the OpenFlow agent. Spanning tree and source learning do not operate on OpenFlow assigned ports.

OpenFlow Normal Mode - In Normal Mode, the logical switch operates as per the OpenFlow standards.

OpenFlow Hybrid Mode (API) - In Hybrid mode, logical switch acts as an interface through which the Controller may insert flows. These flows are treated as QoS policy entries and offer the same functionality. A Hybrid mode logical switch operates on all ports, link aggregates, and VLANs not assigned to other OpenFlow logical switches. Only one logical switch can be active in Hybrid mode.

CPU Protection
In some network scenarios high CPU utilization can be seen due to a large number of multicast packets being processed by the CPU. IPv4 or IPv6 multicast protocol packets such as HSRP, EGRP or any type of end to end multicast application using the 224.0.0.0/24 or ff02:0::/32 address range that is not expected to be processed by an L2 switch can affect CPU utilization causing issues with the normal handling of other protocols such as LACP or ERP. Typically this is seen in Carrier Ethernet Networks where Ethernet services are provisioned on the OmniSwitch which is deployed for L2 access on the service provider network. But this scenario can also apply to any large L2 access/core type of network.

The processing of IPV6 protocol packets are controlled by the presence of IPv6 interface. If an iPv6 interface exists then the packets are trapped to the CPU else the packets are transparently forwarded.
To control the processing of IPv4 protocol packets the following command is introduced.
-> ip multicast dynamic-control drop-all status {enable | disable}

Metro

Non-GBPT SW mac-tunnel uni-profile
When MAC-tunneling is enabled globally, the GBPT frames of the UNI profile which do not have MAC-tunneling configured are also captured to the CPU and transferred at CPU rate at the NNI.

In order to avoid the GBPT packets from being rate limited to CPU at the NNI, MAC-Tunneling can be enabled on per SVLAN for a UNI profile. This allows the GBPT packets to be tunneled through hardware at wire rate and the MAC –tunneled packets are trapped to CPU on a per SVLAN basis. To enable MAC-tunneling on per SVLAN basis, MAC-tunneling has to be disabled globally.

Hybrid mode with Q in Q and 802.1a VLANS on same NNI
Standard VLAN support on NNI ports' allows any standard (non-service) VLAN to be associated to NNI ports of type untagged or 802.1q tagged. However, VLAN 1 cannot be associated as untagged member to a NNI port. 802.1q services, QinQ service and untagged services can be configured using the same uplink NNI port. This allows using an untagged management VLAN to manage the switch through NNI ports.

All features/properties supported with the standard VLANs (standard VLAN being configured on fixed ports) are now supported on standard VLANs, configured on NNI interface. Some of these are mobile-tag enable/disable, mac or mac-range rule, IP-rules and so on.

PDUs for EVC MEG
Configuring EVC MEGs (MEPs) on per customer VLAN (CVLAN) in a SVLAN allows supporting connectivity and faulting management. The EVC MEG/MEP can be configured on the UNI-N of the provider bridge. The EVC MEG shall assist the service provider to instantiate a MEP instance for each customer VLAN on the UNI-N port itself to perform OAM action for individual CVLAN traffic bound to the EVC.

CPE Test Head enhancements
The OmniSwitch supports the following enhancements:

Bi-directional test functionality Support
In bidirectional test, the test traffic is bidirectional. The traffic analysis is performed by the generator switch. The test traffic is reflected back to the generator switch using the hardware loopback function on the analyzer switch.

L2 SAA Test Support
The CPE test can be used to measure the Round Trip Time (RTT) and Jitter. The L2 SAA test will run along with the data traffic test. The test results are captured at the generator switch.

Remote Sys Mac Support
The CPE test allows configuring a remote device to receive the test OAM messages on the generator side. The generator device can gather the test OAM messages from the remote device and store it in the local data base.

Saving the Test Results on the /flash
The test results can be stored on the /flash directory of the switch. The test information is appended at the end of the default text file. Two files are used to maintain the test statistics on the /flash directory active file (testoamActiveStats.txt) and inactive file (testoamInactiveStats.txt).

The current test statistics will be stored in the active file. When there is no space in the active file to store the test statistics, the active file is made inactive and the inactive file is made active and the stats are written by overwriting the old data.

