Release Notes

OmniSwitch 6250/6450

RELEASE 6.6.4.R01

This release notes accompany release 6.6.4.R01 software for the OmniSwitch 6250/6450 Metro and Enterprise 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.

Release Notes
Part Number 032864-00 Rev. B

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 User 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 User 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 6.6.4 R01:

- OmniSwitch 6250/6450 Series Release 6.6.4.R01 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 6.6.4.R01 AOS software available from Service & Support.

OmniSwitch 6250 (All Models)

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

OmniSwitch 6450-24/P24/48/P48

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

OmniSwitch 6450-U24

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

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

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

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

New Hardware Supported

Chassis Models

OmniSwitch 6450-24L[1,2]
Provides 24 RJ-45 10/100/1000BaseT Ethernet ports, 2 non-combo SFP+ ports, 1 expansion slot for optional stacking or uplink modules, an internal AC power supply, and an optional slide-in 90W AC or DC redundant power supply.

OmniSwitch 6450-48L[1,2]
Provides 48 RJ-45 10/100/1000BaseT Ethernet ports, 2 non-combo SFP+ ports, 1 expansion slot for optional stacking or uplink modules, an internal AC power supply, and an optional slide-in 90W AC or DC redundant power supply.

OmniSwitch 6450-P24L[1,2]
Provides 24 RJ-45 10/100/1000BaseT 802.3at Power Over Ethernet ports, 2 non-combo SFP+ ports, 1 expansion slot for optional stacking or uplink modules, an internal AC power supply, and an optional external 550W AC power supply, no other external power supplies supported.

OmniSwitch 6450-P48L[1,2]
Provides 48 RJ-45 10/100/1000BaseT 802.3at Power Over Ethernet ports, 2 non-combo SFP+ ports, 1 expansion slot for optional stacking or uplink modules, an internal AC power supply, and an optional external 900W AC power supply, no other external power supplies supported.

1. The 'Lite' models support 10/100 only on the RJ-45 non-combo ports and can be upgraded to support 10/100/1000 with an upgrade license.
2. The fixed 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 stacking OS6450-XNI-U2 plug-in module.

Transceivers

SFP-DUAL-SM10
Dual Speed 100Base-LX or 1000Base-LX Ethernet optical transceiver (SFP MSA). Supports single-mode fiber over 1310nm wavelength with an LC connector. Typical reach of 10Km at Gigabit speed and 100Mbit speed.

Note: This transceiver is not supported in the initial GA release but support will be added for the OS6450 in the near future. Please Contact Service & Support for information.

SFP-DUAL-BX-D
1000Base-BX10-D SFP transceiver with an LC type interface. This dual-speed, bi-directional transceiver is designed for use over single-mode fiber optic on a single strand link up to 10KM point-to-point. It can operate at 100/1000Mbit speed, transmits at 1550nm and receives at 1310nm optical signal.

Note: AOS release 6.6.4 adds support for OS6250.

SFP-DUAL-BX-U
1000Base-BX10-U SFP transceiver with an LC type interface. This dual-speed, bi-directional transceiver is designed for use over single-mode fiber optic on a single strand link up to 10KM point-to-point. It can operate at 100/1000Mbit speed, transmits at 1310nm and receives at 1550nm optical signal.

Note: AOS release 6.6.4 adds support for OS6250.

SFP-GIG-BX-D20
1000Base-BX SFP transceiver with an LC type connector. This bi-directional transceiver is designed for use over single-mode fiber on a single strand link up to 20 km. Transmits at 1490nm and receives at 1310nm optical signal. Designed for use with SFP-GIG-BX-U20.

Note: Supported on OS6450 only.

SFP-GIG-BX-U20
1000Base-BX SFP transceiver with an LC type connector. This bi-directional transceiver is designed for use over single-mode fiber on a single strand link up to 20 km. Transmits at 1310 nm and receives at 1490nm optical signal. Designed for use with SFP-GIG-BX-D20.

Note: Supported on OS6450 only.

SFP-GIG-EXTND
1000Base-SX Gigabit Ethernet optical transceiver (SFP MSA). Supports multimode fiber over 1310nm wavelength with an LC connector. Typical reach up to 2 Km on 62.5/125 µm MMF and 50/125 µm MMF.

Note: AOS release 6.6.4 adds support for OS6450.

SFP-10G-GIG-SR Transceiver
Dual-speed SFP+ optical transceiver. Supports multimode fiber over 850nm wavelength (nominal) with an LC connector. Supports 1000BaseSX and 10GBASE-SR.

Note: This transceiver is not supported in the initial GA release but support will be added to the OS6450 in the near future. Please Contact Service & Support for information.

Supported Hardware/Software Combinations

The following table shows the 6.6.X software releases that support each of the listed existing OS6250 models:

Model	Part Number	6.6.1.R01	6.6.2.R01	6.6.3.R01	6.6.4.R01
6250-8M	902735-90 903092-90	Supported Not Supported	Supported Supported[1]	Supported Supported	Supported Supported
6250-24M	902736-90 903093-90	Supported Not Supported	Supported Supported[1]	Supported Supported	Supported Supported
6250-24MD	902737-90 903094-90	Supported Not supported	Supported Supported[1]	Supported Supported	Supported Supported
6250-24	902734-90 903091-90 902908-90 903099-90	Supported Supported[1] Supported Supported[1]	Not Supported Not Supported Not Supported Not Supported	Supported Supported Supported Supported	Supported Supported Supported Supported
6250-P24	902738-90 903095-90	Supported Supported[1]	Not Supported Not Supported	Supported Supported	Supported Supported

1. Minimum maintenance release required.

The following table shows the 6.6.X software releases that support each of the listed existing OS6450 models:

Model	Part Number	6.6.1.R01 6.6.2.R01	6.6.2.R02	6.6.3.R01	6.6.4.R01
6450-10	903005-90 903406-90	Not Supported Not Supported	Supported Supported	Supported Supported	Supported Supported
6450-P10	903016-90 903407-90	Not Supported Not Supported	Not Supported Not Supported	Supported Supported	Supported Supported
6450-10L	903006-90 903408-90	Not Supported Not Supported	Not Supported Not Supported	Supported Supported	Supported Supported
6450-P10L	903017-90 903409-90	Not Supported Not Supported	Not Supported Not Supported	Supported Supported	Supported Supported
6450-24	903007-90 903173-90	Not Supported Not Supported	Not Supported Not Supported	Supported Supported	Supported Supported
6450-P24	903018-90 903174-90	Not Supported Not Supported	Not Supported Not Supported	Supported Supported	Supported Supported
6450-24L	903425-90	Not Supported	Not Supported	Not Supported	Supported
6450-P24L	903426-90	Not Supported	Not Supported	Not Supported	Supported
6450-48	903107-90 903176-90	Not Supported Not Supported	Not Supported Not Supported	Supported Supported	Supported Supported
6450-P48	903108-90 903177-90	Not Supported Not Supported	Not Supported Not Supported	Supported Supported	Supported Supported
6450-48L	903427-90	Not Supported	Not Supported	Not Supported	Supported
6450-P48L	903428-90	Not Supported	Not Supported	Not Supported	Supported
6450-U24	903038-90 903175-90	Not Supported Not Supported	Not Supported Not Supported	Supported Supported	Supported Supported

6.6.4 New Software Features and Enhancements

The following software features are new with the 6.6.4.R01 release, subject to the feature exceptions and problem reports described later in these release notes:

6.6.4 New Feature/Enhancements Summary

Feature	Platform	License
Hardware		
6450L license upgrade	OS6450	
6450-10 stacking to 4 units	OS6450	
DDM Support	OS6250/6450	
Remote Stacking	OS6450 (24/48 port models)	
IEEE 802.3az	OS6450	
DHCP		
DHCP Server	OS6250/6450	
Support of dhcp vendor class and switch type	OS6250/6450	
Preference to an OXO dhcp server	OS6250/6450	
IP helper "ip-source-filter" and persistency commands	OS6250/6450	
Metro		
Control Frame Tunneling Stats	OS6250/6450	Metro License Required
CF hardware tunnel	OS6250/6450	Metro License Required
PPPoE IA to support ATM default parameter	OS6250/6450	Metro License Required
TDR	OS6250/6450	
Security		
LPS Sticky mode	OS6250/6450	
Unique session id for radius accounting	OS6250/6450	
Accept lower case lettering with MAC-based auth	OS6250/6450	
UNP ingress/egress bw limiting via radius		
RADIUS non-supplicant/supplicant acct. including valid NAS-PORT	OS6250/6450	
Radius acct of Gig words	OS6250/6450	
Radius attribute calling station ID	OS6250/6450	
System		
Improved L2 multicast convergence after takeover	OS6250/6450	
SNMP healthmonportrap per port	OS6250/6450	
show QoS queue stats in bits/second	OS6250/6450	
New stats display with filters for ingress	OS6250/6450	

Feature	Platform	License
traffic		
Storm control options	OS6250/6450	
SAM triggered CLI config change	OS6250/6450	

6.6.4 New Software Features and Enhancements Descriptions

Hardware

6450L License Upgrade
Upon purchasing a license a Card ID will be issued. With this Card ID, the customer can request a license file from the ALU Web Portal.
Following are the license packages available:

- Gig package - This allows the 6450-24L/P24L and 6450-48L/P48L ports to run at 10/100/1000.

Additionally, the following licenses are also available.

- 10G package - This allows the fixed SFP/SFP+ interfaces to run at 10Gbps.
- Metro package - This allows the metro features to be activated on the Enterprise Models.

6450-10 Stacking Up To 4 Units
The OmniSwitch 6450-10 models now support stacking up to four units. OmniSwitch 6450-10 switches can only be stacked with other OS6450-10 switches. Stacking OS6450-10 model with other OS6450 models is not supported.

DDM Support
Digital Diagnostics Monitoring allows an OmniSwitch to monitor the status of a transceiver by reading the information contained on the transceiver's EEPROM. The transceiver can display Actual, Warning-Low, Warning-High, Alarm-Low and Alarm-High for the following:

- Temperature
- Supply Voltage
- Current
- Output Power
- Input Power

Note: Not all transceivers support DDM; refer to the Transceivers Guide for additional DDM information.

Remote Stacking
The OmniSwitch supports stacking multiple chassis into a virtual chassis using SFP+ fiber transceivers. A distance of up to 10Km is supported.

IEEE 802.3az
Energy Efficient Ethernet (EEE) is a protocol to allow ports to operate in idle or low power mode when there is no traffic to send. When EEE is enabled on a port it will advertise its EEE capability to its link partner. If the partner supports EEE they will operate in EEE mode. If the partner does not support EEE the ports will operate in legacy mode. This allows EEE capable switches to be deployed in existing networks avoiding backward compatibility issues.

- EEE is only applicable to OmniSwitch copper ports operating at 100/1000Mbps speed.
- The LLDP option in IEEE 802.3az standard is not currently supported.

The following CLI commands are added/modified as part of this feature implementation:

```
interfaces slot/port[-port] eee {enable | disable}
```

DHCP

DHCP Server
A DHCP server provides dynamic IP addresses on lease for client interfaces on a network. It manages a pool of IP addresses and information about client configuration parameters. The DHCP server obtains an IP address request from the client interfaces. After obtaining the requests, the DHCP server assigns an IP address, a lease period, and other IP configuration parameters, such as the subnet mask and the default gateway.

For enabling the DHCP-server in switch the files dhcpd.pcy and dhcpd.conf should be present in /flash/switch directory and should contain the information about ip address details assigned to client when DHCP-client sends DHCP-request.

The DHCP-server configuration file can be edited using the VI editor. The server can be restarted manually to update the changes made to the configuration file.
The leases offered by the DHCP and the DHCP server statistics can be viewed using the CLI.

The following CLI commands are added/modified as part of this feature implementation:

dhcp-server {enable | disable}
dhcp-server restart
show dhcp-server leases [ip-address ip_address | mac-address mac_address | type {static | dynamic} | count]
show dhcp-server statistics [packets | hosts | subnets | all]
clear dhcp-server statistics

Support of DHCP vendor class and switch type
The information of vendor class and switch type will be sent in DHCP discover or request packets during the Remote Configuration Load (RCL). The vendor class and switch type will be a part of DHCP option-60 filed as OmniSwitch-<Module Type> (Example: OmniSwitch-OS6250-24). The OXO server will send its information in Option-43 in DHCP OFFER or ACK, and AOS will decode Option-43 to give preference to the OXO server.

Preference to an OXO DHCP server
The DHCP client extracts the Vendor Specific Information (VSI) from the DHCP response packets (DHCPACK) to provide preference to the desired OXO DHCP server. The response from the OXO server is recognized with its VSI (Example: "alcatel.a4400.0").
The VSI string “alcatel.a4400.0” is hard coded and is used to configure the OXO server during the RCL process. To configure the OXO server after the RCL process, VSI filter is used.
The vsi-accept-filter can be configured in order to provide preference to the desired OXO DHCP server.

The following CLI commands are added/modified as part of this feature implementation:

ip interface dhcp-client [vlan vid ifindex id | vsi-accept-filter filter-string | release | renew | option-60 opt60_string | admin {enable | disable}]
show ip interface [name | vlan vlan id | dhcp-client]

IP helper “ip-source-filter” and persistency commands
The feature is enhanced to support configuration of Ingress Source Filtering (ISF) at VLAN level. When ISF is enabled at vlan level, switch shall also try to match the VLAN of the packet received along with IP/MAC/Port.

The following CLI commands are added/modified as part of this feature implementation:

ip helper dhcp-snooping ip-source-filter {vlan num | port slot/port[-port] | linkagg num} {enable | disable}
ip helper dhcp-snooping binding persistency {enable | disable}
show ip helper dhcp-snooping port
show ip helper dhcp-snooping ip-source-filter {vlan | port}

Metro

Control Frame Tunneling Stats
The Control protocol tunneling frame statistics feature is used to view the statistics of tunneling protocols using CLI commands. Only port level statistics can be collected in software. The statistics provided are as follows:

- RX frame statistics at UNI port level: On per port and per protocol basis, this is the number of frames that are trapped to CPU, number of frames tunneled, dropped, peered and MAC tunneled by the CPU operation; the source MAC of the last received frame on each port for each protocol.
- TX frame statistics at UNI port level: On per port and per protocol basis, this is the number of frames that are de-tunneled, and transmitted on UNI port.
- RX frame statistics at NNI port level: This is the number of frames that are trapped to CPU per NNI port, as their destination MAC matches with the configured tunnel MAC address and the number of frames discarded from the trapped frames.
- RX frame statistics at UNI profile level: This is the number of frames received on all ports bind to a UNI profile per protocol per UNI profile.

The following CLI commands are added/modified as part of this feature implementation:

show ethernet-service uni l2pt-statistics
clear ethernet-service uni l2pt-statistics
show ethernet-service uni-profile l2pt- statistics
clear ethernet-service uni-pofile l2pt-statistics

CF hardware tunnel

This feature is used to unconditionally forward all MAC tunnel packets irrespective of its UNI profile as and when required. This feature can be enabled or disabled using global flag "noMacTunnelFeature" in the AlcatelDebug.cfg file. The feature is functional after reboot. The global tunnel-mac PCL entry is not applied if this flag is enabled. Therefore, all the tunneled-mac PDUs will be hardware tunneled from NNI.
Once the system gets rebooted, all the mac-tunneled packets will not be trapped to CPU at NNI and will get tunneled from hardware.

Warning: When the "noMacTunnelFeature" is enabled, all MAC tunnel packets are tunneled and there is no check on which protocol it is associated with.
This feature does not introduce/modify any CLI commands.

PPPoE IA to support ATM default parameter

PPPoE-IA is a means by which the discovery packets of PPPoE are tagged at the access switch of the service provider using Vendor Specific Attributes (VSA) to add the line-specific information at the switch.
The purpose of an IA is to help service provider and the Broadband Network Gateway to distinguish between different end hosts connected over Ethernet to the access switch. The Ethernet frames from different users are appropriately tagged by the IA to provide this distinction. The AOS implementation of PPPoE-IA enables the rate limiting and insertion of VSA tags into the PPPoE Active Discovery (PAD) messages. The tag is allowed to contain information such as the base MAC address of the switch, interface, customer VLAN, system name, and a user-defined string depending on the configuration.
In the current release, PPPoE will support the circuit-ID encoding for the ATM parameter along with the Ethernet parameter for default circuit-ID.

The following CLI commands are added/modified as part of this feature implementation:

pppoe-ia circuit-id {default [atm] ascii [base-mac | system-name | interface | vlan | cvlan | interfacealias | user-string string | delimiter char]}
show pppoe-ia configuration

TDR

Time Domain Reflectometry (TDR) is a feature that is used to detect cable faults. This feature is deployed in networks where service providers and system administrators want to quickly diagnose the state of a cable during outages, before proceeding with further diagnosis.

Extended TDR is a feature that is used to know the attached cable characteristics. It is implemented by monitoring the transmitted signals amplitude received from the link partner. Both the tests are used to find out different parameter of a cable under different scenarios. The TDR Test (CLIs related to TDR-Test) can run on both 6250 and 6450 platforms. While the Extended-TDR Test (CLIs related to Extended-TDR Test) can run only on a switch with 1 GIG link capability (6450 switch).

When a TDR test is initiated, a signal is sent down a cable to determine the distance to a break or other discontinuity in the cable path. The length of time it takes for the signal to reach the break and return is used to estimate the distance to the discontinuity.

The following CLI commands are added/modified as part of this feature implementation:

interfaces tdr-test-start
interfaces no tdr-statistics
interfaces tdr-extended-test-start
interfaces no tdr-extended-statistics
show interfaces tdr-statistics
show interfaces tdr-extended-statistics

SECURITY

LPS Sticky mode
The LPS sticky mode provides the following enhancements in the learning window. Use the **port-security shutdown** command to configure LPS sticky mode.

Automatic conversion of MAC address:
The MAC addresses learned during the learning window are directly converted to static even if the convert to static option is not enabled. With **learn-as-static** option enabled, MACs will get directly learned as static during learning window. The **convert-to-static** option need not be manually enabled per port or globally when the learning window is active. This can be used only when **no-aging** is enabled.

MAC movement for the pseudo static MAC:
If a pseudo static MAC learned is present on more than one port in the same VLAN, the MAC will be allowed to move to the new port and get learned as pseudo static MAC. The option '**mac-move**' in learning window, will allow pseudo static MACs to move from one port to another based on the condition applied. This can be used only when '**no-aging**' is enabled.

Infinite learning window:
In infinite learning window mode the learning window will not expire. Infinite learning window can be configured for all the LPS learning options **boot-up**, **no-aging**, **learn-as-static**, and **mac-move** when the shutdown value is set to zero. For example, to configure the infinite learning window for no-aging, convert-to-static, and boot-up, enter:

-> port-security shutdown 0 no-aging enable convert-to-static enable boot-up enable

The following CLI commands are added/modified as part of this feature implementation:

port-security shutdown <num> no-aging enable [learn-as-static {enable|disable]
port-security shutdown <num> no-aging enable [mac-move {enable|disable]

Unique session id for radius accounting
RADIUS Accounting Session ID feature maintains a unique session ID in RADIUS accounting for 802.1x supplicant or non-supplicant clients, captive portal users, and management sessions like FTP, telnet, HTTP, console, HTTPS, and SSH.
When accounting is configured to use RADIUS accounting, at the start of service delivery, an Accounting Start packet is generated describing the type of service being delivered and the client it is being delivered to, and will send that to the RADIUS Accounting server. The RADIUS server will send back an acknowledgement that the packet has been received. At the end of service delivery, the client will generate an Accounting Stop packet describing the type of service that was delivered. This information is sent to the RADIUS accounting server, which will send back an acknowledgement that the packet has been received.
When unique session ID for RADIUS accounting is enabled, RADIUS attributes carry the specific authentication, authorization, and accounting details for the request and response along with the Acct-Session-Id, which gives a unique accounting ID. The unique accounting ID helps to match the start and stop records in a log file. The start and stop records for a given session must have the same Acct-Session-Id.