MEF CE 2.0 Certification
The OmniSwitch 6450 and OmniSwitch 6250 are now CE 2.0 certified across two service definition, E-Line and E-LAN. CE 2.0 certification ensures service compliance to specifications and interworking between vendors by testing product compliance across these two MEF service types. The CE 2.0 product certification designation applies to the tested configuration and, through compliance, to currently supported hardware and software in general.

QoS

Per port rate limiting for port group
The OmniSwitch supports the following enhancements:

- Port Group and Per Port Rate Limiting
  Per port rate limiting allows configuring a policy rule that specifies a rate limiter for the group of ports or individual port. This can be achieved by configuring specific mode for the port group. The following two modes are supported:
  - Non-split: This mode applies the rate limiting rule to a group of ports specified in the rule. This is the default behavior for the source port group.
  - Split: This mode applies the rate limiting rule to an individual port specified in the group of ports in the rule.
  - Rate limiting is not supported for destination port group, and an error is displayed at the time of rule creation for the destination port group condition.
- Port Groups and Maximum Bandwidth
  Maximum bandwidth policies are applied to source (ingress) ports and flows. This applies to flows that involve more than one port (port group). Based on the rate limit mode set on the port group, the maximum bandwidth is applied to ports individually or together.

Buffer Management Custom Profiles
The ability to modify the number of buffers in the shared pool is now enhanced. The switch now supports a shared pool of buffers and descriptors that allows a queue to use a shared resource, when its guaranteed resource is exceeded. This enhancement gives a limited buffering capability to support bursts of traffic without discarding traffic by associating different port profile (includes resources like Buffers & Descriptors). Please contact Service & Support for additional information on activating the buffer management feature.

Security / BYOD

BYOD and External Captive Portal
The Alcatel-Lucent OmniSwitch implementation of BYOD leverages the Aruba ClearPass Policy Manager (CPPM) and Access Guardian features on the OmniSwitch. It allows guest acces or onboarding of both wired or wireless devices such as employee, guest, employee owned or silent devices through an OmniSwitch edge device with ClearPass as a RADIUS server or RADIUS proxy. This feature supports the following functionalities:

- Unified access policy management solution for Wireline and Wireless networks using CPPM
- Integration with Access Guardian UNPs and 802.1x authentication
- Restricts access to the network and validation for end user devices including employees with IT supplied devices, IP phones, employee's personal devices, guest devices, access points, cameras, and silent devices such as printers.
- CPPM can act as a RADIUS server for new deployments or RADIUS proxy for existing networks. Self-service/self-registration by Employees when they connect to the Enterprise network using their personal device through CPPM.
- Captive portal hosted on CPPM for this feature.
- Device Profiling and Posture Check. Registration and tracking of devices associated with Employees and approved for usage.
- Redirection and restricted access for non-compliant devices.
- Zero-touch Auto-configuration of employee personal devices based on pre-defined role-based Configuration profiles.
- Differentiated access & user experience policies based on Corporate or Employee Personal device, Applications and Role.
- Integration with RADIUS Server and CPPM for Authentication, Authorization and Accounting.
- Automatic provisioning of Applications such as NAC Agent, MDM Client as part of the device enrollment process on Employee Personal Devices.
- Automatic provisioning of Device Certificates that are dynamically requested, issued and installed on the Employee Personal Device with association to Employee corporate Credentials
- Provides notification of BYOD policy violations, usage statistics, time and cost information to the end-user in real-time.
- RADIUS Change of Authorization (CoA)
  - A mechanism to change AAA attributes of a session after authentication
  - New Profile sent as an attribute in the message
  - Disconnect Message to terminate user session and discard all user context
  - Port bounce capability can be configured on the OmniSwitch to ensure a clean re-authentication process for non-supplicant devices.
  - URL redirect and port location information

In addition to BYOD section in OmniSwitch user guides additional configuration examples can be viewed on the Alcatel-Lucent Enterprise Demo channel:
http://www.youtube.com/playlist?list=PLrzAZN530GJ8kfUJCNsjIhJW6cAV5AACb

mDNS relay for Apple TV/Airprint
mDNS is a zero configuration host name resolution service used to discover services on a LAN. mDNS allows resolving host names to IP addresses within small networks without the need of a conventional DNS server. The mDNS protocol uses IP multicast User Datagram Protocol (UDP) packets and is implemented by Apple Bonjour, Avahi (LGPL), and Linux NSS-MDNS. To resolve a host name, the mDNS client broadcasts a query message asking the host having that name to identify itself. The target machine then multicasts a message that includes its IP address. All machines in that subnet will use that information to update their mDNS caches.
As an example Apple's Bonjour architecture implements the following three fundamental operations to support zero configuration networking service:

- Publication (Advertising a service)

- Discovery (Browsing for available services)
- Resolution (Translating service instance names to address and port numbers for use)

The Aruba AirGroup feature provides optimization that limits the unnecessary flooding of Bonjour traffic to improve Wifi performance and also allow the Bonjour services to extend across VLANs. The OmniSwitch enhancement supports an mDNS relay function by configuring a GRE tunnel interface between the WLAN controller and the OmniSwitch. The OmniSwitch can intercept and relay the mDNS frames from the wired devices advertising a service using Bonjour messages to the WLAN controller thus preventing flooding of the mDNS frames.
Note: mDNS relay is only supported for wireless clients. Wired clients are not supported.

Console disable command
This feature can be used in security-sensitive networks and deployment by managing the access to the switch configuration shell through the console port. The feature allows the following operations:

- Enable or Disable the access to the switch configuration shell through the console port.
- Stores the access configuration in the configuration file (boot.cfg) so that even after a reboot the access to the switch remains the same through console port.

It is recommended to create a back-up of the configuration file before using this feature. If remote access to the switch is lost (i.e Telnet, SSH, Webview) the console session to the switch can be restored by contacting customer support.

SSH for read-only user
Prior to this release only users with read-write permissions could access the switch using SSH. This restricted the users with read-only access from using the more secure SSH method of accessing the switch. This enhancement allows users with read-only permissions to access the switch using SSH.

AAA TACACS command authorization
Prior to this enhancement command authorization with TACACS was done based on the partition-management family that the command belongs to. The OmniSwitch now supports CLI based authorization with a TACACS+ server. Use **aaa tacacs command-authorization** to enable or disable command based authorization. If enabled the authorization of every CLI command executed on the switch is sent for authorization to the TACACS+ server along with-mode of operation (read or read-write). After authorization, the server will send the response message to the TACACS+ client. If this feature is disabled then authorization is based on the partition-management family, that is, partition-management family is sent for authorization.

CLI for TACACS new wait time
The OmniSwitch supports configuring the wait time of the TACACS+ server during the user's command authorization process. Use **aaa tacacs server-wait-time** command to configure server wait time.

When the CLI command is entered, it is passed on to the aaa task for authorization with a wait time of only 5 seconds. However, if the TACACS server timeout is configured to a higher value and there are multiple servers configured, then the usual response from the TACACS+ server is longer than 5 seconds. The CLI task is timed-out and the positive response from the TACACS server for the previous command is used for next authorization transactions. Thus, the unauthorized users were able to perform write operations on switch based on the positive authorization for previous command. Hence, the command **aaa tacacs server-wait-time** and variable **tacacs-new-wait-time** are introduced to set the wait time for aaa response.

SSH Key Size Increase
The current SSH key size is 512 bit. In this release the SSH key size for certificate generation is increased from 512 bits to 1024 bits for additional security.

Since the certificate is stored persistently in flash, to allow the new key size to take effect the certificate must be regenerated. The certificate file must be deleted and switch rebooted with the new code changes.

Increase Authentication / Accounting Servers

The number of servers that can be specified for 802.1x, MAC, and AAA authentication and accounting is increased from four to five.