The following CLI commands are added/modified as part of this feature implementation:

aaa radius-server server host {hostname | ip_address} [hostname2 | ip_address2] key secret [retransmit retries] [timeout seconds] [auth-port auth_port] [acct-port acct_port] [nas-port {default | ifindex} | nas-port-id {enable | disable}] nas-port-type [xdsl | x75x25 | x25 | wireless-other | wireless-ieee-802-11 | virtual | sync | sdsl-symmetric-dsl | piafs | isdn-sync | isdn-async-v120 | isdn-async-v110 | idsl | hdlc-clear-channel | g3-fax | Ethernet | cable | async | adsl-dmt | adsl-cap-asymmetric-dsl] unique-acct-session-id {enable | disable}
show aaa server
show configuration snapshot aaa

Accept lower case lettering with MAC-based auth
Case sensitive MAC address Authentication can be applied to RADIUS server for authentication on supplicant, non-supplicant devices or for Captive portal authentication.

The **aaa radius-server** command configures or modifies RADIUS server attributes with different options for Authenticated Switch Access or 802.1X port access control.

The MAC address is sent in following attributes in Radius packets. The following data is sent as lowercase when MAC address format is selected as lowercase using the **mac-address-format lowercase** keywords:

- User-name and password, in Access-Request
- Accounting-Session-ID in Accounting-Request
- Calling-Station-ID in Access-Request packet

Case-sensitive MAC address authentication can be enabled using the **mac-address-format-status** option along with **aaa radius-server** command as follows:
CLI: aaa radius-server "Server1" mac-address-format-status enable

To specify that the MAC address format and other IDs sent to RADIUS server will be in lowercase use the command as follows:
CLI: aaa radius-server "Server1" mac-address-format-status enable mac-address-format lowercase

The **mac-address-format** can be applied only when **mac-address-format-statu**s is enabled.

UNP ingress/egress bandwidth limiting via radius
This feature applies maximum ingress and egress bandwidth limiting, maximum default depth on a port on the basis of UNP classification. When a user is successfully authenticated under a UNP policy either through RADIUS returned UNP attribute or through a local UNP policy, bandwidth limitations are applied on the port.

User can be a supplicant, non-supplicant, or a captive portal client. Bandwidth profiling per user is not supported. If there are multiple users authenticated under a port, then bandwidth limitation of the latest user overwrites the existing bandwidth limitations, if any.

The following CLI commands are added/modified as part of this feature implementation:

aaa user-network-profile name profile_name vlan vlan-id [hic {enable | disable}] [policy-list-name list_name] [maximum-ingress-bandwidth num [K(kilo) | M(mega)| G (giga)| T (tera)]] [maximum-egress-bandwidth num [K(kilo) | M(mega)| G (giga)| T (tera)]] [maximum-default-depth num [K(kilo) | M(mega)| G (giga)| T (tera)]]
show aaa user-network-profile
show 802.1x rate-limit

RADIUS non-supplicant/supplicant acct. including valid NAS-PORT

A Network Access Server (NAS) operates as a client of RADIUS. The client is responsible for passing user information along with various RADIUS attributes to the designated RADIUS server, and then act on the response returned.

AOS currently supports configuration of NAS port, NAS port ID, and NAS port type to contain in the access request and accounting request packet sent to the RADIUS server.

This feature is supported for 802.1x supplicant or non-supplicant clients, and Authenticated Switch Access users (ASA), that is, management sessions like FTP, telnet, HTTP, console, HTTPS, and SSH.

The following CLI commands are added/modified as part of this feature implementation:

aaa radius-server server host {hostname | ip_address} [hostname2 | ip_address2] key secret [retransmit retries] [timeout seconds] [auth-port auth_port] [acct-port acct_port] [nas-port {default | ifindex} | nas-port-id {enable | disable}] nas-port-type [xdsl | x75x25 | x25 | wireless-other | wireless-ieee-802-11 | virtual | sync | sdsl-symmetric-dsl | piafs | isdn-sync | isdn-async-v120 | isdn-async-v110 | idsl | hdlc-clear-channel | g3-fax | Ethernet | cable | async | adsl-dmt | adsl-cap-asymmetric-dsl]
show aaa server
show configuration snapshot aaa

Radius acct of Gig words

Acct-Input-Octets (type-42) and Acct-Output-Octets (type-43) are sent to the RADIUS Server in accounting packets. These statistics are used by the service providers for billing of users. As these two fields are 4 bytes longer as per Radius standard, it can support a maximum value of 4GB (2^32 -1= 4294967295). Whenever a user uses more than 4GB, the exact count of usage is lost.

Acct-Input-Gigawords (type-52) and Acct-Output-Gigawords (type-53) attributes are introduced to overcome the limitation due to the 4 bytes size of Acct-Input-Octets and Acct-Output-Octets with a maximum 4GB(2^32) of Octets can be represented. These attributes indicates how many times the Acct-Input-Octets and Acct-Output-Octets counter has wrapped the 4GB traffic over the course the service being provided.

Whenever the input octets and output octets exceeds 2^32-1 bytes, before sending accounting packet to the Radius Server, these octets are converted into multiples of 4GB and will be sent in Acct-Input-Gigawords (type-52) and Acct-Output-Gigawords (type -53) attributes. For every 4GB traffic, the value is incremented and the remaining amount of traffic is displayed in Acct-Input-Octets and Acct-Output-Octets attribute.

Radius attribute calling station id

Calling-Station-ID is used by the NAS (Network Access Server) in an Access-Request packet to indicate that a call is being received. Based on the Calling-Station-ID or Calling-Station-ID attribute, the RADIUS server sends Access-Accept to answer the call or an Access-Reject to reject the call.

Calling-Station-ID attribute is supported in Access-Request and Accounting-Request packet for Authenticated Switch Access users (ASA) users, supplicant and non-supplicant users, and captive portal users.
The following table shows the default behavior of Calling-Station-Id attribute in RADIUS packets:

RADIUS Message	ASA users	Supplicant users	Non-Supplicant users	Captive Portal users
Access-Request	Not applicable	Access request is sent with Calling-Station-Id (MAC address of the supplicant user) connecting to the OmniSwitch.	Access request is sent with Calling-Station-Id (MAC address of the non-supplicant user) connecting to the OmniSwitch.	Access request is sent with Calling-Station-ID (MAC address of the captive portal user) connecting to the OmniSwitch.
Accounting-Request	Account request message is sent with Calling-Station-Id (IP address of the ASA users/host) connecting to the OmniSwitch.	Accounting request is sent with Calling-Station-Id (MAC address of the supplicant user) connecting to the OmniSwitch.	Accounting request is sent with Calling-Station-Id (MAC address of the non-supplicant user) connecting to the OmniSwitch.	Access request is sent with Calling-Station-ID (MAC address of the captive portal user) connecting to the OmniSwitch.

However, by setting the "radCallingStationOId" variable in AlcatelDebug.cfg file, the Calling-Station-Id attribute behavior can be set to the following:

RADIUS Message	ASA users	Supplicant users	Non-Supplicant users	Captive Portal users
Access-Request	Not applicable	Access request is sent with Calling-Station-Id (MAC address of the supplicant user) connecting to the OmniSwitch.	Not applicable	Not applicable
Accounting-Request	Account request message is sent with Calling-Station-Id (IP address of the ASA users/host) connecting to the OmniSwitch.	Accounting request is sent with Calling-Station-Id (IP address of the supplicant user) connecting to the OmniSwitch.	Accounting request is sent with Calling-Station-Id (IP address of the non-supplicant user) connecting to the OmniSwitch.	Accounting request is sent with Calling-Station-Id (IP address of the captive portal user) connecting to the OmniSwitch.

SYSTEM

Improved L2 multicast convergence after takeover
Currently on OS6250/OS6450 switches, multicast layer 2 traffic is disrupted after takeover happens in Stack systems. After takeover, a timer of 120 seconds is started, during which, new flows are not learned on the new primary CMM. A drop filter is applied by IPMS NI for any new flows. This period of 120 seconds is also known as “quiet” period.

- During this period, ageing of any flows does not happen.
- During this period, new primary CMM does not have any source and forwarding information.

- The flows learned on the NI that goes down during the takeover is not forwarded during this quiet period.
- The flows received on aggregable ports are dropped on the NI which goes down during takeover.
- Once the timer stops, then all the existing flows learned on NI are flushed. This triggers the relearning of all flows causing a disruption of 3-4 seconds. The flow information is populated on the new primary CMM.

SNMP healthmonportrap per port
Health monitoring is performed for all the ports in an AOS switch when the threshold value is above or below the configured value. However, the health-monitoring trap can now be disabled, filtered, or enabled for specific ports in an AOS switch the "receive" and "transmit" statistics for the health monitoring are currently maintained on a per slot/port basis. The health monitoring traps are generated only for the ports that are configured for the traps and the port-trap threshold is enabled.

Health threshold monitoring is enabled by default on all chassis ports. The **health threshold port-trap** command is used to enable or disable the health threshold monitoring on a slot, port, or a range of ports. Health threshold monitoring traps can be enabled only on uplink ports or only on a set of configured ports. This is to prevent the NMS from being flooded with too many threshold monitoring messages in big networks and prevent overwriting of threshold monitoring traps.

To verify health threshold monitoring settings for a slot, port, or a range of ports, use the **show health threshold port-trap** command.
The following CLI commands are added/modified as part of this feature implementation:

show health threshold
health threshold port-trap
show health threshold port-trap

show QoS queue statistics in bits/second
The QoS queue statistics output command now displays "Rate of Mbits transmitted per port/cos" and "Rate of Mbits dropped per port/cos". A new show cli "show qos queue statistics" command is introduced to display Statistics of packet transmitted per port/cos and Statistics of Packet dropped per port/cos.

The following CLI commands are added/modified as part of this feature implementation:

show qos queue statistics

New statistics display with filters for ingress traffic
The accounting function is supported with both policy rule as well as policy list. Only ingress and UNP type list is supported. The number of bytes and packets satisfying a particular user policy can be tracked now. The policy rule is set with a new parameter that enables the accounting function. The filters to identify the traffic pattern that needs to be accounted are specified in the policy condition using the existing policy condition framework. For pure accounting function, the action would be simply "disposition accept". No new action is required. However any other action that can be configured using the existing frame work is also be supported. The accounting function applies for all frames matching the policy rule regardless of the configured policy action.

The following CLI commands are added/modified as part of this feature implementation:

show active policy rule [rule_name] accounting
show active policy list [rule_name] accounting [details]
show policy rule

show active policy rule
policy rule <rule_name > accounting
policy rule <rule_name > no accounting

SAM triggered CLI configuration change

This is a Metro feature. SAM is the SNMP agent in the switch that has the ability to send traps to the management station. In this feature, a trap informs the management station when the switch configuration is saved using CLI/SNMP/WEB.

If there are any configuration changes, a trap is sent to Service Aware Manager (SAM) to enforce a poll when configuration file is saved. The running configuration is not saved in the configuration file (boot.cfg) until the user commits the changes using the write memory or copy running-config working command. The configuration changes that are not committed are not detected by the switch until these commands are applied.

The related traps are raised on the following commands:

- write memory
- write memory flash-synchro
- copy running-config working

The trap can also be raised using the **debug trap generate** command.

Storm control options

A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. The traffic storm control feature prevents LAN ports from being disrupted by a broadcast, multicast or unknown unicast traffic storm on a physical interface. This storm control is applied on per port basis .In this feature, individual rate limit shall be applied for each type of flood traffic (unknown unicast, multicast and broadcast) on a port. The storm is controlled by global port rate limit. The configured rate applies to both broadcast flooding and unknown unicast flooding. Optionally, the rate control can also be applied to multicast flooding.

The following CLI commands are added/modified as part of this feature implementation:

interfaces {slot | slot/port | slot/port1-port2} flood {broadcast | multicast | unknown-unicast | all} rate {mbps num | pps num | percentage num | default}
interfaces {slot | slot/port | slot/port1-port2} flood {broadcast | multicast | unknown-unicast | all} {enable | disable}
show interfaces [slot | slot/port | slot/port1-port2] flood rate [broadcast | multicast | unknown-unicast]

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

No.	Trap Name	Platforms	Description
			for this condition are configured 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

No.	Trap Name	Platforms	Description
			violated.
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

No.	Trap Name	Platforms	Description
			one port of the link aggregate 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.

No.	Trap Name	Platforms	Description
95	chassisTrapsPossibleDuplicateMac	all	The old PRIMARY element cannot 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

No.	Trap Name	Platforms	Description
			a local or remote threshold 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

No.	Trap Name	Platforms	Description
			address is assigned to the DHCP 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

No.	Trap Name	Platforms	Description
			test traffic. Once this trap is 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

No.	Trap Name	Platforms	Description
213	Reserved	all	Reserved
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	ConfigSavedSucceededTrap	All	Config change trap is sent each time a config is saved via Cli/Snmp/Web.

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]

Unsupported MIBs

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

Feature	MIB
BGP	AlcatelIND1Bgp IETF_BGP4
DVMRP	AlcatelIND1Dvmrp IETF_DVMRP_STD_DRAFT
IPSec	AlcatelIND1IPsec.mib
IPX	AlcatelIND1Ipx.mib
IS-IS	AlcatelIND1Isis IETF_ISIS
Multicast Routing	AlcatelIND1Ipmrm AlcatelIND1IpMcastDraft
OSPF/OSPFv3	AlcatelIND1DrcTm AlcatelIND1Ospf AlcatelIND1Ospf3 IETF_OSPF IETF_OSPFv3 IETF_OSPF_TRAP
PIM	AlcatelIND1Pim AlcatelIND1PimBsrDraft AlcatelIND1PimStdDraft IETF_PIM
Quality of Service (QoS)	IETF_P_BRIDGE
SLB	AlcatelIND1Slb.mib
Traffic Anomaly Detection	AlcatelIND1Ns

Unsupported MIB Variables

MIB Name	Unsupported MIB variables / tables
AlcatelIND1AAA	aaauProfile aaaAuthenticatedUserTable aaaAvlanConfig aaaAuthVlanTable aaaAvlanAddressTable aaaHicSvrTable aaaHicAllowedTable aaaHicOverrideTable aaaHicHostTable aaaHicConfigInfo
AlcatelIND1Chassis	chasControlVersionMngt chasEntPhysAdminStatus [powerOn, powerOff] chasEntPhysAdminStatus [reset] chasEntPhysAdminStatus [takeover] chasSupervisionRfsLsTable
AlcatelIND1Dot1Q	qPortVlanForceTagInternal
AlcatelIND1EService.mib	alaEServiceTable alaEServiceNniSvlanTable alaEServicePortTable alaEServiceSapTable alaEServiceSapUniTable alaEServiceSapCvlanTable

MIB Name	Unsupported MIB variables / tables
	alaEServiceSapProfileTable alaEServiceUNIProfileTable alaEServiceInfo
AlcatelIND1Eoam.mib	alaCfmBase alaCfmMepTable
AlcatelIND1GroupMobility	vPortIpBRuleTable vMacIpBRuleTable vMacPortProtoBRuleTable vCustomRuleTable vMacPortIpBRuleTable vMacPortBRuleTable vPortProtoBRuleTable
AlcatelIND1Health	healthDeviceTemperatureCmmCpuLatest healthDeviceTemperatureCmmCpu1MinAvg healthDeviceTemperatureCmmCpu1HrAvg healthDeviceTemperatureCmmCpu1HrMax
AlcatelIND1InLinePowerEthernet_mib	alaPethPsePortTable alaPethMainPseTable alaPethMainTable
AlcatelIND1Ip. mib	alaIpInterfaceTunnelSrcAddressType alaIpInterfaceTunnelSrc alaIpInterfaceTunnelDstAddressType alaIpInterfaceTunnelDst
AlcatelIND1IPv6.mib	alaIPv6ConfigTunnelV4Source alaIPv6ConfigTunnelV4Dest
AlcatelIND1Ipms	alaIpmsForwardSrcIpAddr alaIpmsForwardSrcIfIndex
AlcatelIND1UDPRelay	iphelperForwOption
AlcatelIND1LAG	alcLnkaggAggEniActivate alcLnkaggSlotTable
AlcatelIND1Pcam	alcatelIND1PCAMMIBObjects alaCoroL3HrePerModeTable alaCoroL3HrePerCoronadoStats Table alaCoroL3HreChangeTable
AlcatelIND1Port	esmPortCfgLongEnable esmPortCfgRuntEnable esmPortCfgRuntSize esmPortPauseSlotTime esmPortCfgFLow alcether10GigTable

MIB Name	Unsupported MIB variables / tables
AlcatelIND1QoS	alaQoSAppliedRuleReflexive alaQoSActionSourceRewriteIpAddr alaQoSActionSourceRewriteIpAddrStatus alaQoSActionSourceRewriteIpMask alaQoSActionTable alaQoSActionSourceRewriteNetworkGroup alaQoSActionTable alaQoSActionSourceRewriteNetworkGroupStatus alaQoSActionTable alaQoSActionDestinationRewriteIpAddr alaQoSActionTable alaQoSActionDestinationRewriteIpAddrStatus alaQoSActionTable alaQoSActionDestinationRewriteIpMask alaQoSActionTable alaQoSActionDestinationRewriteNetworkGroup alaQoSActionTable alaQoSActionDestinationRewriteNetworkGroupStatus alaQoSActionTable alaQoSActionLoadBalanceGroup alaQoSActionTable alaQoSActionLoadBalanceGroupStatus alaQoSActionTable alaQoSActionPermanentGatewayIpAddr alaQoSActionTable alaQoSActionPermanentGatewayIpAddrStatus alaQoSActionTable alaQoSActionAlternateGatewayIpAddr alaQoSActionAlternateGatewayIpAddrStatus alaQoSActionName alaQoSActionMinimumBandwidth alaQoSActionPermanentGatewayIpAddr alaQoSActionDscp alaQoSActionMapFrom alaQoSActionMapTo alaQoSActionMapGroup alaQoSActionMapGroupStatus alaQoSAppliedActionSourceRewriteIpAddr alaQoSAppliedActionSourceRewriteIpAddrStatus alaQoSAppliedActionSourceRewriteIpMask alaQoSAppliedActionSourceRewriteNetworkGroup alaQoSAppliedActionSourceRewriteNetworkGroupStatus alaQoSAppliedActionDestinationRewriteIpAddr alaQoSAppliedActionDestinationRewriteIpAddrStatus alaQoSAppliedActionDestinationRewriteIpMask alaQoSAppliedActionDestinationRewriteNetworkGroup alaQoSAppliedActionDestinationRewriteNetworkGroupStatus

MIB Name	Unsupported MIB variables / tables
	alaQoSAppliedActionLoadBalanceGroup alaQoSAppliedActionLoadBalanceGroupStatus alaQoSAppliedActionPermanentGatewayIpAddr alaQoSAppliedActionPermanentGatewayIpAddr Status alaQoSAppliedActionAlternateGatewayIpAddr alaQoSAppliedActionAlternateGatewayIpAddrS tatus alaQoSAppliedActionName alaQoSAppliedActionMaximumBandwidth alaQoSAppliedActionPermanentGatewayIpAddr alaQoSAppliedActionDscp
AlcatelIND1QoS	alaQoSConditionInnerSourceVlanStatus alaQoSConditionInnerSourceVlan alaQoSConditionInner8021pStatus alaQoSConditionInner8021p alaQoSConditionIpv6NH alaQoSConditionIpv6NHStatus alaQoSConditionIpv6FlowLabel