SNMP Traps

No.	Trap Name	Platforms	Description
0	coldStart	all	The SNMP agent in the switch is reinitiating and itsk configuration may have been altered.
1	warmStart	all	The SNMP agent in the switch is reinitiating itself and its configuration is unaltered.
2	linkDown	all	The SNMP agent in the switch recognizes a failure in one of the communications links configured for the switch.
3	linkUp	all	The SNMP agent in the switch recognizes that one of the communications links configured for the switch has come up.
4	authenticationFailure	all	The SNMP agent in the switch has received a protocol message that is not properly authenticated.
5	entConfigChange	all	An entConfigChange notification is generated when a conceptual row is created, modified, or deleted in one of the entity tables.
6	aipAMAPStatusTrap	all	The status of the Alcatel-Lucent Mapping Adjacency Protocol (AMAP) port changed.
7	aipGMAPConflictTrap	—	This trap is not supported.
8	policyEventNotification	all	The switch notifies the NMS when a significant event happens that involves the policy manager.
9	chassisTrapsStr	all	A software trouble report (STR) was sent by an application encountering a problem during its execution.
10	chassisTrapsAlert	all	A notification that some change has occurred in the chassis.
11	chassisTrapsStateChange	all	An NI status change was detected.
12	chassisTrapsMacOverlap	all	A MAC range overlap was found in the backplane eeprom.
15	healthMonDeviceTrap	all	Indicates a device-level threshold was crossed.
16	healthMonModuleTrap	all	Indicates a module-level threshold was crossed.
17	healthMonPortTrap	all	Indicates a port-level threshold was crossed.
20	esmDrvTrapDropsLink	all	This trap is sent when the Ethernet code drops the link because of excessive errors.
21	pimNeighborLoss	all	This trap is not supported.
24	risingAlarm	all	An Ethernet statistical variable has exceeded its rising threshold. The variable's rising threshold and whether it will issue an SNMP trap for this condition are configured

No.	Trap Name	Platforms	Description
			by an NMS station running RMON.
25	fallingAlarm	all	An Ethernet statistical variable has dipped below its falling threshold. The variable's falling threshold and whether it will issue an SNMP trap for this condition are configured by an NMS station running RMON.
26	stpNewRoot	all	Sent by a bridge that became the new root of the spanning tree.
27	stpRootPortChange	all	A root port has changed for a spanning tree bridge. The root port is the port that offers the lowest cost path from this bridge to the root bridge.
28	mirrorConfigError	all	The mirroring configuration failed on an NI. This trap is sent when any NI fails to configure mirroring. Due to this error, port mirroring session will be terminated.
29	mirrorUnlikeNi	all	The mirroring configuration is deleted due to the swapping of different NI board type. The Port Mirroring session which was active on a slot cannot continue with the insertion of different NI type in the same slot.
30	slPCAMStatusTrap	all	The trap status of the Layer 2 pesudoCAM for this NI.
31	unused	—	
32	unused	—	
34	ifMauJabberTrap	all	This trap is sent whenever a managed interface MAU enters the jabber state.
35	sessionAuthenticationTrap	all	An authentication failure trap is sent each time a user authentication is refused.
36	trapAbsorptionTrap	all	The absorption trap is sent when a trap has been absorbed at least once.
37	alaStackMgrDuplicateSlotTrap	all	Two or more slots claim to have the same slot number.
38	alaStackMgrNeighborChangeTrap	all	Indicates whether or not the stack is in loop.
39	alaStackMgrRoleChangeTrap	all	Indicates that a new primary or secondary stack is elected.
40	lpsViolationTrap	all	A Learned Port Security (LPS) violation has occurred.
41	alaDoSTrap	all	Indicates that the sending agent has received a Denial of Service (DoS) attack.
42	gmBindRuleViolation	all	Occurs whenever a binding rule which has been configured gets violated.

No.	Trap Name	Platforms	Description
43	unused	—	
44	unused	—	
45	unused	—	
46	unused	—	
47	pethPsePortOnOff	P24	Indicates if power inline port is or is not delivering power to the a power inline device.
48	pethPsePortPowerMaintenanceStatus	P24	Indicates the status of the power maintenance signature for inline power.
49	pethMainPowerUsageOn	P24	Indicates that the power inline usage is above the threshold.
50	pethMainPowerUsageOff	P24	Indicates that the power inline usage is below the threshold.
53	httpServerDoSAttackTrap	all	This trap is sent to management station(s) when the HTTP server is under Denial of Service attack. The HTTP and HTTPS connections are sampled at a 15 second interval. This trap is sent every 1 minute while the HTTP server detects it is under attack.
54	alaStackMgrDuplicateRoleTrap	all	The element identified by alaStackMgrSlotNINumber detected the presence of two elements with the same primary or secondary role as specified by alaStackMgrChasRole on the stack.
55	alaStackMgrClearedSlotTrap	all	The element identified by alaStackMgrSlotNINumber will enter the pass through mode because its operational slot was cleared with immediate effect.
56	alaStackMgrOutOfSlotsTrap	all	One element of the stack will enter the pass through mode because there are no slot numbers available to be assigned to this element.
57	alaStackMgrOutOfTokensTrap	all	The element identified by alaStack MgrSlotNINumber will enter the pass through mode because there are no tokens available to be assigned to this element.
58	alaStackMgrOutOfPassThruSlotsTrap	all	There are no pass through slots avail able to be assigned to an element that is supposed to enter the pass through mode.
59	gmHwVlanRuleTableOverloadAlert	all	An overload trap occurs whenever a new entry to the hardware VLAN rule table gets dropped due to the overload of the table.
60	lnkaggAggUp	all	Indicates the link aggregate is active. This trap is sent when any one port of the link aggregate