MIB Name	Unsupported MIB variables / tables
	alaQoSConditionIpv6FlowLabelStatus alaQoSConfigQMMACGroup alaQoSConfigQMPath alaQoSConfigNatTimeout alaQoSConfigAppliedNatTimeout alaQoSConfigReflexiveTimeout alaQoSConfigAppliedReflfexiveTimeout alaQoSConfigFragmentTimeout alaQoSConfigAppliedFragmentTimeout alaQoSConfigAppliedDefaultRoutedDisposition alaQoSConfigClassifyFragments alaQoSConfigAppliedClassifyFragments alaQoSConfigQMPage alaQoSPortCOS0MinimumBandwidth alaQoSPortCOS0MinimumBandwidthStatus alaQoSPortCOS1MinimumBandwidth alaQoSPortCOS1MinimumBandwidthStatus alaQoSPortCOS2MinimumBandwidth alaQoSPortCOS2MinimumBandwidthStatus alaQoSPortCOS3MinimumBandwidth alaQoSPortCOS3MinimumBandwidthStatus alaQoSPortCOS4MinimumBandwidth alaQoSPortCOS4MinimumBandwidthStatus alaQoSPortCOS5MinimumBandwidth alaQoSPortCOS5MinimumBandwidthStatus alaQoSPortCOS6MinimumBandwidth alaQoSPortCOS6MinimumBandwidthStatus alaQoSPortCOS7MinimumBandwidth alaQoSPortCOS7MinimumBandwidthStatus alaQoSPortDefaultQueues alaQoSPortAppliedDefaultQueues alaQoSPortPdiTable alaQoSSlotPcamTable alaQoSPortProtocolTable alaQoSSlotProtocolTable alaQoSSlotDscpTable alaQoSRuleReflexive
AlcatelIND1SystemService	systemUpdateStatusTable
AlcatelIND1VlanManager	vlanIpxNet vlanIpxEncap vlanIpxRipSapMode vlanIpxDelayTicks vlanIpxStatus vlanSetIpxRouterCount vlanSetMultiRtrMacStatus
AlcatelIND1UDLD.mib	alcatelIND1UDLDMIBObjects alaUdldPortConfigTable alaUdldPortStatsTable alaUdldPortNeighborStatsTable
AlcatelIND1WebMgt	alaIND1WebMgtRFSConfigTable alaIND1WebMgtHttpPort alaIND1WebMgtHttpsPort
IETF_802_1ag.mib	Dot1agCfmStackTable Dot1agCfmDefaultMdLevelTable Dot1agCfmMd

MIB Name	Unsupported MIB variables / tables
	dot1agCfmMdTable dot1agCfmMa dot1agCfmMaTable dot1agCfmMaMepListTable dot1agCfmMepTable dot1agCfmLtrTable dot1agCfmMepDbTable
IEEE_802_1X	dot1xAuthDiagTable dot1xAuthSessionStatsTable dot1xSuppConfigTable dot1xSuppStatsTable
IETF_BRIDGE	dot1dTpPortTable dot1dStaticTable
IETF_ENTITY	entLogicalTable entLPMappingTable entAliasMappingTable
IETF_ETHERLIKE	dot3CollTable dot3StatsSQETestErrors dot3StatsInternalMacTransmitErrors dot3StatsCarrierSenseErrors dot3StatsInternalMacReceiveErrors dot3StatsEtherChipSet dot3StatsSymbolErrors dot3ControlInUnknownOpcodes
IETF_IF	ifRcvAddressTable ifTestTable
IETF_IP_FORWARD_MIB	ipForwardTable
IETF_IPMROUTE_STD	ipMrouteScopeNameTable
IETF_MAU (RFC 2668)	rpMauTable rpJackTable broadMauBasicTable ifMauFalseCarriers ifMauTypeList ifMauAutoNegCapability ifMauAutoNegCapAdvertised ifMauAutoNegCapReceived
IETF_OSPF (RFC 1850)	ospfAreaRangeTable
IETF_OSPF_TRAP	ospfTrapControl
IETF-PIM	pimRPTable
IETF_P_BRIDGE	dot1dExtBase dot1dPortCapabilitiesTable dot1dPortPriorityTable dot1dUserPriorityRegenTable dot1dTrafficClassTable dot1dPortOutboundAccessPriorityTable dot1dPortGarpTable dot1dPortGmrpTable dot1dTpHCPortTable dot1dTpPortOverflowTable
IETF_Q_BRIDGE (RFC 2674)	dot1qTpGroupTable dot1qForwardAllTable dot1qForwardUnregisteredTable dot1qStaticMulticastTable dot1qPortVlanStatisticsTable

MIB Name	Unsupported MIB variables / tables
	dot1qPortVlanHCStatisticsTable dot1qLearningConstraintsTable
IETF_RIPv2	rip2IfConfDomain
IETF_RMON	hostControlTable hostTable hostTimeTable hostTopNControlTable hostTopNTable matrixControlTable matrixSDTable matrixDSTable filterTable channelTable bufferControlTable captureBufferTable
IETF_RS_232 (RFC 1659)	all synchronous and sdlc objects and tables rs232SyncPortTable
IETF_SNMPv2	sysORTable snmpTrap sysORLastChange
IETF_SNMP_ COMMUNITY (RFC 2576)	snmpTargetAddrExtTable
IETF_SNMP_ NOTIFICATION (RFC 2576)	snmpNotifyTable snmpNotifyFilterProfileTable snmpNotifyFilterTable
IETF_SNMP_PROXY (RFC 2573)	snmpProxyTable
IETF_SNMP_TARGET (RFC 2573)	snmpTargetAddrTable snmpTargetParamsTable snmpTargetSpinLock
IETF_SNMP_USER_BASED_SM (RFC 2574)	UsmUser
IETF_SNMP_VIEW_BASED_ACM (RFC 2575)	vasmMIBViews

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.

Security

PR	Description	Workaround
178982	Captive portal user has to enter credentials every re-authentication period. Once re-authentication period expires, user is re-directed to captive portal for re-authentication.	Increase the re-authentication timeout period/value (for example to 24 hours) to reduce frequency of re-authentication.
180335	When user traffic is received immediately after boot-up, non-supplicant user authentication fails with the authentication server down error message.	Configure server down policy option on the switch using the 802.1x auth-server-down policy command followed by a User-Network-Policy or block, condition. If user connection fails the first time due to server connectivity issues, the user is authenticated correctly in the next cycle.

System

General

PR	Description	Workaround
179358	The following error message is observed rarely on some OS 6450s during boot-up "+++ ==PHYDRV== (1 : 9 : 5) HALP_config_phy_set_speed_7 - failed to configure speed " There is no impact on functionality of the port when this message is seen on console during boot-up.	There is no known workaround at this time.
179635	When the other-end of a fiber link is terminated at any Fast Ethernet PHY (max - capability of 100 Mbps), then only pairs 1,2,3,and 6 are used in cable & pairs 4,5,7, and 8 are not used. Hence in such scenario, distance to fault will be observed always on these pairs (4,5 and 7,8).	There is no known workaround at this time.
181640	DDM values not displayed on 1 Gig (OS-GNI-U2) expansion slot of OS6450-C24.	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.

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 6.6.4.R01 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 6.6.4.R01.
- OmniSwitch 6450 models being upgraded to AOS 6.6.4.R01.

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.
- Read and understand the **AOS 6.6.3 File System Error Issue in Appendix C** 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 6.6.4.R01 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 6.6.4.R01.

Version Requirements – Upgrading to AOS Release 6.6.4.R01

Version Requirements to Upgrade to AOS Release 6.6.4.R01			
	AOS	**Uboot/Miniboot**	**CPLD**
6250-24/P24/8M/24M	6.6.4.177.R01 GA	6.6.3.259.R01 (minimum) 6.6.4.158.R01 (new - optional)	12 (minimum) 14 (new - optional)
6450-10/10L/P10/P10L 6450-24/P24/48/P48 6450-U24 6450-24L/P24L/48L/P48L	6.6.4.177.R01 GA 6.6.4.177.R01 GA 6.6.4.177.R01 GA 6.6.4.177.R01 GA	6.6.3.259.R01 6.6.3.259.R01 6.6.3.259.R01 6.6.4.54.R01 (new)	6 (new) 11 (new) 6 (new) 11 (new)
• 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 are newly released versions in 6.6.4.R01. • CPLD versions 14, 6, and 11 are newly released versions in 6.6.4.R01. • Uboot/Miniboot version 6.6.3.259R01 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 6.6.4.R01.

Upgrading to AOS Release 6.6.4.R01

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 6.6.4.R01 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 6.6.4 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 6.6.4 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 (if required)
   - AOS Files – KFbase.img, KFeni.img, KFos.img, KFsecu.img
   - CPLD File - KFfpga_upgrade_kit
2. FTP (Binary) the 6.6.4.R01 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 6.6.4.R01 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 6.6.4.R01.

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 6.6.4.R01, 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       6.6.4.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
```

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 6.6.4.R01 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 6.6.4.R01.
- OmniSwitch 6450 models being downgraded from AOS 6.6.4.R01.

Prerequisites

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

- 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 6.6.4.R01 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 downgrade procedures could result in the malfunctioning of the switch. All steps in these procedures should be reviewed before beginning.

OmniSwitch Downgrade Requirements

These tables list the required Uboot/Miniboot, CPLD and AOS combinations for downgrading an OmniSwitch. The Uboot/Miniboot and CPLD versions must be downgraded to the versions listed below to support the respective AOS version.

Version Requirements – Downgrading to AOS Release 6.6.3.R01

Version Requirements to Downgrade to AOS 6.6.3.R01				
	AOS	**Uboot**	**Miniboot**	**CPLD**
6250-24/P24/8M/24M	6.6.3.439.R01 (GA) or later maintenance	6.6.3.259.R01	6.6.3.259.R01	12
6450-10/10L/P10/P10L	6.6.3.439.R01 (GA) or later maintenance	6.6.3.259.R01	6.6.3.259.R01	5
6450-24/P24/48/P48	6.6.3.439.R01 (GA) or later maintenance	6.6.3.259.R01	6.6.3.259.R01	10
6450-U24	6.6.3.439.R01 (GA) or later maintenance	6.6.3.259.R01	6.6.3.259.R01	5
6450-24L/P24L/48L/P48L	Not Supported	---	---	--

- This table applies to factory shipped switches that need to be downgraded to AOS 6.6.3.R01 from AOS 6.6.4.R01.
- Contact Service & Support for information on downgrading to a version other than the ones listed above.
- The Uboot/Miniboot and CPLD must be downgraded to the versions shown above to support AOS Release 6.6.3.R01.

- If downgrading a factory shipped OS6250 to AOS Release 6.6.3.R01 the AOS, Uboot/Miniboot, and CPLD must all be downgraded to the versions listed above.
- If downgrading a factory shipped OS6450 to AOS Release 6.6.3.R01 the AOS, and CPLD must be downgraded to the version listed above. The Uboot/Miniboot will already be at the correct version.

- OS6450-24/P24/48/P48/U24 models require the CPLD to be downgraded before downgrading the AOS.
- The OS6450-24L/P24L/48L/P48L cannot be downgraded, AOS Release 6.6.4 is required.

Downgrading to AOS 6.6.3.R01 – OS6250 Models

Downgrading to AOS 6.6.3.R01 from AOS 6.6.4.R01 consists of the following steps. The steps must be performed in order. Observe the following prerequisites before performing the steps as described below:

- Refer to the Version Requirements table to determine the proper code versions.
- Download the appropriate AOS, Uboot/Miniboot, and CPLD files from the Service & Support website.

Summary of Steps

1. FTP all the required files to the switch
2. Downgrade the Uboot/Miniboot and AOS images as required (Reboot Required)
3. Downgrade the CPLD as required. (switch automatically reboots)
4. Verify the downgrade.

Downgrading - Step 1. FTP the 6.6.3 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 6.6.3.R01 archive from the Service & Support website. The archive will contain the following files to be used for the downgrade:
   - Uboot/Miniboot File – kfu-boot.bin, kfminiboot.bs
   - AOS Files – Kfbase.img, KFeni.img, KFos.img, KFsecu.img
   - CPLD File – KFfpga_upgrade_kit
2. FTP (Binary) the 6.6.3.R01 Uboot/Miniboot files listed above to the **/flash** directory on the primary CMM.
3. FTP (Binary) the CPLD downgrade kit listed above to the **/flash** directory on the primary CMM, if required.
4. FTP (Binary) the 6.6.3.R01 image files listed above to the **/flash/working** directory on the primary CMM.

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 Uboot/Miniboot and AOS

Follow the steps below to downgrade the Uboot/MiniBoot and AOS to version 6.6.3. This step will downgrade both Uboot/Miniboot and AOS once the switch/stack is rebooted.

Note: If no Uboot/Miniboot downgrade is required skip to step 2 and reboot the switch with the proper AOS images to complete the downgrade.

1. Execute the following CLI command to downgrade the Uboot/Miniboot File 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 downgraded version.

WARNING: DO NOT INTERRUPT the downgrade 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 and AOS to 6.6.3 version.
   -> reload working no rollback-timeout
3. Once the switch reboots, certify the new versions:
   - If you have a single CMM enter:
   -> copy working certified
   - If you have redundant CMMs enter:
   -> copy working certified flash-synchro

Downgrading - Step 3. Downgrade the CPLD

Follow the steps below to downgrade the CPLD. 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 downgrade, the switch will stop passing traffic. When the downgrade 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 downgrade:
   -> update fpga cmm

The switch will downgrade the CPLD and reboot.

Stack Procedure

Downgrading a stack requires all elements of the stack to be downgraded. The CPLD downgrade 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 downgrade for all the elements of a stack.
   -> update fpga ni all

The stack will downgrade the CPLD and reboot.

Proceed to Verifying the Downgrade to verify the proper versions.

Downgrading to AOS 6.6.3.R01 – OS6450-24/P24/48/P48/U24 Models

Downgrading to AOS 6.6.3.R01 from AOS 6.6.4.R01 consists of the following steps. The steps must be performed in order. Observe the following prerequisites before performing the steps as described below:

- Refer to the Version Requirements table to determine the proper code versions.
- Download the appropriate AOS images and CPLD files from the Service & Support website.

Summary of Steps

1. FTP all the required files to the switch
2. Downgrade the CPLD.
3. Downgrade the AOS images.
4. Verify the downgrade.

Downgrading - Step 1. FTP the 6.6.3 Files to the Switch

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

1. Download and extract the 6.6.3.R01 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
   - CPLD File – KFfpga_upgrade_kit
2. FTP (Binary) the CPLD downgrade kit listed above to the **/flash** directory on the primary CMM, if required.
3. FTP (Binary) the 6.6.3.R01 image files listed above to the **/flash/working** directory on the primary CMM.

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 CPLD

Follow the steps below to downgrade the CPLD. 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 downgrade, the switch will stop passing traffic. When the downgrade 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 downgrade:
   -> update fpga cmm

The switch will downgrade the CPLD and reboot.

Stack Procedure

Downgrading a stack requires all elements of the stack to be downgraded. The CPLD downgrade 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 downgrade for all the elements of a stack.
   -> update fpga ni all

The stack will downgrade the CPLD and reboot.

Downgrading - Step 3. Downgrade the AOS

Follow the steps below to downgrade the AOS to version 6.6.3.

1. Reboot the switch. **This will update the AOS to 6.6.3 version**.
   -> reload working no rollback-timeout
2. Once the switch reboots, certify the new versions:
   - 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 to verify the proper versions.

Verifying the Downgrade

The following examples show what the code versions should be after downgrading from AOS Release 6.6.4.R01.

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

Verifying the Software Downgrade

To verify that the AOS software was successfully downgraded 6.6.4.R01, use the show microcode command as shown below. The display below shows a successful image file downgrade.

```
-> show microcode
Package          Release         Size       Description
-----------------+--------------+-----------+-----------------------------------------------
KFbase.img       6.6.3.R01    15510736  Alcatel-Lucent Base Software
KFos.img         6.6.3.R01     2511585   Alcatel-Lucent OS
KFeni.img        6.6.3.R01     5083931   Alcatel-Lucent NI software
KFsecu.img       6.6.3.R01      597382   Alcatel-Lucent Security Management
```

Verifying the U-Boot/Miniboot and CPLD Downgrade
To verify that the CPLD was successfully downgraded 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            : 6.6.3.259.R01,
Product ID Register         : 05
Hardware Revision Register  : 30
FPGA Revision Register      : 012
```

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:          0012/00,
  UBOOT Version :             n/a,
  UBOOT-miniboot Version:     6.6.3.259.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 downgraded version as shown above.

Remove the CPLD and Uboot/Miniboot Downgrade Files
After the switch/stack has been downgraded and verified the downgrade files can be removed from the switch.

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

Appendix C: AOS 6.6.3 File System Error Issue

This section explains the AOS 6.6.3 File System Error issue, identified in PR 174986, that may exist on some OmniSwitch OS6250 or OmniSwitch 6450 switches running an AOS 6.6.3.R01 version of code. The issue may exist on a switch that has failed to reboot or on a switch that is operational and running an AOS Release 6.6.3.R01 version of code listed below. This issue has been identified and can be fixed with a software upgrade.

AOS Release 6.6.3.439.R01 fixes the AOS 6.6.3 File System Error issue. However, it's possible that a switch running an earlier AOS Release 6.6.3.R01 version of code may have experienced the issue. All impacted switches must first be checked prior to any AOS upgrade. An identification and recovery procedure is available from Service & Support.

Impacted Switches

A limited number of installed switches are impacted by this problem as listed below:

- OmniSwitch 6450 switches, running build AOS 6.6.3.372.R01 (GA) through maintenance build AOS 6.6.3.413.R01, all manufacturing part numbers.
- OmniSwitch 6250 switches, running build AOS 6.6.3.372.R01 (GA) through maintenance build AOS 6.6.3.413.R01, only the manufacturing part numbers listed below are affected:

Description	Revision
OS6250-24	903091-90
OS6250-8M	903092-90
OS6250-24M	903093-90
OS6250-24MD	903094-90
OS6250-P24	903095-90
OS6250-P24	903096-90
BOS6250-P48	903097-90
BOS6250-48	903098-90
OS6250-24	903099-90
DNV6250-P48	903100-90

Problem Identification

There are two methods for identifying a switch with the issue as listed below:

- The size of the KFbase.img file will be '0' bytes
- A file system check will identify an error with the KFbase.img file

Solution

A recovery procedure is available for OmniSwitch 6250s and 6450s that have experienced the flash driver issue. For step-by-step instructions on identifying and recovering a switch refer to the followingTech Tips on the Service & Support site :

- Tech Tip 12505 – OmniSwitch 6450s
- Tech Tip 12506 – OmniSwitch 6250s

Appendix D: Existing Software Feature Support

6.6.3 Hardware and Software Feature Summary

The following hardware and software features were introduced in AOS Release 6.6.3 on the OmniSwitch 6250 and OmniSwitch 6450.

OmniSwitch 6450-10(L)[1]
Provides 8 RJ-45 10/100/1000BaseT Ethernet ports, 2 SFP/RJ-45 combo ports, 2 SFP non-combo ports, and an internal AC power supply.

Note: The OmniSwitch 6450-10 was initially released in 6.6.2.R02.

OmniSwitch 6450-24[2]
Provides 24 RJ-45 10/100/1000BaseT Ethernet ports, 2 non-combo SFP+ ports, 1 expansion slot for optional stacking or uplink modules, an internal AC power supply, and an optional slide-in 90W AC or DC redundant power supply.

OmniSwitch 6450-48[2]
Provides 48 RJ-45 10/100/1000BaseT Ethernet ports, 2 non-combo SFP+ ports, 1 expansion slot for optional stacking or uplink modules, an internal AC power supply, and an optional slide-in 90W AC or DC power supply.

OmniSwitch 6450-P10(L)[1]
Provides 8 RJ-45 10/100/1000BaseT 802.3at Power Over Ethernet ports, 2 SFP/RJ-45 combo ports, 2 SFP non-combo ports, and an internal AC power supply.