No.	Trap Name	Platforms	Description
			group goes into the attached state.
61	lnkaggAggDown	all	Indicates the link aggregate is not active. This trap is sent when all ports of the link aggregate group are no longer in the attached state.
62	lnkaggPortJoin	all	This trap is sent when any given port of the link aggregate group goes to the attached state.
63	lnkaggPortLeave	all	This trap is sent when any given port detaches from the link aggregate group.
64	lnkaggPortRemove	all	This trap is sent when any given port of the link aggregate group is removed due to an invalid configura tion.
65	pktDrop	all	The pktDrop trap indicates that the sending agent has dropped certain packets (to blocked IP ports, from spoofed addresses, etc.).
66	monitorFileWritten	all	A File Written Trap is sent when the amount of data requested by the user has been written by the port monitor ing instance.
69	gmHwMixModeSubnetRuleTableOverloadAlert	all	A subnet overload trap occurs in mixed mode whenever a new entry to the HW subnet rule table gets dropped in OS6800 due to the overload of the table.
70	pethPwrSupplyConflict	all	Power supply type conflict trap.
71	pethPwrSupplyNotSupported	all	Power supply not supported trap.
72	lpsPortUpAfterLearningWindowExpiredTrap	all	When an LPS port joins or is enabled after the Learning Window is expired, the MAC address learning on the port will be disabled, and this trap is generated as a notification. This trap will also be generated at the time the Learning Window expires, with a slice and port value of 0.
92	dot1agCfmFaultAlarm	all	A MEP has lost contact with one or more MEPs. A notification (fault alarm) is sent to the management entity with the OID of the MEP that has detected the fault.
93	Unused	all	-
94	lldpRemTablesChange	all	A lldpRemTablesChange notification is sent when the value of lldpStatsRemTableLastChangeTime changes.
95	chassisTrapsPossibleDuplicateMac	all	The old PRIMARY element cannot

No.	Trap Name	Platforms	Description
			be detected in the stack. There is a possiblity of a duplicate MAC address in the network.
101	lpsLearnMac	all	Generated when an LPS port learns a bridged MAC address.
102	gvrpVlanLimitReachedEvent	all	Generated when the number of vlans learned dynamically by GVRP has reached a configured limit.
105	udldStateChange	all	Generated when the state of the UDLD protocol changes.
106	healthMonIpcTrap		IPC pools exceed usage/ causing trap."
107	Reserved	-	-
108	Reserved	-	-
109	arpMaxLimitReached	all	Generated when the hardware table has reached supported maximum entries.
110	ndpMaxLimitReached	all	Generated when the hardware table has reached supported maximum entries.
111	ripRouteMaxLimitReached	all	Generated when RIP database has reached supported maximum entries. RIP will discard any new updates.
112	ripngRouteMaxLimitReached	all	Generated when RIPng database has reached supported maximum entries. RIPng will discard any new updates.
113-118	Reserved	-	
119	dot3OamThresholdEvent	all	This trap is sent when a local or remote threshold crossing event is detected. A local threshold crossing event is detected by the local entity, while a remote threshold crossing event is detected by the reception of an Ethernet OAM Event Notification OAMPDU that indicates a threshold event.
120	dot3OamNonThresholdEvent	all	This trap is sent when a local or remote non-threshold crossing event is detected. A local event is detected by the local entity, while a remote event is detected by the reception of an Ethernet OAM Event Notification OAMPDU that indicates a non-threshold crossing event.
121	alaDot3OamThresholdEventClear	all	This trap is sent when is sent when a local or remote threshold