OmniSwitch 6450-P24[2]
Provides 24 RJ-45 10/100/1000BaseT 802.3at Power Over Ethernet ports, 2 non-combo SFP+ ports, 1 expansion slot for optional stacking or uplink modules, an internal AC power supply, and an optional external 550W AC power supply, no other external power supplies supported.

OmniSwitch 6450-P48[2]
Provides 48 RJ-45 10/100/1000BaseT 802.3at Power Over Ethernet ports, 2 non-combo SFP+ ports, 1 expansion slot for optional stacking or uplink modules, an internal AC power supply, and an optional external 900W AC power supply, no other external power supplies supported.

OmniSwitch 6450-U24[2]
Provides 22 SFP ports, 2 RJ-45/SFP combo ports, 2 non-combo SFP+ ports, 1 expansion slot for optional stacking or uplink modules, an internal AC power supply, and an optional slide-in 90W AC or DC power supply.

- The 'Lite' models support 10/100 only on the 8 RJ-45 non-combo ports and can be upgraded to support 10/100/1000 with the OS6450-10L-UPGD Upgrade License.
- 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.

OS6450-GNI-C2
Provides 2 RJ-45 10/100/1000BaseT Ethernet ports. Inserts into the expansion slot at the rear of the chassis.

OS6450-GNI-U2
Provides 2 SFP ports. Inserts into the expansion slot at the rear of the chassis.

OS6450-XNI-U2
Provides 2 SFP+ ports that can be used for stacking capability. Inserts into the expansion slot at the rear of the chassis. This module can not be used as an uplink module. Supports stacking only with 1m and 60cm direct attached copper SFP+ transceiver cable.

OS6450-BP (PS-90W-AC)
90W slide-in AC backup power supply. Provides backup power to one non-PoE switch. Inserts into the backup power supply bay at the rear of the chassis.

OS6450-BP-D (PS-90W-DC)
90W slide-in DC backup power supply. Provides backup power to one non-PoE switch. Inserts into the backup power supply bay at the rear of the chassis.

OS6450-BP-PH (PS-550W-AC-P)
550W external AC backup power supply. Provides backup PoE power (390W) to an OS6450-P24 PoE switch. Ships with remote power connection cable, a United States power cord, power shelf and rack mounts for a 2 RU configuration.

OS6450-BP-PX (PS-900AC-P)
900W external AC backup power supply. Provides backup PoE power (780W) to an OS6450-P48 PoE switch. Ships with remote power connection cable, a United States power cord, power shelf and rack mounts for a 2 RU configuration.

Supported on OmniSwitch 6450 models only.

SFP-10G-SR
10-Gigabit optical transceiver (SFP+). Supports multi-mode fiber over 850nm wavelength with an LC connector. Typical reach of 300 m.

SFP-10G-LR
10-Gigabit optical transceiver (SFP+). Supports single mode fiber over 1310nm wavelength with an LC connector. Typical reach of 10 km.

SFP-10G-ER
10-Gigabit optical transceiver (SFP+). Supports single mode fiber over 1550nm wavelength with an LC connector. Typical reach of 40 km.

SFP-10G-LRM
10-Gigabit optical transceiver (SFP+). Supports multi mode fiber over 1310nm wavelength with an LC connector. Typical reach of 220 m.

SFP-10G-C1M/3M/7M
10-Gigabit direct attached copper transceiver (SFP+) available in 1m, 3m, 7m lengths.

Note: The 1m length is used for stacking and the 3m/7m lengths are used for uplinks.

OS6450S-CBL-60
10-Gigabit direct attached copper transceiver (SFP+) stacking cable available in 60cm.

Supported on OmniSwitch 6250/6450 models.

SFP-GIG-SX
1000Base-SX Gigabit Ethernet optical transceiver (SFP MSA). Supports multimode fiber over 850nm wavelength with an LC connector. Typical reach up to 300 m on 62.5/125 µm or 550m 50/125 µm MMF.

SFP-GIG-LX
1000Base-LX Gigabit Ethernet optical transceiver (SFP MSA). Supports single-mode fiber over 1310nm wavelength with an LC connector. Typical reach up to 10 Km on 9/125 µm SMF.

SFP-GIG-LH40
1000Base-LH Gigabit Ethernet optical transceiver (SFP MSA). Supports single-mode fiber over 1310nm wavelength with an LC connector. Typical reach up to 40 Km on 9/125 µm SMF.

SFP-GIG-LH70
1000Base-LH Gigabit Ethernet optical transceiver (SFP MSA). Supports single-mode fiber over 1310nm wavelength with an LC connector. Typical reach up to 70 Km on 9/125 µm SMF.

SFP-GIG-T
10/100/1000Base-T Gigabit Ethernet transceiver (SFP MSA). Supports category 5, 5E, and 6 copper cabling up to 100m.

SFP-GIG-EXTND
1000Base-SX Gigabit Ethernet optical transceiver (SFP MSA). Supports multimode fiber over 850nm wavelength with an LC connector. Typical reach up to 2 Km on 62.5/125 µm MMF and 50/125 µm MMF. Note: Not supported on OS6450.

SFP-GIG-CWD60
A group of 8 CWDM Gigabit Ethernet optical transceivers (SFP MSA). Supports single-mode fiber from 1470nm to 1610nm wavelength (based on transceiver) with an LC connector. Typical reach of 62 Km on 9/125 µm SMF.

Note: Not supported on OS6250.

SFP-GIG-BX-D
1000Base-BX SFP transceiver with an LC type connector. This bi-directional transceiver is designed for use over single-mode fiber on a single strand link up to 10 km. Transmits at 1490nm and receives at 1310nm optical signal. Designed for use with SFP-GIG-BX-U.

SFP-GIG-BX-U
1000Base-BX SFP transceiver with an LC type connector. This bi-directional transceiver is designed for use over single-mode fiber on a single strand link up to 10 km. Transmits at 1310 nm and receives at 1490nm optical signal. Designed for use with SFP-GIG-BX-D.

Supported on OmniSwitch all 6250/6450 models.

SFP-100-BX20LT
100Base-BX SFP transceiver with an SC type interface. This bi-directional transceiver is designed for use over single-mode fiber optic on a single strand link up to 20KM point-to-point. Transmits at 1550nm and receives at 1310nm optical signal.

SFP-100-BX20NU
100Base-BX SFP transceiver with an SC type interface. This bi-directional transceiver is designed for use over single-mode fiber optic on a single strand link up to 20KM point-to-point. Transmits at 1310nm and receives at 1550nm optical signal.

SFP-100-BXLC-D
100Base-BX SFP transceiver with an LC type interface. This bi-directional transceiver is designed for use over single-mode fiber optic on a single strand link up to 20KM point-to-point. Transmits at 1550nm and receives at 1310nm optical signal.

SFP-100-BXLC-U
100Base-BX SFP transceiver with an LC type interface. This bi-directional transceiver is designed for use over single-mode fiber optic on a single strand link up to 20KM point-to-point. Transmits at 1310nm and receives at 1550nm optical signal.

SFP-100-LC-MM
100Base-FX SFP transceiver with an LC type interface. This transceiver is designed for use over multimode fiber optic cable.

SFP-100-LC-SM15
100Base-FX SFP transceiver with an LC type interface. This transceiver is designed for use over single-mode fiber optic cable up to 15KM.

SFP-100-LC-SM40
100Base-FX SFP transceiver with an LC type interface. This transceiver is designed for use over single-mode fiber optic cable up to 40KM.

Supported on OmniSwitch 6450 models.

SFP-DUAL-BX-D
1000Base-BX10-D SFP transceiver with an LC type interface. This dual-speed, bi-directional transceiver is designed for use over single-mode fiber optic on a single strand link up to 10KM point-to-point. It can operate at 100/1000Mbit speed, transmits at 1550nm and receives at 1310nm optical signal.

Note: Not supported on OS6250.

SFP-DUAL-BX-U
1000Base-BX10-U SFP transceiver with an LC type interface. This dual-speed, bi-directional transceiver is designed for use over single-mode fiber optic on a single strand link up to 10KM point-to-point. It can operate at 100/1000Mbit speed, transmits at 1310nm and receives at 1550nm optical signal.

Note: Not supported on OS6250.

6.6.3 Software Feature Summary

Feature	Platform	License
Hardware		
- IEEE 802.3ah Dying Gasp	OS6250/6450	Metro
- Power Over Ethernet – Automatic Class Detection	OS6250/6450	
Access Guardian		
- MAC Accounting for Non-supplicants	OS6250/6450	
- User Network Profiles (UNP)	OS6250/6450	
- Host Integrity Check (HIC)	OS6250/6450	
- Captive Portal Enhancements	OS6250/6450	
- Control Over Access Guardian	OS6250/6450	
DHCP		
- DHCP Option 82 ASCII Support	OS6250/6450	
- DHCP Traffic Marking and Prioritization	OS6250/6450	
- DHCP Broadcast over VLAN 127	OS6250/6450	
- DHCP Option 2	OS6250/6450	
- DHCP Option 12	OS6250/6450	
- TFTP option (66/67)	OS6250/6450	
IP Enhancements		
- Selectable IP Interface for Management Services	OS6250/6450	
- IP Interface name up to 32 characters	OS6250/6450	
Link Aggregation		
- Auto Linkagg Detection	OS6250/6450	
- Dual-Home Link (DHL) – Active-Active	OS6250/6450	
LLDP Network Policies		
- Voice Vlan Support	OS6250/6450	
- Voice Application Support	OS6250/6450	
Metro		
- CPE Testhead (8 streams)	OS6250/6450	Metro
- MAC Forced Forwarding	OS6250/6450	Metro
- Virtual UP MEP	OS6250/6450	Metro
- LAG AutoNegotiation	OS6250/6450	Metro
Ethernet Services		
- Custom-L2-protocol	OS6250/6450	Metro
- Built-in UNI Profile	OS6250/6450	Metro
- UNI TPID	OS6250/6450	Metro
- Transparent Bridging	OS6250/6450	Metro

Feature	Platform	License
Service Assurance Agent (SAA)		
- SAA Interval	OS6250/6450	Metro
PPPoE-IA	OS6250/6450	Metro
Multicast		
- L2 MC VLAN Replication (MVR)	OS6250/6450	
Management VLAN 127	OS6250/6450	
License Management		
Zero Touch License Upgrade	OS6250/6450	
License Upgrade to Metro, Gig and 10G		
- Metro Package	OS6250/6450	
- Gig Package	OS6450	
- 10G Package	OS6450	
Link Monitoring/Diagnostics/Recovery		
- Interface Violation Recovery	OS6250/6450	
LLDP		
- Rogue Detection	OS6250/6450	
Quality of Service (QoS)		
- CIR 0	OS6250/6450	Metro
- Equal Scheduling of Yellow Traffic	OS6250/6450	
- Inner VLAN/Inner 802.1p in Policy Condition	OS6250/6450	
Security		
802.1x Radius down policies	OS6250/6450	
Learned Port Security Enhancements	OS6250/6450	
Radius Calling-Station-ID	OS6250/6450	
Radius Test Tool	OS6250/6450	
AAA/802.1x		
- 802.1x passthrough	OS6250/6450	
- Enhanced 802.1x show command	OS6250/6450	
- Client IP in Accounting Message	OS6250/6450	
- Service Type in Access Request	OS6250/6450	
Ethernet OAM		
- ETHOAM Syslog	OS6250/6450	
- Hashing Control	OS6250/6450	
- CCM Interval 100ms	OS6250/6450	
System		

Feature	Platform	License
- Configurable Port on Telnet	OS6250/6450	
- Hostname 19 Characters	OS6250/6450	
- Default User Profile	OS6250/6450	
- Configurable SYSLOG Facility ID	OS6250/6450	
- Hostname Automatically in Prompt	OS6250/6450	
- USB Support	OS6250/6450	
- OpenSSL/SSH	OS6250/6450	
Out of the Box Auto Configuration	OS6250/6450	
VRRP Support	OS6250/6450	

6.6.3 Software Features and Enhancements Descriptions

Hardware

IEEE 802.3ah Dying Gasp
This feature is designed to send a message on power loss. There are three types of messages sent:

1. SNMP Trap
As soon as the power failure is detected, a SNMP trap message is sent to the first three configured SNMP stations. The trap includes the following information:

- Slot number
- Power supply type (primary/backup)
- Time of the failure

2. Syslog Message
As soon as the power failure is detected a syslog message is sent to the first four syslog servers configured.

3. Link OAM PDU
As soon as the power failure is detected, an 802.3ah OAM Information PDU is sent to all ports of the NI for which link OAM is enabled. The PDU will have the Dying Gasp bit set.

The following table shows the 6.6.x release and model combinations required to support the Dying Gasp feature.

Dying Gasp Support Matrix

Model	Part Number	AOS Release	FPGA	Dying Gasp Support
Any	Any	6.6.1	10	Not Supported
Any	Any	6.6.2	10	Not Supported
6450	Any	6.6.3	Any	Supported
6250-Enterprise Models	Any	6.6.3	12	Supported
6250-8M	902735-90	6.6.3	12	Supported
6250-24M	902736-90 Rev E01 and below	6.6.3	12	Primary Power Supply Only
6250-24M	902736-90 Rev F and above	6.6.3	12	Primary and Backup Power Supplies
6250-24MD	902736-90 Rev E01 and below	6.6.3	12	Primary Power Supply Only
6250-24MD	902736-90	6.6.3	12	Primary and Backup

Model	Part Number	AOS Release	FPGA	Dying Gasp Support
	Rev F and above			Power Supplies

Note: Use the following command to determine the hardware revision of the OS650-24M/24MD.

```
-> show ni
        Module in slot 1
                Model Name:                 6250 24 PORT COPPER FE,
                Description:                6250 24 PORT COPPER FE,
                Part Number:                902736-90,
                Hardware Revision:          F,
                Serial Number:              K2182393,
                Manufacture Date:           JUN 27 2009,
                Firmware Version:           ,
                Admin Status:               POWER ON,
                Operational Status:         UP,
                Power Consumption:          43,
                Power Control Checksum:     0x6b36,
                CPU Model Type  :           ARM926 (Rev 1),
                MAC Address:                00:e0:b1:c2:ee:89,
                ASIC - Physical 1:          MV88F6281 Rev 2,
                FPGA - Physical 1:          0011/00,
                UBOOT Version:              n/a,
                UBOOT-miniboot Version:     6.6.1.602.R01,
                POE SW Version:             n/a
```

Power Over Ethernet – Automatic PoE Detection
This feature allows the OmniSwitch to automatically detect the Class (Class 0, Class1, Class2, Class3 or Class4) of the connected powered device. This allows the OmniSwitch to automatically adjust the maximum allowed power for a port preventing the OmniSwitch from delivering more power than the device requires.

Access Guardian

MAC Accounting for Non-supplicants
The option enables to create an accounting server entry for the non-supplicant mac-based authentication.

User Network Profiles (UNP)
Currently, users can only be classified in a UNP based on authentication result (802.1X, Captive Portal, or MAC auth) or based on classification rules (IP or MAC ranges). If no authentication mechanisms are configured, the switch has no way of assigning a user to a UNP.
This feature enhances the current protocol between the HIC server and the OmniSwitch by allowing the HIC server to return a UNP. A specific user (that is MAC address) would then be placed into this UNP based on the information sent. For example, users can be classified into UNPs based on Active Directory group memberships, machine specific parameters, and so on.

Host Integrity Check (HIC)
This feature allows the configuration of a primary and backup HIC server (Cyber Gate Keeper) to provide HIC server redundancy. The mode can be configured to determine what happens to users currently in the HIC authentication process when neither of the HIC servers is reachable:

- **Hold** - Hosts stay in their UNP and in a HIC in progress state and do not have network access.
- **Pass-through** - Hosts stay in their UNP but are removed from the HIC in progress state. Hosts have network access according the policy list set for their UNP.

Captive Portal Enhancements
The following Captive Portal Enhancements have been added:

- **Custom Proxy Port** – Allows an administrator to define a custom proxy port for users being authenticated through Captive Portal.
- **Inactivity Logout Timer** –. When enabled, this feature will flush a user from the Captive Portal user table if there is no activity for a set amount of time. The inactivity timer is equal to the MAC aging timer.
- **Public Certificate Support** – This feature allows the administrator to change the name of the Captive Portal URL to match that of a public certificate on the switch. This allows PKA authentication when using Captive Portal.

Control Over Access Guardian
This feature provides flexibility at the port-level to determine which Access Guardian process is performed first on a device attempting to log on to the network through an 802.1x-enabled port. This flexibility allows the administrator to first apply MAC authentication to the device, even if the device uses 802.1x EAPOL frames for supplicant authentication. After MAC authentication is done, subsequent 802.1x authentication can be applied to the same device.
Applying MAC authentication first allows the system to check if the MAC address of the supplicant device is on a "black list" and should not be allowed to access the network. If the address checks out OK, the device can under go 802.1 x authentications or be classified as a non-supplicant.

DHCP

DHCP Option 82 ASCII Support
When the OmniSwitch is configured to stamp, DHCP option-82 can be configured to provide a flexible ASCII string for the Circuit-ID value.

DHCP Traffic Marking and Prioritization
The DHCP packets that are trapped to CPU when DHCP snooping is enabled are relayed and retransmitted by software with the proper priority assignments (802.1p marking, ToS/DSCP marking and internal priority) dictated by user configured policy rules that the DCHP packets would match.

The priority assignment is not only controlled by policy rules but can also be controlled by the ingress qos port settings (that is. trusted/untrusted, default classification, default 802.1p and default DSCP) or the ethernet-service sap profile (i.e. fixed priority, map inner 802.1p to outer 802.1p and map dscp to outer 802.1p).

DHCP Broadcast over VLAN 127
Currently, the automatic remote configuration feature only supports two DHCP methods to get the initial IP address. Some Metro networks historically use a fixed tagged VLAN 127 for initial IP assignment. To facilitate the install of an OmniSwitch in such networks, support for a third DHCP method has been introduced on this tagged VLAN 127. DHCP client timing out in few minutes causes operational concerns. Hence DHCP client operation has been modified to continuously try to obtain a DHCP lease using any of these three methods alternatively:

- Static DHCP client on untagged VLAN 1
- Dynamic DHCP client on tagged VLAN 127
- Dynamic DHCP client on LLDP tagged management VLAN

DHCP Option 2
The DHCP option 2 is used to specify the time zone. The DHCP option 2 automatically sets the time zone when the switch is in the DHCP mode.

DHCP Option 12
The DHCP option 12 is used to specify the host name. The DHCP option 12 automatically sets the host name when the switch is in the DHCP mode.

TFTP option (66/67)
There are two mechanisms for a DHCP server to indicate the TFTP information:

- From Option 66 and Option 67.
- From the header fields “Server Host Name” and “Boot file Name”.

IP Enhancements

Selectable IP Interface for Management Services
Provides ability to configure a permanent source IP interface to be used when sending packets. The source IP interface can be the Loopback0 address or an existing IP interface on the switch and can be defined for the following applications:

- DNS, FTP, LDAP-SERVER, NTP, RADIUS, SFLOW, SNMP, SSH, SYSLOG, TACACS, TELNET, TFTP

IP Interface name up to 32 characters
The IP interface name is enhanced to accept up to 32 characters.

Link Aggregation

Auto Linkagg Detection
DHCP Server Association and DHCP Client creation works on fixed ports. When an OmniSwitch is newly introduced to a network, an assigned peer network device detects this device as new. If the peer device has a link aggregate configuration on the detecting port, then it sends LACP PDU to the newly connected OmniSwitch. In such instances, LACP PDUs must be acknowledged by OmniSwitch. The Remote Configuration Manager on OmniSwitch detects any LACP PDUs on combo or uplink ports and configures a link aggregate automatically during Automatic Remote Configuration.

Dual-Home Link (DHL) – Active-Active
Dual-Home Link (DHL) Active-Active is a high availability feature that provides fast failover between core and edge switches without using Spanning Tree. To provide this functionality, DHL Active-Active splits a number of VLANs between two active links. The forwarding status of each VLAN is modified by DHL to prevent network loops and maintain connectivity to the core when one of the links fails.
This implementation of DHL Active-Active is provided in addition to the previously released LACP-based DHL Active-Standby solution. Both versions are supported. The DHL Active-Active feature, however, is configurable on regular switch ports and on logical link aggregate ports (linkagg ID) instead of just LACP aggregated ports. In addition, the two DHL links are both active, as opposed to the active and standby mode used with LACP.

LLDP Network Policies
LLDP Network policy allows the advertisement of VLAN id, 802.1p and DSCP for the following applications: Voice, Voice Signaling, Guest Voice, Guest Voice Signaling, Soft phone voice, Video Conferencing, Streaming voice and Video Signaling.
The OmniSwitch use LLDP-MED Network Policies to advertise the Voice VLAN to the connected IP Phones through explicit definition of LLDP-MED Network Policy that contains information about the VLAN-ID and the associated L2 and L3 priorities. The binding of the network policies can be done globally or on a per port basis. The VLAN must be created explicitly. When using authenticated or mobile VLANs it is recommended to use mobile-tag rules to dynamically associate the devices according to the incoming tagged traffic.

Metro

CPE Testhead (8 streams)
The OmniSwitch CPE Test group feature provides a remote test generator and analyzer capability for testing and validating the Multi-CoS customer Ethernet service domain from end-to-end. The feature supports up to eight concurrent test flows. The OmniSwitch CPE Test group feature allows the service provider to perform the following tasks without the need for an external test head device:

- Generate specific flow-based traffic across the customer’s Ethernet Virtual Circuit (EVC) to help identify flow-based issues.
- Identify the impact of QoS settings (SAP profile or QoS policies) on the overall traffic.
- Confirm throughput across the provider network.
- Debug flow-specific traffic forwarding across the provider network.

- Analyze the behavior of various user-defined traffic patterns across the provider network.
- Perform the handover testing after initial deployment.
- Perform on-demand testing and results monitoring using a central entity.

MAC Forced Forwarding (Dynamic Proxy ARP)
MAC-Forced Forwarding (Dynamic Proxy ARP) is a mechanism to ensure the L2 separation of stations in the same VLAN beyond the local switch. The current port mapping functionality is limited to isolate user ports in the same switch. With MAC-FF the capability is extended to shared topologies such as rings or daisy chains to prevent users from communicating directly and ensuring that all communication happens through their default gateway. To accomplish this, the OmniSwitch supports Dynamic Proxy ARP which combines the functionality of port mapping and DHCP-snooping to dynamically learn a router's addresses and act as a local ARP proxy for the VLAN's router. Dynamic Proxy ARP - MAC Forced Forwarding uses the following features:

- **Port Mapping** - Port Mapping forwards traffic from user-ports only to network-ports, preventing communication between L2 clients in the same VLAN in the same switch. This prevents direct communication between clients in the same VLAN forcing all traffic to be forwarded to the head end router.

- **Dynamic Proxy ARP** - All ARP requests received on port mapping user-ports are answered with the MAC address of the head end router. Dynamic Proxy ARP dynamically learns the IP and MAC address of a head end router and responds with the MAC address of the router instead of flooding the ARP request.

- **DHCP Snooping** - Snoops the DHCP packets between the server and clients. DHCP snooping is used to dynamically learn the IP address of the head end router.

Virtual UP MEP
The Virtual UP MEP allows the creation of a management domain that does not have physical MEPs.

LAG AutoNegotiation
Auto-negotiation is supported for UPLINK ports that function as both combo and stacking ports. Auto-negotiation must be enabled on ports on both sides of the network or it must be disabled on both the sides for link aggregate auto negotiation to function correctly.

Ethernet Services

Custom-L2-Protocol
Custom L2 protocol is configured globally. The configured custom L2 protocol name can be associated to a UNI profile for specific packet control (Tunnel, MAC-tunnel and Discard) for proprietary protocol with multicast MAC address.
The custom L2 protocol can be applied specific actions (tunnel, MAC-tunnel and discard). The following table describes the actions that can be associated:

Action	Description
Tunnel	Tunnels the specified PDU across the provider network without modifying the MAC address.
MAC-tunnel	Changes the destination MAC address to the configured tunnel MAC address of the UNI profile before forwarding.
Discard	Discards the specified PDU.

Based on the configuration, the custom L2 protocols are classified as qualified L2 protocols and unqualified L2 protocols.
The qualified L2 protocols are the custom L2 protocols that are fully defined with an Ether-Type and optionally a Sub-Type or SSAP/DSAP. The action can be set to "Tunnel", "Discard" or "Mac-Tunnel".

The unqualified L2 protocols are the custom L2 protocols that are only defined with a MAC-address or MAC-address with mask. The action can be set to "Tunnel" or "Discard".

Built-in UNI Profile
Two built-in UNI profiles IEEE-FWD-ALL and IEEE-DROP-ALL are created to forward and drop the L2 protocol control frames having a destination mac-address of 01-80-C2-00-00-XX.

IEEE-FWD-ALL
When a UNI port is attached to this profile, all L2 protocol control frames having a destination MAC-address of 01-80-C2-00-00-XX are forwarded as normal data in hardware. The frames are forwarded without modification (i.e. no mac tunnel) .Exceptions is 01-80-C2-00-00-01 and 01-80-C2-00-00-04 (always discarded). When a tunneled L2 protocol control frames (i.e. tagged frame with SVLAN-ID) is received on NNI ports, the L2 protocol control frames is forwarded in hardware as normal data.

IEEE-DROP-ALL
When a UNI port is attached to this profile, all L2 protocol control frames having a destination MAC-address of 01-80-C2-00-00-XX are discarded in hardware. When a tunneled L2 protocol control frames (i.e. tagged frame with SVLAN-ID) is received on NNI ports, the L2 protocol control frames is still forwarded in hardware as normal data.

Note: Exception is BPDU or GVRP control frames. When NNI port is enabled for STP or GVRP legacy-bpdu, this trapps any STP or GVRP frames to CPU.

UNI TPID
UNI port now accepts all data frames with TPIDs 0x8100, 0x88a8 and 0x9100. However, in Translation mode UNI port accepts only data frames with TPID 0x8100.
Frame received on UNI ports can have any TPID and will be forwarded to the NNI ports with the appropriate cvlan-svlan translation. However, frame received on NNI port will always be forwarded to the UNI port with the translated cvlan and ether type 0x8100.

Transparent Bridging
The feature is supported on NNI ports.

Service Assurance Agent

SAA Interval
The minimum SAA interval is enhanced to one minute. The configuration of SAA interval below 10 minutes only allows the value 1, 2 or 5 minutes.

PPPoE-IA
PPPoE-IA is a means by which the discovery packets of PPPoE are tagged at the access switch of the service provider using Vendor Specific Attributes (VSA) to add the line-specific information at the switch.
The purpose of an IA is to help service provider and the Broadband Network Gateway to distinguish between different end hosts connected over Ethernet to the access switch. The Ethernet frames from different users are appropriately tagged by the IA to provide this distinction. The AOS implementation of PPPoE-IA enables the rate limiting and insertion of VSA tags into the PPPoE Active Discovery (PAD) messages. The tag is allowed to contain information such as the base MAC address of the switch, interface, customer VLAN, system name, and a user-defined string depending on the configuration.

Multicast

L2 MC VLAN Replication (MVR)

IP Multicast VLAN involves the creation of separate, dedicated VLANs constructed specifically for multicast traffic distribution. These distribution VLANs connect to the nearest multicast router and support multicast traffic only. The IP Multicast feature works in both the enterprise environment and the VLAN Stacking environment. The ports are separately classified as VLAN stacking ports or as legacy ports (Fixed ports/Tagged Ports). To ascertain that data flow is limited to either the VLAN Stacking domain or the enterprise domain, VLAN Stacking ports must be members of only the VLAN Stacking VLANs, while the normal legacy ports must be members of only enterprise mode VLANs.

Users have an option to configure "Receiver VLANs" (RVLANs) on the receiver ports. By configuring the receiver VLAN, the traffic from sender port is routed to different "Receiver VLANs" configured by the user. IGMP snooping is aware of the RVLANs so that the reports on those VLANs are handled appropriately.

Management VLAN 127
A management svlan should be created for management connectivity to the switch from the NNI port. The management vlan 127 is only for initial boot-up without a configuration file.

License Management

Zero Touch License Upgrade
The Automatic Remote Configuration Download feature supports automatic license upgrade process for remote devices. This allows the metro features on all its switches to have each switch in a network automatically upgraded with the set license, once they are installed in the network, by running a script file.

This allows the switch to activate the metro features for 15 days, giving time to the customer to identify the MAC-address/serial number of the newly installed switches and obtain the license file from the Alcatel-Lucent portal.

License Upgrade to Metro, Gig and10G
Upon purchasing of a license, the customer gets a Card ID. With this Card ID, the customer can request a license file from the ALU Web Portal.
The license key is a 40 byte encrypted string containing:

- The license ID: the time of the generation of the license
- MAC address
- Serial Number
- License type (permanent / demo)
- A license key can only accommodate one feature.

The demo duration is not part of the key and the duration is fixed at 60 days.

After the license key is validated, the license information is written in the chassis EEPROM.

- License ID – 4 bytes
- License Type – 2 bits
- Feature – 6 bits
- Time remaining (days) in case of demo license – 8 bits

Following are the three license package available:

- **Metro package** - This allows the metro features to be activated on 6250-24, 6250-P24 and 6450.
- **Gig package** - This allows the 6450-10L and 6450-P10L ports to run at 10/100/1000.
- **10G package** - This allows the fixed SFP/SFP+ interfaces on 6450-24, 6450-P24, 6450-48, 6450-P48 and 6450-U24 to run at 10Gbps.

Link Monitoring/Diagnostics/Recovery

Interface Violation Recovery
The OmniSwitch allows features to shutdown an interface when a violation occurs on that interface. To support this functionality, the following interfaces violation recovery mechanisms are provided:

- Manual recovery of a downed interface using a CLI command.

- An automatic recovery timer that indicates how much time a port remains shut down before the switch automatically brings the port back up
- A maximum number of recovery attempts setting that specifies how many recoveries can occur before a port is permanently shutdown
- A wait-to-restore timer that indicates the amount of time the switch waits to notify features that the port is back up
- An SNMP trap that is generated each time an interface is shutdown by a feature. This can occur even when the interface is already shutdown by another feature. The trap also indicates the reason for the violation.
- An SNMP trap that is generated when a port is recovered. The trap also includes information about how the port was recovered.
- The auto recovery timer is not specific to UDLD.

LLDP

Rogue Detection
LLDP rogue detection provides secure access to the network by detecting rogue devices and preventing such devices from connecting through any OmniSwitch port. A trusted LLDP agent can be assigned to individual ports, slots or the whole chassis. A trusted agent can be assigned by configuring the chassis ID sub type that will be used to validate the chassis ID type of the incoming LLDPDU.
The port can be moved to a violation state and a trap and/or port shutdown can be configured when the following instances occur:

- If more than one LLDP remote agent is learned on a port
- If no LLDPDU is received within three times the LLDP transmit interval (30 seconds) after link activation on a port that has no trusted remote agent configured
- If the same chassis ID and port ID of the remote agent exists in the trusted remote agent database but on a different port.

Quality of Service (QoS)

CIR 0
To provision a best effort service that has all the service frames as yellow, the ingress bandwidth profile associated to this service must have a CIR/CBS of 0 and a given PIR/PBS.

CIR/CBS can now be set to 0 in a sap-profile ingress bandwidth and saved in the running configuration.

- If only CIR 0 is entered, then the configuration is removed.
- If CIR=0 is entered with any other information (CBS, PIR, PBS), the configuration is saved in the running configuration and the policer is set according to the entered parameters. The CBS, PIR, PBS can be set to 0.
- Ideally if CIR=0 is entered, the CBS must be null as well.

Equal Scheduling of Yellow Traffic
This functionality enables equal scheduling of yellow traffic by configuring priority value for yellow traffic globally on the Omniswitch. This configuration is global and ensures fair sharing of yellow traffic. When the egress link is congested, the incoming yellow traffic on the link on all egress queues is fairly distributed equally shared based on the ingress traffic.

Inner VLAN/Inner 802.1p in Policy Condition
To provide customized inner or outer priority mapping, inner VLAN and inner 802.1p conditions are supported. The typical configuration is:

Inner 802.1p	Outer 802.1p / Priority
0	0
1	0
2	1

3	2
4	3
5	3
6	3
7	0

When inner vlan/802.1p is specified, the ingress filtering entry should be set with the following fields
IsTag = 1

- This indicates that the native packet is tagged. Since the inner vlan/802.1p condition is only supported on UNI port, this indicates the packet is cvlan tagged (i.e. outer tag is the inner tag).
- Two UDB fields represent the inner vlan and inner 802.1p value.

Security

802.1x Radius down policies
Allows users to be moved to a specified profile when the RADIUS server is not available. This feature is supported for 802.1x and MAC-based authentication, but not for users being authenticated by captive-portal. Users classified through the auth-server-down policy are flagged for re-authentication when the authentication server becomes reachable. Users can configure the re-authentication period put in the UNP (or being blocked) when RADIUS server is not available at the time of authentication.

Learned Port Security Enhancements
The following Learned Port Security (LPS) enhancements have been added:

- LPS now continues to learn filtering MAC addresses after the learning window has expired, but only up to the configured filtering MAC address limit.
- A new type of static MAC address (pseudo-static) is maintained. A pseudo-static MAC address is not user-configured; it is a dynamically learned MAC address that is treated the same as a regular static address (will not age out or be flushed during the learning window time period). However, the pseudo-static MAC is not saved in the running configuration.
- New parameter options for the LPS **port-security shutdown** CLI command:
  - **No Aging of Learned MAC Addresses**. A new **no-aging** parameter specifies whether or not LPS will learn MAC addresses as "pseudo-static" addresses.
  - **Convert MAC Addresses to Static MACs**. A new **convert-to-static** parameter specifies whether or not pseudo-static and dynamically learned MAC addresses are converted to static MAC addresses when the learning window time expires.
  - **Learning Window Start at Boot-up**. A new **boot-up** parameter specifies whether or not LPS will start the learning window time when the switch boots up.
- New **admin-state** parameter for the **port-security** CLI command. This parameter is used to enable, disable, or lock an LPS port. In addition, the **port-security** command will now accept a range of ports.
- Creating a static MAC address on a port now automatically enables LPS on that port.
- New **brief** parameter for the **show port-security** CLI command. This parameter is used to provide a summary of the LPS status, configuration, and MACs learned on all the LPS ports.
- The VLAN ID bound to an LPS static MAC address is automatically updated when the default VLAN for the LPS port is changed.
- Duplicate LPS static MAC addresses are now allowed on different ports within the same VLAN. However, dynamic MAC addresses that match a configured static MAC address within the same VLAN are not learned.
- The "Bridge MAC Learned" and "LPS Violation" SNMP traps now have three fields of information: port number, VLAN ID, and MAC address.
- A new LPS shutdown violation mode, "discard", is now supported. This mode administratively disables the port, but the port remains physically up. The "shutdown" and "restricted" modes are still supported.

Radius Calling-Station-ID

When a user logs in to the switch, the event is logged using the RADIUS accounting server. This is now enhanced to capture the Calling Station-ID details. The radius accounting messages sent from the switch to the RADIUS server is added with an attribute radius Calling Station-ID. The IP address of the host trying to login to the switch is the value for that attribute.

Radius Test Tool
Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users to connect and use a network service.
The RADIUS test tool provides the administrator with the utility to test the reach ability of RADIUS server from the Network Access Server (AOS Switch). This test tool is useful in validating the RADIUS server configuration such as server-name, IP address, UDP authentication-port/accounting-port, and secret key.
The RADIUS test tool allows the administrator to validate authentication of the given username and password. This tool helps in simulating the RADIUS client on the AOS Switch, providing the network administrator with a utility to verify the authentication/accounting of a client with a RADIUS server.

AAA/802.1x

802.1x passthrough
The feature globally sets the switch to transparently forward the 802.1x EAP frames. Pass through mode must be enabled on the Layer2 switch to allow EAP packets to be trapped on the Layer3 switch for authentication.
Enhanced 802.1 show command
The following fields are added in the “show 802.1x user” output:

- Auth Failure Reason: Reason for authentication failure as “SERVER UNREACHABLE” or “AUTHENTICATION FAILURE”. In the case of successful authentication “- “ is returned
- Auth Retry Count: Number of times the switch re-transmits a request for authentication information to the 802.1x user
- Last Successful Auth Time: Latest successful authentication time. If port was not authenticated before then “-“is returned.

Client IP in Accounting Message
The feature depends on DHCP snooping being enabled and DHCP being used by the 802.1x supplicant to obtain an IP address. Upon successful 802.1x authentication, the IP address of the user is sent to the accounting server.

Service Type in Access Request
The OmniSwitch will add the Service Type attribute in the Access Request to be used by the RADIUS server to distinguish between different request types.
The Service Type attribute in the Access Request Message is used by the RADUIS server to distinguish between different request types. This will allow the server to forward the request to other servers.

Ethernet OAM

ETHOAM Syslog
During every FNG state machine change a swlog event is generated. The swlog event is then forwarded to the syslog server as per the swlog output configuration. The swlog output can be configured to console, flash, and syslog servers.

Hashing Control
Currently, the Layer-2 table lookup is based on an XOR hash.
The hash-control mode fdb command can be used to configure or change the hash mode of the Layer 2 table. The options available are XOR or CRC mode.

The default value set is XOR. If hash-control mode is required to work on a stack, it must be configured individually on all units of a stack.
Changing the hash-control mode requires a switch or stack reboot.

CCM Interval 100ms
The CCM interval of 100ms is introduced to speed up the ERP CCM interval in fractions of 100ms.

Systems

Configurable Port on Telnet
While establishing a telnet session to a device from AOS, the destination TCP port for the telnet port (between 1024 and 65535) can be specified.

Hostname 19 Characters
The system name command is enhanced to accept up to 255 characters.

Default User Profile
Currently, a user can configure its personal settings comprising the prompt, the more settings and the aliases. The settings are only valid during the life of the session and are lost once the user logs out. To save the personal settings, the "user profile save" command is used. The command is enhanced to add a default profile for ALL users connecting to the switch.

The "user profile save" command has been modified to specify that the current settings must be in a global profile file or in the user specific profile file -> user profile save [global-profile]

The settings are then saved in a text file (/flash/switch/xxxx.txt) and there is one file per user. When a user logs in, its personal settings from the profile file are loaded. During the session, the user can remove the personal settings with the "user profile reset" command and go back to the factory default settings (no prompt (i.e. "prompt" command), no more, no alias). This does not delete the user profile file.

The personal settings are configurable and can be saved by any users, regardless of their privileges. For instance, a read only user can configure the prompt, more and aliases and can save the settings in the file.

Configurable SYSLOG Facility ID
User can configure the SYSLOG facility ID.

Hostname Automatically in Prompt
Hostname sets the prompt to the current system of the switch. By default, the system name is set to 'Vx Target'. Every time the host name is modified, the prompt is also modified.

USB Support
The USB port can be used with an Alcatel-Lucent certified USB Flash drive to provide the following functions:

- Disaster Recovery – The switch can boot from the USB drive if it is unable to load AOS from flash.
- Upload / Download Image and Configuration Files - To create or restore backup files.
- Upgrade Code - Upgrade code with the image files stored on the USB drive.

OpenSSL/SSH
OpenSSL 0.9.8.o and OpenSSH 5.0 are supported.