No.	Trap Name	Platforms	Description
			crossing event is recovered.
122	alaDot3OamNonThresholdEventClear	all	This trap is sent is sent when a local or remote non-threshold crossing event is recovered.
123-146	Reserved	-	
147	halHashCollisionTrap	all	This trap is sent when an SFP/XFP/SFP+ Rx optical power has crossed any threshold or reverted from previous threshold violation for a port represented by ifIndex. It also provides the current real time value of SFP/XFP/SFP+ Rx optical power.
148	alaLbdStateChangeToShutdown	all	This trap is sent when an SFP/XFP/SFP+ Rx optical power has crossed any threshold or reverted from previous threshold violation for a port represented by ifIndex. It also provides the current real time value of SFP/XFP/SFP+ Rx optical power.
149	alaLbdStateChangeForClearViolationA	all	This trap is sent when an SFP/XFP/SFP+ Rx optical power has crossed any threshold or reverted from previous threshold violation for a port represented by ifIndex. It also provides the current real time value of SFP/XFP/SFP+ Rx optical power.
150	alaLbdStateChangeForAutoRecovery	all	This trap is sent when an SFP/XFP/SFP+ Rx optical power has crossed any threshold or reverted from previous threshold violation for a port represented by ifIndex. It also provides the current real time value of SFP/XFP/SFP+ Rx optical power.
151	Reserved	all	Reserved
152	Reserved	all	Reserved
153	alaErpRingStateChanged	all	This trap is sent when the ERP Ring State has changed.
154-158	Reserved	all	Reserved
159	alaDhcpClientAddressAddTrap	all	This trap is sent when a new IP address is assigned to DHCP Client interface.
160	alaDhcpClientAddressExpiryTrap	all	This trap is sent when the lease time expires or when the DHCP client is not able to renew/rebind an IP address
161	alaDhcpClientAddressModifyTrap	all	This trap is sent when the DHCP client is unable to obtain the existing IP address and a new IP address is assigned to the DHCP

No.	Trap Name	Platforms	Description
			client.
162	alaDyingGaspTrap	all	This trap is sent when a switch has lost all power.
163	alaTestOamTxDoneTrap	all	After a configured time interval, this trap is sent to the NMS from Generator switch when the test duration expires.
164	alaTestOamRxReadyTrap	all	This trap is sent to the NMS once the switch with Analyzer or Loopback Role is ready to receive test traffic. Once this trap is received, the Generator is activated for generating test traffic.
165	alaTestOamTestAbortTrap	all	This trap is sent to the NMS from the switch, if the test is aborted during takeover.
166	Reserved	all	Reserved
167	Reserved	all	Reserved
168	alaSaaIPIterationCompleteTrap	all	This trap is sent when an IP SAA iteration is completed.
169	alaSaaEthIterationCompleteTrap	all	This trap is sent is sent when a Eth-LB or Eth-DMM SAA iteration is completed.
170	alaSaaMacIterationCompleteTrap	all	This trap is sent is sent when a MAC SAA iteration is completed.
171	aaaHicServerChangeTrap	all	This trap is sent when the active HIC server is changed from or to primary.
172	aaaHicServerUpTrap	all	This trap is sent when at least one of the HIC servers comes UP.
173	alaLldpTrustViolation	all	This trap is sent when there is an LLDP Trust Violation, and gives the reason for the violation
174	alaStackMgrIncompatibleModeTrap	all	Not Supported
175	Reserved	all	Reserved
176	alaDHLVlanMoveTrap	all	When linkA or linkB goes down or comes up and both ports are are part of some vlan-map, this trap is sent to the Management Entity, with the DHL port information.
177	esmPortViolation	all	This trap is sent when an interface is shut down by a feature due to violation.
178	Reserved	all	Reserved
179	Reserved	all	Reserved
180	alaTestOamGroupTxDoneTrap	all	After a configured time interval, this trap is sent to the NMS from Generator switch when the test duration expires.
181	alaTestOamGroupRxReadyTrap	all	This trap is sent to the NMS once the switch with Analyzer or Loopback Role is ready to receive test traffic. Once this trap is