VRRP Support
The Virtual Router Redundancy Protocol version 3 (VRRPv3) implementation is based on the latest Internet-Draft for VRRP for IPv6. VRRP version 2 (VRRPv2) is based on RFC 2338.
Similar to VRRPv2, VRRPv3 is a standard router redundancy protocol that provides redundancy by eliminating the single point of failure inherent in a default route environment. The VRRPv3 router, which controls the IPv6 address associated with a virtual router is called the master router, and is responsible for forwarding virtual router advertisements. If the master router becomes unavailable, the highest priority backup router will transition to the master state.

Both versions of VRRP allow routers on a LAN to back up a static default route with a virtual router. VRRP dynamically assigns responsibility for a virtual router to a physical router (VRRP router) on the LAN. The virtual router is associated with an IP address (or set of IP addresses) on the LAN. A virtual router master is elected to forward packets for the virtual router's IP address. If the master router becomes unavailable, the highest priority backup router will transition to the master state.
Authentication is not supported.
In addition, both versions support VRRP Tracking. A virtual router's priority may be conditionally modified to prevent another router from taking over as master. Tracking policies are used to conditionally modify the priority setting whenever an ip interface, slot/port, and/or IP address associated with a virtual router goes down.
VRRPv2 is available on all supported OmniSwitch platforms in this release.

Out of the Box Auto-Configuration (Zero-Touch Configuration)
The Out-of-the-Box Auto-Configuration capability automates and simplifies the deployment of large network installations eliminating the need for manual configuration of each device. It also ensures that each device is compliant with the centrally controlled device configuration policies and firmware revisions.
This feature allows a newly deployed OmniSwitch to automate the process through an instruction file that provides the necessary actions to download its configuration or any necessary firmware upgrades with no user intervention by doing the following:

1. Lease an IP address, mask, default gateway, and system name from a reachable DHCP server.
2. Download an instruction file with information to obtain the configuration file, image files and/or script files from given TFTP, FTP, or SCP servers.
3. Download and apply the image and configuration file.
4. Automatically reboot with the upgraded image files and switch configuration file or if no images or boot configuration is downloaded scripted instructions are executed on the fly and the switch is made available remotely.

Learned Management VLAN using Nearest-Edge Mode
An OmniSwitch running the Auto-Configuration feature is automatically enabled to process LLDP PDUs with the unique Nearest-Edge destination MAC address. In Nearest-Edge mode the Management OmniSwitch will use a unique MAC address when sending LLDP PDUs. The Automatic Remote Configuration feature will look for these unique packets to determine a Management VLAN. It will then create a DHCP client interface on that tagged VLAN. The Nearest-Edge mode is useful when a DHCP client interface needs to be configured on a VLAN other than the default VLAN.

Newly deployed or upgraded switches with no **boot.cfg** file running AOS 6.6.3 will automatically run the Auto-Configuration process. This causes the OK LED to blink green while the process is running. If the Auto-Configuration process is not successful, the OK LED will eventually turn solid green indicating the switch has booted and is ready to be configured.

6.6.3.439. R01 Software Features and Enhancements

Control Frame Tunnel Statistics
This feature Enhancement provides the facility to view the statistics of the processing of Layer 2 control frames received per port per protocol on UNI and NNI ports as set according to the UNI-Profile.

Platforms Supported:
OmniSwitch 6450, 6250M

Commands usage

-> show ethernet-service uni [[linkagg<num>] / <port>]] l2pt-statistics
This command displays per UNI port statistics of all protocols. When no port(s) specified, statistics of all UNI ports are displayed.

Syntax Definitions:
Num Linkagg whose statistics are requested.
Port Port whose statistics are requested.

Usage Guidelines:
The port should be an UNI port.

Output Example:

```
PS1: 172.25.50.70-> show ethernet-service uni l2pt-statistics
Rx,Tunnel and Drop are counted only in software

                              MAC          Source
 Port            L2 Protocol                  Rx          Tunnel        Drop
   Peer       MAC Tunnel    De-tunnel         MAC
------+--------------------------------+------------+------------+------------+-
----------+------------+------------+----------------
 0/1      802.3ad                                    0             0             0
          0              0             0         -
 0/1      LACPMARKER                                 0             0             0
          0              0             0         -
 0/1      OAM                                        0             0             0
          0              0             0         -
 0/1      802.1x                                     0             0             0
          0              0             0         -
 0/1      802.1ab                                    0             0             0
          0              0             0         -
 0/1      AMAP                                       0             0             0
          0              0             0         -
 0/1      PAGP                                       0             0             0
```

-> show ethernet-service nni [[linkagg<num>] / <port>]] l2pt-statistics
This command displays per NNI port statistics of all protocols. When no port(s) specified, statistics of all NNI ports are displayed.

Syntax Definitions:
Num Linkagg whose statistics are requested.
Port Port whose statistics are requested.

Usage Guidelines:

The port should be an NNI port

Output Example:

```
PS2: 172.25.50.73-> show ethernet-service nni l2pt-statistics

  Port    Rx Mac-Tunnel    Mac-tunnel discard
-------+---------------+--------------------
  1/3              169                  0

PS2: 172.25.50.73->
```

-> show ethernet-service uni-profile [<profile_name>] l2pt-statistics
This command displays per uni-profile statistics of all protocols. When no profile specified, statistics of all UNI profiles are displayed.

Syntax Definitions:
Uni profile name Name of the uni-profile whose statistics to be displayed.

Usage Guidelines:
When the name is given, the uni-profile entry should be already configured.

Output Example:

```
->
->
-> show ethernet-service uni-profile u4 l2pt-statistics
UNI Profile: u4
        Total RX:                                                    97,
        L2 Protocol:
                802.3ad, OAM, LACPMARKER
                        Rx:                                           0,
                        Hardware processing:                        CPU,
                802_1x
                        Rx:                                           0,
                        Hardware processing:                       DROP,
                802.1ab
                        Rx:                                           4,
                        Hardware processing:                       DROP,
                AMAP
                        Rx:                                           3,
                        Hardware processing:                       DROP,
                PAPG, UDLD, CDP, DTP, VTP, PVST, VLAN, UPLINK
                        Rx:                                           0,
                        Hardware processing:                        CPU,
                STP
                        Rx:                                          90,
                        Hardware processing:                        CPU,
                GVRP, MVRP
                        Rx:                                           0,
                        Hardware processing:                        FWD,
```

-> clear ethernet-service uni [[linkagg<num>] / <port>]] l2pt-statistics
This command clears UNI port statistics of all protocols.

Syntax Definitions:
Num Linkagg whose statistics to be cleared.
Port Port whose statistics to be cleared.

Usage Guidelines:
The port should be an UNI port.

-> clear ethernet-service nni [[linkagg<num>] / <port>]] l2pt-statistics
This command clears NNI port statistics of all protocols.

Syntax Definitions:
Num Linkagg whose statistics to be cleared.
Port Port whose statistics to be cleared.

Usage Guidelines:
The port should be an NNI port.

-> clear ethernet-service uni-profile [<uni profile_name>] l2pt-statistics
This command clears uni profile statistics of all protocols.

Syntax Definitions:
Uni profile name Name of the uni-profile whose statistics to be displayed.

Usage Guidelines:
When the name is given, the uni-profile should be already configured.

Limitations:
None

Acct-Input-Gigawords & Acct-Output-Gigawords
This enhancement feature provides the facility to identify how many times the Acct-Input-Octets(type-42), Acct-Output-Octets(Type-43) counter has wrapped around 2^32 it will calculate the value in multiples of 4GB and send using the attributes Acct-Input-Gigawords (type 52) & Acct-Output-Gigawords (type 53).Earlier, size of Acct-Input-Octets & Acct-Output-Octets with which we can only represent maximum 4GB(2^32) of Octets. In this enhancement Acct-Input-Gigawords, Acct-Output-Gigawords will be sent in Interim-Update, Periodic-Interim-Update & Stop Messages. Acct-Input-Gigawords, Acct-Output-Gigawords that are sent in accounting packets for both supplicant and non-supplicant users.

Platforms Supported:
Omni Switch 6250
Omni Switch 6450

Commands usage:
No New commands introduced

Limitations:
None

Case Sensitive Mac-Address Authentication
This enhancement feature enables the AOS switches to send MAC address of the non-supplicant client in lower case as username and password for authentication to the authentication server. During non-supplicant authentication the client MAC address is sent as username and password. Earlier, for non-supplicant authentication the client MAC address is sent as username and password .This MAC address is sent in Uppercase for username and password. This enhancement enables to the send the MAC address of client as username and password in lower case.

Platforms Supported:
Omni Switch 6250
Omni Switch 6450

Commands usage:
No New commands introduced

Limitations:
None

UNP Bandwidth Rate Limiting
This feature Enhancement provides the facility to apply ingress and egress bandwidth limitations on a port on basis of UNP classification locally or remotely through radius-server return attribute. A UNP profile will be associated with maximum ingress and egress bandwidth, whenever authenticates under UNP policy either through radius returned UNP attribute or through local policy, associated bandwidth limitations are applied on port. When Qos port with ingress or egress bandwidth specified will override bandwidth associated due to UNP. If ingress/egress bandwidth is set through qos port command then any change in qos port parameter will over ride bandwidth set due to UNP.

When multiple users authenticate under same port latest bandwidth limitation will overwrite the previous limitation existing on the port. Earlier there was no option to associate bandwidth parameters with UNP. Hence No bandwidth limitation can be applied to the port on basis of UNP classification.

Platforms Supported:
OmniSwitch 6450
OmniSwitch 6250/ OS6250M

Commands usage:

-> aaa user-network-profile name <profile-name> vlan <vlan> [maximum-ingress-bandwidth <num> maximum-egress-bandwidth <num> maximum-default-depth <num>]

Syntax Definitions:

Maximum-ingress-bandwidth	Ingress bandwidth to be applied on the port.
Maximum-egress-bandwidth	egress bandwidth to be applied on the port.
Maximum-default-depth	depth to be applied on the port.

Defaults:

Maximum-ingress-bandwidth	-1 (no rate-limit)
Maximum-egress-bandwidth	-1 (no rate-limit)
Maximum-default-depth	-1 (1 Mbps)

-> show 802.1X rate-limit

Output Example:

```
-> show 802.1x rate-limit

Slot  Max               Ingress BW                      Max               Egress BW
Port  Ingress-BW  Type  UNP-ProfileName                 Egress-BW   Type  UNP-ProfileName
-----+----------+------+-------------------------------+----------+------+-------------------------------
 3/7         64K    UNP                           geetha8        64K    UNP                           geetha8
```

Limitations:
None

DHCP SERVER
A DHCP server provides dynamic IP addresses on lease for client interfaces on a network. It manages a pool of IP addresses and information about client configuration parameters. The DHCP server obtains an IP address request from the client interfaces. After obtaining the requests, the DHCP server assigns an IP address, a lease period, and other IP configuration parameters, such as the subnet mask and the default gateway.

For enabling the DHCP-server in DUT we have to keep the below files in flash/switch directory and it is having the information about ip address details assigned to client when DHCP-client sends DHCP-request.
dhcpd.pcy
dhcpd.conf

Platforms Supported:
Omni Switch 6450

Commands usage:

dhcp-server {enable | disable | restart}
Enables, disables, or restarts the DHCP server operation.

Syntax Definitions:
Enable Enables operation status of the DHCP server.

Disable Disables operation status of the DHCP server.

Restart Restarts the DHCP Server.

-> clear dhcp-server statistics
Clears the packet counters of dhcp-server statistics.

-> show dhcp-server statistics [packets | hosts | subnets | all]
Displays the statistics of the DHCP server.

Syntax Definitions:
packets Displays general statistical information along with specific information

about data packets received, dropped and transmitted.

hosts — Displays general statistical information along with specific information about hosts related to all the subnets.

subnets — Displays general statistical information along with specific information about all the subnets.

all — Displays all statistical information related to the DHCP server.

-> show dhcp-server leases [ip_address | mac_address | count] [type {static | dynamic}]
Displays the leases offered by the DHCP server.

Syntax Definitions:
ip_address — Specifies IP address of the interface configured with DHCP server.

mac_address — Specifies MAC address of the interface configured with DHCP server.

static — Displays only static leases.

Dynamic — Displays only dynamic leases.

Limitations:
None

6.6.1/6.6.2 Feature Summary

The following software features were introduced in AOS Release 6.6.1 or 6.6.2 on the OmniSwitch 6250 Enterprise/Metro models and are now supported on the OmniSwitch 6450 models:

Feature	Platform	License
802.1ab	OS6250	
802.1Q	OS6250	
802.1x Multiple Client Support	OS6250	
802.1x Device Classification (Access Guardian)	OS6250	
Mac Authentication for 802.1x Supplicants	OS6250	
Access Guardian	OS6250	
Captive Portal	OS6250	
Captive Portal Web Pages	OS6250	
Access Control Lists (ACLs)	OS6250	
Access Control Lists (ACLs) for IPv6	OS6250	
L4 ACLs over IPv6	OS6250	
ACL & Layer 3 Security	OS6250	
ARP Defense Optimization	OS6250	
ARP Poisoning Detection	OS6250	
Authenticated Switch Access	OS6250	
Partitioned Switch Management	OS6250	
Account & Password Policies	OS6250	
Command Line Interface (CLI)	OS6250	
DHCP Relay **Per-VLAN DHCP Relay**	OS6250	
DHCP Option-82	OS6250	
DHCP Snooping	OS6250	
L2 DHCP Snooping	OS6250	
Option-82 Data Insertion Format	OS6250	
DNS Client	OS6250	
Dynamic VLAN Assignment (Mobility)	OS6250	
End User Partitioning	OS6250	
Ethernet Interfaces	OS6250	
Ethernet OAM	OS6250	
Ethernet Services (VLAN Stacking)	OS6250	
Ethernet OAM 802.3ah - EFM	OS6250	

Feature	Platform	License
Flood/Storm Control	OS6250	
Flow Control (802.3x)	OS6250	
GVRP	OS6250	
Health Statistics	OS6250	
HTTP/HTTPS Port Configuration	OS6250	
Interswitch Protocols (AMAP)	OS6250	
IPv4 Routing	OS6250	
31-bit Network Mask Support	OS6250	
IPv6 Routing	OS6250	
IPv6 Client and/or Server Support	OS6250	
IP DoS Filtering	OS6250	
IPv4 Multicast Switching (IPMS)	OS6250	
IPv6 Multicast Switching (MLD)	OS6250	
IPv4 Multicast Switching (Proxying)	OS6250	
IPv6 Multicast Switching (Proxying)	OS6250	
IP MC VLAN (Multiple Sender Ports)	OS6250	
IP Multinetting	OS6250	
IP Route Map Redistribution	OS6250	
Learned Port Security (LPS)	OS6250	
Learned MAC Address Notificaton	OS6250	
Link Aggregation (static & 802.3ad)	OS6250	
Loopback Detection (LBD)	OS6250-Metro	
Mac Retention	OS6250	
NTP Client	OS6250	
Policy Server Management	OS6250	
Policy Based Routing (Permanent Mode)	OS6250	
Port Mapping	OS6250	
Port Mirroring (24:1)	OS6250	
Port Monitoring	OS6250	
Power over Ethernet (PoE)	OS6250-Enterprise	
Quality of Service (QoS)	OS6250	
Auto-Qos Prioritization of IP Phone Traffic	OS6250	
Auto-Qos Prioritization of NMS Traffic	OS6250	
DSCP Range Condition	OS6250	
Policy Based Mirroring	OS6250	

Feature	Platform	License
Port-based Ingress Limiting	OS6250	
Redirection Policies (Port and Link Agg)	OS6250	
Tri-Color Marking	OS6250	
Remote Port Mirroring	OS6250	
RIPv1/RIPv2	OS6250	
ECMP RIP Support	OS6250	
RIPng	OS6250	
RMON	OS6250	
Router Discovery Protocol (RDP)	OS6250	
Routing Protocol Preference	OS6250	
Secure Copy (SCP)	OS6250	
Secure Shell (SSH)	OS6250	
SSH Public Key Authentication	OS6250	
sFlow	OS6250	
SNMP	OS6250	
Source Learning	OS6250	
- L2 Static Multicast Address	OS6250	
- Disable MAC learning per VLAN	OS6250-Metro	
- Disable MAC learning per port	OS6250-Metro	
Spanning Tree	OS6250	
802.1Q 2005 (MSTP)	OS6250	
Automatic VLAN Containment (AVC)	OS6250	
PVST+	OS6250	
RRSTP	OS6250	
Switch Logging	OS6250	
Syslog to Multiple Hosts	OS6250	
Trivial File Transfer Protocol (TFTP) Client	OS6250	
Text File Configuration	OS6250	
UDLD	OS6250-Metro	
User Definable Loopback Interface	OS6250	
User Network Profiles	OS6250	
VLANs	OS6250	
Web-Based Management (WebView)	OS6250	
Out of the Box Auto-Configuration with Dynamic Management VLAN	OS6250-Metro	

Feature	Platform	License
DHCP Client with configurable option 60	OS6250-Metro	
IEEE 802.3ah Dying Gasp	OS6250-Metro	
CPE Test Head capability	OS6250-Metro	
Ethernet OAM		
- IEEE 802.1ag Version 8.1	OS6250-Metro	
- ITU Y.1731	OS6250-Metro	
Ethernet Ring Protection (ERP) - G.8032	OS6250-Metro	
Ethernet Services		
- L2 Protocol MAC tunneling	OS6250-Metro	
- Advanced Ethernet Loopback	OS6250-Metro	
Quality of Service (QoS)		
- Egress Policy Rules	OS6250-Metro	
- IEEE 802.1q/ad CFI/DEI Bit Stamping	OS6250-Metro	
- Policy Condition Enhancements (VLAN group, 802.1p Range)	OS6250-Metro	
- Flexible Inner DSCP/ToS Mapping to Outer 802.1p	OS6250-Metro	
- QOS Statistics	OS6250-Metro	
Service Assurance Agent (SAA)		
- SAA - Ethernet OAM	OS6250-Metro	
- SAA - IP ping	OS6250-Metro	Base
- Generic L2 SAA	OS6250-Metro	Base

6.6.2 Feature Summary

The following software features were introduced with the 6.6.2.R01 release and were supported on the OmniSwitch 6250 Metro Models:

Feature	Platform	Software Package
Out of the Box Auto-Configuration with Dynamic Management VLAN	OS6250-Metro	Base
DHCP Client with configurable option 60	OS6250-Metro	Base
IEEE 802.3ah Dying Gasp	OS6250-Metro	Base
CPE Test Head capability	OS6250-Metro	Base
Ethernet OAM		
- IEEE 802.1ag Version 8.1	OS6250-Metro	Base
- ITU Y.1731	OS6250-Metro	Base
Ethernet Ring Protection (ERP) - G.8032	OS6250-Metro	Base
Ethernet Services		
- L2 Protocol MAC tunneling	OS6250-Metro	Base
- Advanced Ethernet Loopback	OS6250-Metro	Base
Quality of Service (QoS)		
- Egress Policy Rules	OS6250-Metro	Base
- IEEE 802.1q/ad CFI/DEI Bit Stamping	OS6250-Metro	Base
- Policy Condition Enhancements (VLAN group, 802.1p Range)	OS6250-Metro	Base
- Flexible Inner DSCP/ToS Mapping to Outer 802.1p	OS6250-Metro	Base
- QOS Statistics	OS6250-Metro	Base
Service Assurance Agent (SAA)		
- SAA - Ethernet OAM	OS6250-Metro	Base
- SAA - IP ping	OS6250-Metro	Base
- Generic L2 SAA	OS6250-Metro	Base

6.6.1 Feature Summary

The following software features were introduced with the 6.6.1.R01 release and were supported on both the OmniSwitch 6250 Enterprise and Metro models:

Feature	Platform	Software Package
802.1ab	OS6250	base
802.1Q	OS6250	base
802.1x Multiple Client Support	OS6250	base
802.1x Device Classification (Access Guardian)	OS6250	base
Mac Authentication for 802.1x Supplicants	OS6250	base
Access Guardian	OS6250	base
Captive Portal	OS6250	base
Captive Portal Web Pages	OS6250	base
Access Control Lists (ACLs)	OS6250	base
Access Control Lists (ACLs) for IPv6	OS6250	base
L4 ACLs over IPv6	OS6250	base
ACL & Layer 3 Security	OS6250	base
ARP Defense Optimization	OS6250	base
ARP Poisoning Detection	OS6250	base
Authenticated Switch Access	OS6250	base
Partitioned Switch Management	OS6250	base
Account & Password Policies	OS6250	base
Command Line Interface (CLI)	OS6250	base
DHCP Relay **Per-VLAN DHCP Relay**	OS6250	base
DHCP Option-82	OS6250	base
DHCP Snooping	OS6250	base
L2 DHCP Snooping	OS6250	base
Option-82 Data Insertion Format	OS6250	base
DNS Client	OS6250	base
Dynamic VLAN Assignment (Mobility)	OS6250	base
End User Partitioning	OS6250	base
Ethernet Interfaces	OS6250	base
Ethernet OAM	OS6250-Metro	base
Ethernet Services (VLAN Stacking)	OS6250-Metro	base
Ethernet OAM 802.3ah - EFM	OS6250-Metro	base

Feature	Platform	Software Package
Flood/Storm Control	OS6250	base
Flow Control (802.3x)	OS6250	base
GVRP	OS6250	base
Health Statistics	OS6250	base
HTTP/HTTPS Port Configuration	OS6250	base
Interswitch Protocols (AMAP)	OS6250	base
IPv4 Routing	OS6250	base
31-bit Network Mask Support	OS6250	base
IPv6 Routing	OS6250	base
IPv6 Client and/or Server Support	OS6250	base
IP DoS Filtering	OS6250	base
IPv4 Multicast Switching (IPMS)	OS6250	base
IPv6 Multicast Switching (MLD)	OS6250	base
IPv4 Multicast Switching (Proxying)	OS6250	base
IPv6 Multicast Switching (Proxying)	OS6250	base
IP MC VLAN (Multiple Sender Ports)	OS6250	base
IP Multinetting	OS6250	base
IP Route Map Redistribution	OS6250	base
Learned Port Security (LPS)	OS6250	base
Learned MAC Address Notificaton	OS6250	base
Link Aggregation (static & 802.3ad)	OS6250	base
Loopback Detection (LBD)	OS6250-Metro	base
Mac Retention	OS6250	base
NTP Client	OS6250	base
Policy Server Management	OS6250	base
Policy Based Routing (Permanent Mode)	OS6250	base
Port Mapping	OS6250	base
Port Mirroring (24:1)	OS6250	base
Port Monitoring	OS6250	base
Power over Ethernet (PoE)	OS6250-Enterprise	base
Quality of Service (QoS)	OS6250	base
Auto-Qos Prioritization of IP Phone Traffic	OS6250	base
Auto-Qos Prioritization of NMS Traffic	OS6250	base
DSCP Range Condition	OS6250	base
Policy Based Mirroring	OS6250	base

Feature	Platform	Software Package
Port-based Ingress Limiting	OS6250	base
Redirection Policies (Port and Link Agg)	OS6250	base
Tri-Color Marking	OS6250	base
Remote Port Mirroring	OS6250	base
RIPv1/RIPv2	OS6250	base
ECMP RIP Support	OS6250	base
RIPng	OS6250	base
RMON	OS6250	base
Router Discovery Protocol (RDP)	OS6250	base
Routing Protocol Preference	OS6250	base
Secure Copy (SCP)	OS6250	base
Secure Shell (SSH)	OS6250	base
SSH Public Key Authentication	OS6250	base
sFlow	OS6250	base
SNMP	OS6250	base
Source Learning	OS6250	base
- L2 Static Multicast Address	OS6250	base
- Disable MAC learning per VLAN	OS6250-Metro	base
- Disable MAC learning per port	OS6250-Metro	base
Spanning Tree	OS6250	base
802.1Q 2005 (MSTP)	OS6250	base
Automatic VLAN Containment (AVC)	OS6250	base
PVST+	OS6250	base
RRSTP	OS6250	base
Switch Logging	OS6250	base
Syslog to Multiple Hosts	OS6250	base
Trivial File Transfer Protocol (TFTP) Client	OS6250	base
Text File Configuration	OS6250	base
UDLD	OS6250-Metro	base
User Definable Loopback Interface	OS6250	base
User Network Profiles	OS6250	base
VLANs	OS6250	base
Web-Based Management (WebView)	OS6250	base

Existing Software Feature Descriptions

802.1AB with MED Extensions
IEEE 802.1AB (2005) is the latest version for the standards based connectivity discovery protocol. The purpose of the IEEE standard 802.1AB for Link Layer Discovery Protocol (LLDP) is to provide support for network management software, such as OmniVista, that deals with topology discovery. Switches that are compliant with 802.1AB use TLV (Time, Length, Value) frames to exchange information with neighboring devices and maintain a database of the information exchanged. The Link Layer Discovery Protocol-Media Endpoint Discover (LLDP-MED) is designed to extend IEEE 802.1AB functionality to exchange information such as VLANs and power capabilities.

802.1Q
802.1Q is an IEEE standard for sending frames through the network tagged with VLAN identification. 802.1Q tagging is the IEEE version of VLANs. It is a method of segregating areas of a network into distinct VLANs. By attaching a label, or tag, to a packet, it can be identified as being from a specific area or identified as being destined for a specific area.
When a port is enabled to accept tagged traffic, by default both 802.1Q tagged and untagged traffic is automatically accepted on the port. Configuring the port to accept only tagged traffic is also supported.
Access Guardian

802.1X Device Classification Policies
In addition to the authentication and VLAN classification of 802.1x clients (supplicants), this implementation of 802.1x secure port access extends this type of functionality to non-802.1x clients (non-supplicants). To this end device classification policies are introduced to handle supplicant and non- supplicant access to 802.1x ports.

Supplicant policies use 802.1x authentication through a remote RADIUS server and provide alternative methods for classifying supplicants if the authentication process either fails or does not return a VLAN ID.
Non-supplicant policies use MAC authentication through a remote RADIUS server or can bypass authentication and only allow strict assignment to specific VLANs. MAC authentication verifies the source MAC address of a non-supplicant device through a remote RADIUS server. Similar to 802.1 x authentications, the switch sends RADIUS frames to the server with the source MAC address embedded in the user name and password attributes.

The number of possible 802.1X users is 256 users per NI. This number is a total number of users that applies to all authenticated clients, such as 802.1X supplicants or non-supplicants. In addition, the use of all authentication methods and Learned Port Security (LPS) on the same port is supported.

Classification of both supplicant and non-supplicant devices using non-supplicant device classification policies is supported. As a result, MAC authentication is now applicable to both supplicant and non-supplicant devices.

Captive Portal
Captive Portal authentication is a configurable option within Access Guardian that allows Web browser clients to authenticate through the switch using 802.1x or MAC authentication via a RADIUS server. When the Captive Portal option is invoked, a Web page is presented to the user device to prompt the user to enter login credentials. If authentication returns a VLAN ID, the device is assigned to that VLAN. If a VLAN ID is not returned or authentication fails, a separate Captive Portal policy then determines the network access control for the supplicant or non-supplicant.

Captive Portal Web Pages
Customizing the following Captive Portal Web page components is allowed. These components are incorporated and displayed when the Web-based login page is presented to the user.

- Logo
- Welcome text
- Background image
- User Acceptable Policy text

- Login help page

Captive Portal checks the local switch for any customized files before presenting the login Web page to the user. If any such files exist, they are incorporated into the Web page display. If no such files exist, the default Web page components are used.

Captive Portal Browser Support
The Captive Portal authentication feature presents the user with a Web page for entering login credentials. The following table provides the platforms and browser support information for Captive Portal users:

Platforms Supported	Web Browser Supported
Windows XP	IE6, IE7, IE8, FireFox2 and FireFox3
Windows Vista	IE7, Firefox2 and Firefox3
Linux	Firefox2 and Firefox3

Access Control Lists (ACLs)
Access Control Lists (ACLs) are Quality of Service (QoS) policies used to control whether or not packets are allowed or denied at the switch or router interface. ACLs are sometimes referred to as filtering lists. ACLs are distinguished by the kind of traffic they filter. In a QoS policy rule, the type of traffic is specified in the policy condition. The policy action determines whether the traffic is allowed or denied.
In general, the types of ACLs include:

- **Layer 2 ACLs**—for filtering traffic at the MAC layer. Uses MAC addresses or MAC groups for filtering.
- **Layer 3/4 ACLs**—for filtering traffic at the network layer. Uses IP addresses or IP ports for filtering.
- **Multicast ACLs**—for filtering IGMP traffic.

Access Control Lists (ACLs) for IPv6
The following QoS policy conditions are available for configuring ACLs to filter IPv6 traffic:

- source ipv6
- destination ipv6
- ipv6
  - source tcp port
  - destination tcp port
  - source udp port
  - destination udp port

Note the following when using IPv6 ACLs:

- Trusted/untrusted behavior is the same for IPv6 traffic as it is for IPv4 traffic.
- IPv6 policies do not support the use of network groups, service groups, map groups, or MAC groups.
- IPv6 multicast policies are not supported.
- Anti-spoofing and other UserPorts profiles/filters do not support IPv6.
- The default (built-in) network group, "Switch", only applies to IPv4 interfaces. There is no such group for IPv6 interfaces.

ACL & Layer 3 Security
The following additional ACL features are available for improving network security and preventing malicious activity on the network:

- **ICMP drop rules**—Allows condition combinations in policies that will prevent user pings, thus reducing DoS exposure from pings. Two condition parameters are also available to provide more granular filtering of ICMP packets: icmptype and icmpcode.
- **TCP connection rules** — Allows the determination of an established TCP connection by examining TCP flags found in the TCP header of the packet. Two condition parameters are available for defining a TCP connection ACL: established and tcpflags.

- **Early ARP discard** — ARP packets destined for other hosts are discarded to reduce processing overhead and exposure to ARP DoS attacks. No configuration is required to use this feature; it is always available and active on the switch. Note that ARPs intended for use by a local subnet or VRRP are not discarded.
- **UserPorts** — A port group that identifies its members as user ports to prevent spoofed IP traffic. When a port is configured as a member of this group, packets received on the port are dropped if they contain a source IP network address that does not match the IP subnet for the port.
- **UserPorts Profile** —In addition to spoofed traffic, it is also possible to configure a global UserPorts profile to specify additional types of traffic, such as BPDU, RIP, OSPF, DVMRP, PIM, DHCP server response packets and DNS, to monitor on user ports. The UserPorts profile also determines whether user ports will filter the unwanted traffic or will administratively shutdown when the traffic is received. Note that this profile only applies to those ports that are designated as members of the UserPorts port group.
- **DropServices** — A service group that improves the performance of ACLs that are intended to deny packets destined for specific TCP/UDP ports. This group only applies to ports that are members of the UserPorts group. Using the DropServices group for this function minimizes processing overhead, which otherwise could lead to a DoS condition for other applications trying to use the switch.

ARP Defense Optimization
This feature enhances how the OmniSwitch can respond to an ARP DoS attack by not adding entries to the forwarding table until the next hop ARP entry can be resolved.

ARP Poisoning Detection
This feature detects the presence of an ARP-Poisoning host on the network using configured restricted IP addresses for which the switch, on sending an ARP request, should not get back an ARP response. If an ARP response is received, the event is logged and the user is alerted using an SNMP trap.
By default, ARP requests are not added to the ARP cache. Only router solicited ARP requests will be added to the cache.

Authenticated Switch Access
Authenticated Switch Access (ASA) is a way of authenticating users who want to manage the switch. With authenticated access, all switch login attempts using the console or modem port, Telnet, FTP, SNMP, or HTTP require authentication through the local user database or via a third-party server. The type of server may be an authentication-only mechanism or an authentication, authorization, and accounting (AAA) mechanism. AAA servers are able to provide authorization for switch management users as well as authentication. (They also may be used for accounting.) User login information and user privileges may be stored on the servers. The following AAA servers are supported on the switch:

- Remote Authentication Dial-In User Service (RADIUS). Authentication using this type of server was certified with Funk/Juniper Steel Belted RADIUS server (any industry standard RADIUS server should work).
- Lightweight Directory Access Protocol (LDAP).
- Terminal Access Controller Access Control System (TACACS+).

Authentication-only servers are able to authenticate users for switch management access, but authorization (or what privileges the user has after authenticating) is determined by the switch. Authentication- only servers cannot return user privileges to the switch. The authentication-only server supported by the switch is ACE/Server, which is a part of RSA Security's SecurID product suite. RSA Security's ACE/ Agent are embedded in the switch.

By default, switch management users may be authenticated through the console port through the local user database. If external servers are configured for other management interfaces but the servers become unavailable, the switch will poll the local user database for login information if the switch is configured for local checking of the user database. The database includes information about whether a user is able to log into the switch and what kinds of privileges or rights the user has for managing the switch.

Partitioned Switch Management - A user account includes a login name, password, and user privileges. The privileges determine whether the user has read or write access to the switch, and which command domains and

command families the user is authorized to execute on the switch. The privileges are sometimes referred to as authorization; the designation of particular command families or domains for user access is sometimes referred to as partitioned management.

Account & Password Policies - This feature allows a switch administrator to configure password policies for password creation and management. The administrator can configure how often a password must be changed, lockout settings for failed attempts, password complexity, history, and age as well as other account management settings.

Command Line Interface (CLI)
Command Line Interface (CLI) is a text-based configuration interface that allows you to configure switch applications and to view switch statistics. Each CLI command applicable to the switch is defined in the CLI Reference guide. All command descriptions listed in the Reference Guide include command syntax definitions, defaults, usage guidelines, example screen output, and release history.

The CLI uses single-line text commands that are similar to other industry standard switch interfaces.

DHCP Relay
DHCP Relay allows you to forward DHCP broadcast requests to configurable DHCP server IP address in a routing environment.

DHCP Relay is configured using the IP helper set of commands.

Preboot Execution Environment (PXE) support was enabled by default in previous releases. Note that in this release, it is disabled by default and is now a user-configurable option using the ip helper pxe-support commands.

Per-VLAN DHCP Relay - It is possible to configure multiple DHCP relay (ip helper) addresses on a per-vlan basis. For the Per- VLAN service, identify the number of the VLAN that makes the relay request. You may identify one or more server IP addresses to which DHCP packets will be sent from the specified VLAN. Both standard and per VLAN modes are supported.

DHCP Relay Agent Information Option
The DHCP Option-82 feature enables the relay agent to insert identifying information into client-originated DHCP packets before the packets are forwarded to the DHCP server. The implementation of this feature is based on the functionality defined in RFC 3046.
When DHCP Option-82 is enabled, communications between a DHCP client and a DHCP server are authenticated by the relay agent. To accomplish this task, the agent adds Option-82 data to the end of the options field in DHCP packets sent from a client to a DHCP server.
If the relay agent receives a DHCP packet from a client that already contains Option-82 data, the packet is dropped by default. However, it is possible to configure a DHCP Option-82 policy that directs the relay agent to drop, keep, or replace the existing Option-82 data and then forward the packet to the server.

DHCP Client Interface with option 60
The OmniSwitch now supports DHCP client functionality on any one configured VLAN. The DHCP client configured interface on an OmniSwitch can obtain an address from a DHCP server and create an IP interface for that VLAN on the switch.

- Release / Renew
- Lease Time
- Automatically configured the learned router as the switch's default gateway.
- Option 60 is configurable and it is sent as part of DHCP discovery/request packet
- Option 12 can be used to configure the switch's system name

DHCP Snooping
DHCP Snooping improves network security by filtering DHCP packets received from devices outside the network and building and maintaining a binding table (database) to log DHCP client access information. There are two levels of operation available for the DHCP Snooping feature: switch level or VLAN level.

To identify DHCP traffic that originates from outside the network, DHCP Snooping categorizes ports as either trusted or untrusted. A port is trusted if it is connected to a device inside the network, such as a DHCP server. A port is untrusted if it is connected to a device outside the network, such as a customer switch or workstation. The port trust mode is also configurable through the CLI.

Additional DHCP Snooping functionality includes the following:

- **IP Source Filtering** — Restricts DHCP Snooping port traffic to only packets that contain the client source MAC address and IP address obtained from the DHCP lease information. The DHCP Snooping binding table is used to verify the client lease information for the port that is enabled for IP source filtering.
- **Rate Limiting** — Limits the number of DHCP packets on a port. This functionality is provided using the QoS application to configure ACLs for the port.
- **User-configurable Option 82 Suboption Format** — Allows the user to specify the type of information (switch base MAC address, system name, or user-defined string) that is inserted into the Circuit ID and Remote ID suboptions of the Option-82 field. This functionality only applies when DHCP Snooping Option-82 Data Insertion is enabled.

DHCP Snooping – Layer 2
By default, DHCP broadcasts are flooded on the default VLAN for the client/server port. If the DHCP client and server are both members of the same VLAN domain, the broadcast packets from these sources are bridged as Layer 2 traffic and not processed by the relay agent.

The Omnswitch provides enhancements to DHCP Snooping to allow application of DHCP Snooping functionality to bridged DHCP client/server broadcasts without using the relay agent or requiring an IP interface on the client/server VLAN.

When DHCP Snooping is enabled at the switch level or for an individual VLAN, DHCP Snooping functionality is automatically applied to Layer 2 traffic. When DHCP Snooping is disabled at the switch level or disabled on the last VLAN to have snooping enabled on the switch, DHCP Snooping functionality is no longer applied to Layer 2 or Layer 3 traffic.

DNS Client
A Domain Name System (DNS) resolver is an internet service that translates host names into IP addresses. Every time you enter a host name, a DNS service must look up the name on a server and resolve the name to an IP address. You can configure up to three domain name servers that will be queried in turn to resolve the host name. If all servers are queried and none can resolve the host name to an IP address, the DNS fails. If the DNS fails, you must either enter an IP address in place of the host name or specify the necessary lookup tables on one of the specified servers.

Dynamic VLAN Assignment (Mobility)
Dynamic assignment applies only to mobile ports and requires the additional configuration of VLAN rules. When traffic is received on a mobile port, the packets are examined to determine if their content matches any VLAN rules configured on the switch. Rules are defined by specifying a port, MAC address, protocol, network address, or DHCP criteria to capture certain types of network device traffic. It is also possible to define multiple rules for the same VLAN. A mobile port is assigned to a VLAN if its traffic matches any one VLAN rule.

End User Partitioning (EUPM)
EUPM is used for customer login accounts that are configured with end-user profiles (rather than functional privileges specified by partitioned management). Profiles specify command areas as well as VLAN and/or port ranges to which the user has access. These profiles are typically used for end users rather than network administrators.

Ethernet Interfaces

Ethernet and Gigabit Ethernet port software is responsible for a variety of functions that support Ethernet and Gigabit Ethernet. These functions include initialization of ports, notifying other software modules when a port goes down, configuration of basic line parameters, gathering of statistics for Ethernet and Gigabit Ethernet ports, and responding to administrative enable/disable requests.

Configurable parameters include: autonegotiation (copper ports 10/100/1000/10000), trap port link messages, flood control, line speed, duplex mode, inter-frame gap, resetting statistics counters, and maximum and peak flood rates.

Flood control is configurable on ingress interfaces (flood rate and including/excluding multicast).

Ethernet OAM
Ethernet OAM (Operation, Administration, and Maintenance) provides service assurance over a converged Ethernet network. Ethernet OAM focuses on two main areas that are most in need by service providers and are rapidly evolving in the standards bodies: Service OAM and Link OAM. These two OAM protocols have unique objectives but are complementary to each other. Service OAM provides monitoring and troubleshooting of end-to-end Ethernet service instances, while Link OAM allows a provider to monitor and troubleshoot an individual Ethernet link. The end-to-end service management capability is the most important aspect of Ethernet OAM for service providers.