No.	Trap Name	Platforms	Description
			received, the Generator is activated for generating test traffic.
182	alaTestOamGroupAbortTrap	all	This trap is sent to the NMS from the switch, if the test is aborted during takeover.
183	alaDhcpBindingDuplicateEntry	all	This trap is sent to notify the user of MAC Movement in DHCP-Binding Table.
184	esmStormThresholdViolationStatus	all	Not Supported
185	Reserved	all	Reserved
186	Reserved	all	Reserved
187	Reserved	all	Reserved
188	poePowerBudgetChange	all	Not Supported
189	alaDBChange	all	This trap is sent when there is a change in the expansion module presence.
190	alaStackMgrIncompatibleLicenseTrap	all	This trap is sent when an interface enters the pass through mode because element license information is not same as primary element license information.
191	Reserved	all	Reserved
192	Reserved	all	Reserved
193	Reserved	all	Reserved
194	Reserved	all	Reserved
195	Reserved	all	Reserved
196	Reserved	all	Reserved
197	Reserved	all	Reserved
198	aluLicenseManagerLicenseExpiry	all	This trap is sent when the value of aluLicenseTimeRemaining becomes 0 (zero) for a demo licensed application. This notification is applicable only for temporary licenses. This trap can be utilized by an NMS to inform user about application license expiration.
199	Reserved	all	Reserved
200	Reserved	all	Reserved
201	Reserved	all	Reserved
202	Reserved	all	Reserved
203	Reserved	all	Reserved
204	Reserved	all	Reserved
205	Reserved	all	Reserved
206	Reserved	all	Reserved
207	Reserved	all	Reserved
208	Reserved	all	Reserved
209	Reserved	all	Reserved
210	Reserved	all	Reserved
211	Reserved	all	Reserved
212	Reserved	all	Reserved
213	Reserved	all	Reserved

No.	Trap Name	Platforms	Description
214	Reserved	all	Reserved
215	Reserved	all	Reserved
216	Reserved	all	Reserved
217	Reserved	all	Reserved
218	Reserved	all	Reserved
219	Reserved	all	Reserved
220	Reserved	all	Reserved
221	Reserved	all	Reserved
222	Reserved	all	Reserved
223	Reserved	all	Reserved
224	Reserved	all	Reserved
225	Reserved	all	Reserved
226	ConfigSaveSucceededTrap	all	Config change trap is sent each time a config is saved via Cli/Snmp/Web.
227	Reserved83	all	Reserved
228	Reserved84	all	Reserved
229	Reserved85	all	Reserved
230	alaStackSplitProtectionTrap	all	This trap is sent when an element of the stack enters into the Protection state.
231	alaStackSplitRecoveryTrap	all	This trap is sent when an element of the stack recovers from the Protection state.
232	Reserved	all	Reserved
233	alaTestOamStatsWriteDoneTrap	all	This trap is sent when the maximum number of stats records have been written to the testoam stats file maintained in /flash.

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	Software Package
BGP	OS6250/6450	advanced routing
DVMRP	OS6250/6450	advanced routing
IS-IS	OS6250/6450	advanced routing
Multicast Routing	OS6250/6450	advanced routing
OSPF, OSPFv3	OS6250/6450	advanced routing
PIM	OS6250/6450	advanced routing
Traffic Anomaly Detection	OS6250/6450	advanced routing
ACLMAN	OS6250/6450	base
Authenticated VLANs	OS6250/6450	base
IPv6 Sec	OS6250/6450	base
IP Tunnels (IPIP, GRE, IPv6)	OS6250/6450	base
IPX	OS6250/6450	base
Quarantine Manager and Remediation	OS6250/6450	base
Server Load Balancing	OS6250/6450	base

Unsupported CLI Commands

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

Software Feature	Unsupported CLI Commands
AAA	aaa authentication vlan single-mode aaa authentication vlan multiple-mode aaa accounting vlan show aaa authentication vlan show aaa accounting vlan
CPE Test Head	test-oam direction bidirectional test-oam role loopback
Chassis Mac Server	mac-range local mac-range duplicate-eeprom mac-range allocate-local-only show mac-range status
DHCP Relay	ip helper traffic-suppression ip helper dhcp-snooping port traffic-suppression
Ethernet Services	ethernet-services sap-profile bandwidth not-assigned
Flow Control	flow
Hot Swap	reload ni [slot] # [no] power ni all
Interfaces	show interface slot/port hybrid copper counter errors show interface slot/port hybrid fiber counter errors
QoS	qos classify fragments qos flow timeout
System	install power ni [slot]

Open Problem Reports and Feature Exceptions

The problems listed here include problems known at the time of the product's release. Any problems not discussed in this section should be brought to the attention of the 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.

PoE

PR	Description	Workaround
201921	When trying to disable capacitive detection on a switch that booted with capacitive detection enabled, the first attempt may not work.	Re-enter the 'lanpower capacitor-detection enable' and 'lanpower capacitor-detection disable' commands.

QoS

PR	Description	Workaround
199583	If both BPDU filtering and shutdown are configured (ex. **->qos trust ports user-port filter bpdu user-port shutdown bpdu**) the BPDUs will be filtered but the port will not be shutdown. This is due to the filtering option taking precedence over shutdown.	To have the port shutdown use only the shutdown option. (ex. **-> qos trust ports user-port shutdown bpdu**)

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 6.6.5.R02 Upgrade Instructions

OmniSwitch Upgrade Overview

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

- OmniSwitch 6250 models being upgraded to AOS 6.6.5.R02.
- OmniSwitch 6450 models being upgraded to AOS 6.6.5.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 6.6.5.R02 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 6.6.5.R02.

Version Requirements – Upgrading to AOS Release 6.6.5.R02

Version Requirements to Upgrade to AOS Release 6.6.5.R02			
	AOS	**Uboot/Miniboot**	**CPLD**
6250-24/P24/8M/24M	6.6.5.63.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	6.6.5.63.R02 GA 6.6.5.63.R02 GA 6.6.5.63.R02 GA 6.6.5.63.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
• 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.
- All OS6450 models must upgrade the CPLD to the versions listed above to support AOS Release 6.6.5.R02.

Upgrading to AOS Release 6.6.5.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 6.6.5.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 6.6.5 Files to the Switch

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

5. Download and extract the 6.6.5 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 – KFbase.img, KFeni.img, KFos.img, KFsecu.img
   - CPLD File - KFfpga_upgrade_kit
6. FTP (Binary) the 6.6.5.R02 Uboot/Miniboot files listed above to the **/flash** directory on the primary CMM, if required.
7. FTP (Binary) the CPLD upgrade kit listed above to the **/flash** directory on the primary CMM, if required.
8. FTP (Binary) the 6.6.5.R02 image files listed above to the **/flash/working** directory on the primary CMM.
9. 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 6.6.5.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 6.6.5.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       6.6.5.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
```

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 6.6.5.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 6.6.5.R02.
- OmniSwitch 6450 models being downgraded from AOS 6.6.5.R02.

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 6.6.5.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 6.6.5.R02. Previous AOS releases are compatible with the Uboot/Miniboot and CPLD versions shipping from the factory.

Beginning in Q1 2015 OS6450 models will begin shipping with new internal hardware components. These switches require a minimum version of **AOS 6.6.4.285.R01** to operate. Use the '**show cmm**' command to determine the model part number. To downgrade the models in the table below to a different AOS version please contact Service & Support.

Model	Part Number
OS6450-10	903770-90
OS6450-10L	903771-90
OS6450-24	903772-90
OS6450-24L	903773-90
OS6450-48	903774-90
OS6450-48L	903775-90
OS6450-P10	903776-90
OS6450-P10L	903777-90
OS6450-P24	903778-90
OS6450-P24L	903779-90
OS6450-P48	903780-90
OS6450-P48L	903781-90
OS6450-U24	903782-90
OS6450-GNI-C2	903784-90
OS6450-GNI-U2	903785-90
OS6450-XNI-U2	903786-90

Minimum AOS Release Required - 6.6.4.285.R01

```
-> show cmm
CMM in slot 1
  Model Name:                     OS6450-P24,
  Description:                    CMM,
  Part Number:                    903778-90,
  Hardware Revision:              03,
  Serial Number:                  M428086P,
  Manufacture Date:               FEB 21 2015,
  Firmware Version:               n/a,
  Admin Status:                   POWER ON,
  Operational Status:             UP,
  Power Consumption:              0,
  Power Control Checksum:         0xb835,
  CPU Model Type   :              MV88F6281 Rev 2,
  MAC Address:                    e8:e7:32:27:08:90,
```

Example Part Number Output

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 Files to the Switch

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

1. Download and extract the appropriate 6.6.X 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

2. FTP (Binary) the 6.6.X 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       6.6.4.R01   15510736  Alcatel-Lucent Base Software
KFos.img         6.6.4.R01    2511585   Alcatel-Lucent OS
KFeni.img        6.6.4.R01    5083931  Alcatel-Lucent NI software
KFsecu.img       6.6.4.R01     597382  Alcatel-Lucent Security Management
```