This implementation of Ethernet Service OAM supports both IEEE 802.1ag Version 8.1 and ITU-T Y.1731 for connectivity fault management. Performance monitoring is provided by ITU-T Y.1731 using both one-way and two-way ETH-DM. Additionally, this implementation can perform delay measurement for both ITU-T Y.1731 and IEEE 802.1ag maintenance endpoints. Although both standards are supported, the OmniSwitch implementation uses the 802.1ag terminology and hierarchy for Ethernet CFM configuration.

Ethernet OAM 802.3ah – Ethernet First Mile (EFM)
IEEE 802.3ah, defining Ethernet in the access networks that connects subscribers to their immediate service provider. EFM, EFM-OAM and LINKOAM refers to IEEE 802.3ah standard.
LINK OAM (operation, administration, and maintenance) is a tool which monitors Layer-2 link status on the network by sending OAM protocol data units (OAMPDUs) between the network devices. OAMPDUs contain control and status information used to monitor, test, and troubleshoot OAM-enabled links. By enabling LINK OAM on switch ports, network administrators can monitor the link-related issues on the first mile. LINK OAM provides network administrators the ability to monitor link performance, remote fault detection and remote loopback control.

Ethernet Ring Protection (ERP) – G.8032
Ethernet Ring Protection (ERP) switching is a self-configuring algorithm that maintains a loop-free topology while providing data path redundancy and network scalability. ERP provides fast recovery times for Ethernet ring topologies by utilizing traditional Ethernet MAC and bridge functions.

This implementation of ERP is based on ITU-T G.8032 and uses the ring Automatic Protection Switching (APS) protocol to coordinate the prevention of network loops within a bridged Ethernet ring. Loop prevention is achieved by allowing the traffic to flow on all but one of the links within the protected Ethernet ring. This link is blocked and is referred to as the Ring Protection Link (RPL). When a ring failure condition occurs, the RPL is unblocked to allow the flow of traffic to continue through the ring.

ERP – Overlapping Protected VLANs on a Single Node
In a network where all connected nodes cannot belong to a single ERP ring, the OmniSwitch supports multiple ERP rings. Each of the ERP rings has a different Service VLAN configured which allows the ERP PDUs to be processed by the corresponding ERP ring nodes. The Service VLANs configured for each of the ERP rings can be configured as a protected VLAN on the other ERP ring. The protected VLANS can be shared across ERP rings.

Ethernet Services (VLAN Stacking and Translation)
VLAN Stacking provides a mechanism for tunneling multiple customer VLANs (CVLAN) through a service provider network over the Ethernet Metropolitan Area Network (EMAN). The service provider network uses one or more service provider VLANs (SVLAN) by appending an 802.1Q double tag or VLAN Translation on a customer port

that contains the customer's assigned tunnel ID. This traffic is then encapsulated into the tunnel and transmitted through the service provider network. It is received on another Provider Edge (PE) that has the same tunnel ID.

This feature enables service providers to provide their customers with Transparent LAN Services (TLS). This service is multipoint in nature so as to support multiple customer sites or networks distributed over the edges of a service provider network.

This implementation of VLAN Stacking offers the following functionality:

- Ethernet service-based approach that is similar to configuring a virtual private LAN service (VPLS).
- Ingress bandwidth sharing across User Network Interface (UNI) ports.
- Ingress bandwidth rate limiting on a per UNI port, per CVLAN, or CVLAN per UNI port basis.
- CVLAN (inner) tag 802.1p-bit mapping to SVLAN (outer) tag 802.1p bit.
- CVLAN (inner) tag DSCP mapping to SVLAN (outer) tag 802.1p bit.
- Profiles for saving and applying traffic engineering parameter values.

L2 Control Protocol Tunneling
Enhances the User Network Interface (UNI) profile to allow control packets for the OAM and Lacpmarker protocols to be tunneled through the provider network with the configured destination MAC address. Additionally, support for the following Cisco protocols is added: VTP, VLAN, Uplink Fast, UDLD, PAGP, DTP, and CDP.

Advanced Ethernet Loopback
An Ethernet loopback test function is available to perform In-Service and Out-of-Service throughput testing during initial turn-up or on-the-fly in an active network. The loopback tests can be used to validate the configured Service Level Agreements (SLAs) and QoS parameters that are associated with a service or a flow.

Generic UDP Relay
In addition to BOOTP/DHCP relay, generic UDP relay is available. Using generic UDP relay, traffic destined for well-known service ports (for example, NBNS/NBDD, DNS, TFTP, and TACACS) or destined for a user-defined service port can be forwarded to a specific VLAN on the switch.

GVRP
The GARP VLAN Registration Protocol (GVRP), a protocol compliant with 802.1Q, dynamically learns and further propagates VLAN membership information across a bridged network. GVRP dynamically maintains and updates the registration and de-registration of VLANs and prunes unnecessary broadcast and unicast traffic. Through propagation of GVRP information, a device is continuously able to update its knowledge of the set of VLANs that currently have active members and of the ports through which those members can be reached.

Using GVRP, a single switch is manually configured with all the desired VLANs for the network, and all other switches on the network dynamically learn those VLANs. An end station can be plugged into any switch and can be connected to its desired VLAN. However, for end stations to make use of GVRP, they need Network Interface Cards (NIC) aware of GVRP. A trap will be sent if the number of dynamic VLANs exceeds the maximum threshold configured for GVRP.

Health Statistics
To monitor resource availability, the NMS (Network Management System) needs to collect significant amounts of data from each switch. As the number of ports per switch (and the number of switches) increases, the volume of data can become overwhelming. The Health Monitoring feature can identify and monitor a switch's resource utilization levels and thresholds, improving the efficiency in data collection.
Health Monitoring provides the following data to the NMS:

- Switch-level input/output, memory, and CPU utilization levels
- Module-level and port-level input/output utilization levels
- For each monitored resource, the following variables are defined:
- Most recent utilization level (percentage)
- Average utilization level over the last minute (percentage)
- Average utilization level over the last hour (percentage)

- Maximum utilization level over the last hour (percentage)
- Threshold level

Additionally, Health Monitoring provides the capacity to specify thresholds for the resource utilization levels it monitors, and generates traps based on the specified threshold criteria.

HTTP/HTTPS Port Configuration
The default HTTP port and the default Secure HTTP (HTTPS) port can be configured for the embedded Web server in the switch.

IP Multicast VLAN
The IP Multicast VLAN feature provides the ability to configure specific VLANs that are dedicated to distributing multicast traffic. These distribution VLANs connect to the nearest multicast router and support multicast traffic only.

IP Multicast VLANs are supported in both the enterprise environment and the VLAN Stacking environment. The ports are separately classified as VLAN stacking ports or as legacy ports (Fixed ports/Tagged Ports). To ascertain that data flow is limited to either the VLAN Stacking domain or the enterprise domain, VLAN Stacking ports must be members of only the VLAN Stacking VLANs, while the normal legacy ports must be members of only enterprise mode VLANs. Multiple sender ports are supported.

Interswitch Protocol (AMAP)
Alcatel-Lucent Interswitch Protocols (AIP) is used to discover adjacent switches and retain mobile port information across switches. By default, AMAP is enabled.
Alcatel-Lucent Mapping Adjacency Protocol (AMAP) is used to discover the network topology of Alcatel-Lucent switches in a particular installation. Using this protocol, each switch determines which switches are adjacent to it by sending and responding to Hello update packets. For the purposes of AMAP, adjacent switches are those that:

- Have a Spanning Tree path between them.
- Do not have any switch between them on the Spanning Tree path that has AMAP enabled.

IPv4 Support
Internet Protocol (IP) is a network-layer (Layer 3) protocol that contains addressing and control information that allow packets to be forwarded on a network. IP is the primary network-layer protocol in the Internet protocol suite. Along with the Transmission Control Protocol (TCP), IP represents the heart of the Internet protocols. IP is associated with several Layer 3 and Layer 4 protocols. These protocols are built into the base code loaded on the switch and they include:

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Bootstrap Protocol (BOOTP)/Dynamic Host Configuration Protocol (DHCP)
- Simple Network Management Protocol (SNMP)
- Telnet - client and server
- File Transfer Protocol (FTP) – client and server
- Ping
- Traceroute
- Address Resolution Protocol (ARP)
- Internet Control Message Protocol (ICMP)
- RIP I / RIP II
- ECMP
- Static routes

The base IP software allows you to configure an IP router interface, static routes, a default route, the Address Resolution Protocol (ARP), the router primary address, the router ID, the Time-to-Live (TTL) Value, IP-directed broadcasts, and the Internet Control Message Protocol (ICMP). In addition, this software allows you to trace an

IP route, display Transmission Control Protocol (TCP) information, and display User Datagram Protocol (UDP) information.
The switch operates only in single MAC router mode. In this mode, each router interface is assigned the same MAC address, which is the base chassis MAC address for the switch.

31-Bit Network Mask Support – Configuring a 31-bit netmask is supported to allow for a point-to-point Ethernet network between two routers.

IPv6 Support
IPv6 (documented in RFC 2460) is designed as a successor to IPv4 and is supported on the OmniSwitch. The changes from IPv4 to IPv6 fall primarily into the following categories:

- Address size increased from 32 bits (IPv4) to 128 bits (IPv6)
- Dual Stack IPv4/IPv6
- ICMPv6
- Neighbor Discovery
- Stateless Autoconfiguration
- RIPng
- Static Routes
- Ping6
- Traceroute6
- DNS client using Authority records
- Telnetv6 - Client and server
- File Transfer Protocol (FTPv6) – Client and server
- SSHv6 – Client and Server

OmniSwitch 6250 switches support hardware-based IPv6 routing.

IP DoS Filtering
By default, the switch filters the following denial of service (DoS) attacks, which are security attacks aimed at devices that are available on a private network or the Internet:

- ARP Flood Attack
- Invalid IP Attack
- Multicast IP and MAC Address Mismatch
- Ping Overload
- Packets with loopback source IP address

IP Multicast Switching (IPMS)
IP Multicast Switching is a one-to-many communication technique employed by emerging applications such as video distribution, news feeds, conferencing, netcasting, and resource discovery (OSPF, RIP2, and BOOTP). Unlike unicast, which sends one packet per destination, multicast sends one packet to all devices in any subnetwork that has at least one device requesting the multicast traffic. Multicast switching also requires much less bandwidth than unicast techniques and broadcast techniques since the source hosts only send one data stream to the ports on which destination hosts that request it are attached.

Destination hosts signal their intent to receive a specific multicast stream by sending a request to do so to a nearby switch using Internet Group Management Protocol (IGMP). The switch then learns on which ports multicast group subscribers are attached and can intelligently deliver traffic only to the respective ports. This mechanism is often referred to as IGMP snooping (or IGMP gleaning). Alcatel-Lucents implementation of IGMP snooping is called IP Multicast Switching (IPMS). IPMS allows an OmniSwitch to efficiently deliver multicast traffic in hardware at wire speed.

Both IGMP version 3 (IGMPv3), which handles forwarding by source IP address and IP multicast destination, and IGMP version 2 (IGMPv2), which handles forwarding by IP multicast destination address only, are supported. IPMS is supported on IPv4 and IPv6 (MLD) on the OmniSwitch 6250.
IP Multicast Switching (IPMS) - Proxying

IP multicast proxying and configuring the IGMP and MLD unsolicited report interval are available with this implementation of IPMS. Proxying enables the aggregation of IGMP and MLD group membership information and the reduction in reporting queriers. The unsolicited report interval refers to the time period in which to proxy any changed IGMP membership state.

IP Multinetting
IP multinetting allows multiple subnets to coexist within the same VLAN domain. This implementation of the multinetting feature allows for the configuration of up to eight IP interfaces per a single VLAN. Each interface is configured with a different subnet.

IP Route Map Redistribution
Route map redistribution provides the ability to control which routes from a source protocol are learned and distributed into the network of a destination protocol. A route map consists of one or more user- defined statements that can determine which routes are allowed or denied access to the network. In addition, a route map may also contain statements that modify route parameters before they are redistributed. Redistribution is configured by specifying a source and destination protocol and the name of an existing route map. Criteria specified in the route map are applied to routes received from the source protocol.

Learned Port Security (LPS)
Learned Port Security (LPS) provides a mechanism for authorizing source learning of MAC addresses on 10/100/1000, Gigabit, and Gigabit Ethernet ports. Using LPS to control source MAC address learning provides the following benefits:

- A configurable source learning time limit that applies to all LPS ports.
- A configurable limit on the number of MAC addresses allowed on an LPS port.
- Dynamic configuration of a list of authorized source MAC addresses.
- Static configuration of a list of authorized source MAC addresses.
- Two methods for handling unauthorized traffic: Shutting down the port or only blocking traffic that violates LPS criteria.
- A configurable limit to the number of filtered MAC addresses allowed on an LPS port. Conversion of dynamically learned MAC addresses to static MAC address entries.
- Support for all authentication methods and LPS on the same switch port.

Note: LPS is not configurable on link aggregate ports.

Learned MAC Address Notification - The LPS feature enables the OmniSwitch to generate an SNMP trap when a new bridged MAC address is learned on an LPS port. A configurable trap threshold number is provided to determine how many MAC addresses are learned before such traps are generated for each MAC address learned thereafter. Trap contents includes identifying information about the MAC, such as the address itself, the corresponding IP address, switch identification, and the slot and port number on which the MAC was learned.

Link Aggregation (static & 802.3ad)
Alcatel-Lucent's link aggregation software allows you to combine several physical links into one large virtual link known as a link aggregation group. Using link aggregation can provide the following benefits:

- Scalability. You can configure up to 32 link aggregation groups that can consist of 2, 4, or 8 Ethernet ports.
- Reliability. If one of the physical links in a link aggregate group goes down, the link aggregate group can still operate.
- Interoperability with Legacy Switches. Static link aggregation can interoperate with OmniChannel on legacy switches.

Alcatel-Lucent's link aggregation software allows you to configure the following two different types of link aggregation groups:

- Static link aggregate groups
- Dynamic (802.3ad) link aggregate groups

Loopback Detection
Loopback Detection (LBD) automatically detects and prevents L2 forwarding loops on ports in the absence of other loop-detection mechanisms like STP/RSTP/MSTP or when these mechanisms cannot detect it. Typically enabled in Metro Ethernet Access deployments, at the very edge to prevent customer induced network loops.

MAC Retention
The MAC Retention functionality is implemented to enhance Smart Continuous Switching for stackable products by retaining the base MAC address of the primary stack element during a takeover. As a result, both L2 and L3 traffic as well as the associated control protocols (for example, routing protocols, spanning tree) will be minimally affected during takeover. The MAC retention feature also has added enhancements for avoiding duplicate MAC scenarios. If the primary element is not returned to the stack after a preset time, a trap will be generated indicating the possibility of a duplicate MAC. A duplicate MAC scenario would occur if the primary element was put back into the network since the stack has retained the primary element's MAC address.

NTP Client
The Network Time Protocol (NTP) is used to synchronize the time of a computer client or server to another server or reference time source, such as a radio or satellite receiver. It provides client time accuracies within half a second on LANs and WANs relative to a primary server synchronized to Universal Coordinated Time (UTC) (for example, through a Global Positioning Service receiver).

Policy Server Management
Policy servers use Lightweight Directory Access Protocol (LDAP) to store policies that are configured through Alcatel-Lucent's PolicyView network management application. PolicyView is an OmniVista application that runs on an attached workstation.
The Lightweight Directory Access Protocol (LDAP) is a standard directory server protocol. The LDAP policy server client in the switch is based on RFC 2251. Currently, PolicyView is supported for policy management.

Port Mapping (Private VLANs)
Port Mapping is a security feature that controls peer users from communicating with each other. A Port Mapping session comprises a session ID and a set of user ports and/or a set of network ports. User ports within a session cannot communicate with each other and can only communicate via network ports. In a Port Mapping session with user port set A and network port set B, ports in set A can only communicate with ports in set B. If set B is empty, ports in set A can communicate with rest of the ports in the system.

A port mapping session can be configured in unidirectional or bidirectional mode. In the unidirectional mode, the network ports can communicate with each other within the same session. In the bidirectional mode, the network ports cannot communicate with each other. Network ports of a unidirectional port mapping session can be shared with other unidirectional sessions, but cannot be shared with any sessions configured in bidirectional mode. Network Ports of different sessions can communicate with each other.

Port Mirroring
When Port Mirroring is enabled, the active "mirrored" port transmits and receives network traffic normally, and the "mirroring" port receives a copy of all transmit and receive traffic to the active port. You can connect an RMON probe or network analysis device to the mirroring port to see an exact duplication of traffic on the mirrored port without disrupting network traffic to and from the mirrored port.

Up to two Port Mirroring sessions are supported per switch, one of which can be an RSPAN session. The session can be configured to a "N-to-1" session, where up to 24 source ports can be mirrored to a single destination port.

Port Monitoring
The Port Monitoring feature allows you to examine packets to and from a specific Ethernet port (either ingress or egress). You can select to dump captured data to a file, which can be up to 140K. Once a file is captured, you can FTP it to a Protocol Analyzer or PC for viewing.

By default, the switch will create a data file called "pmonitor.enc" in flash memory. When the 140K limit is reached, the switch will begin overwriting the data starting with the oldest captured data. However, you can configure the switch so it will not overwrite the data file. In addition, you can configure additional port monitoring files as long as you have enough room in flash memory. You cannot configure port mirroring and port monitoring on the same NI module.

Power over Ethernet (PoE)
The Power over Ethernet (PoE) software is supported on the OS6250-P24 model. PoE provides inline power directly from the switch's Ethernet ports. From these RJ-45 ports the devices receive both electrical power and data flow. PoE detects power based on PSE devices and not on class.
PoE supports both IEEE 802.3af and non-IEEE 802.3at standards. The redundant power supply for PoE is only for backup. If the primary power supply fails, then PoE can switch over seamlessly to the backup power supply.

Quality of Service (QoS)
Alcatel-Lucent QoS software provides a way to manipulate flows coming through the switch based on user-configured policies. The flow manipulation (generally referred to as Quality of Service or QoS) may be as simple as allowing or denying traffic, or as complicated as remapping 802.1p bits from a Layer 2 network to ToS values in a Layer 3 network. OmniSwitch 6250 switches support 8 queues per port.
QoS is implemented on the switch through the use of policies, created on the switch or stored in Policy View. While policies may be used in many different network scenarios, there are several typical types:

- **Basic QoS**—includes traffic prioritization and bandwidth shaping.
- **802.1p/ToS/DSCP**—includes policies for marking and mapping.
- **Policy Based Routing (PBR)**—includes policies for redirecting routed traffic.
- **Access Control Lists (ACLs)**—ACLs are a specific type of QoS policy used for Layer 2, Layer 3/4, and multicast filtering.

Note: To apply a Layer 2 rule to IPv6 traffic using the source or destination MAC address, add the "ipv6" keyword to a condition for that rule.

Auto-QoS Prioritization for NMS Traffic - This feature can be used to enable the automatic prioritization of NMS traffic—SSH (TCP Port 22), Telnet (TCP Port 23), WebView (HTTP Port 80) and SNMP (TCP port 161)—that is destined for the switch. Prioritization maximizes access for NMS traffic and helps to reduce the potential for DoS attacks.

Note: When automatic NMS prioritization is enabled, QoS policies that specify priority are not applied to the NMS traffic. Other QoS policies, however, are applied to this type of traffic as usual. If a policy specifies rate limiting, then the policy with the lowest rate limiting value is applied.

Auto-QoS Prioritization on IP Phones - This feature is used to automatically enable the prioritization of IP phone traffic. The traffic can be assigned a priority value or, if set to trusted mode, the IP phone packet is used to determine the priority. IP phone traffic is identified by examining the source MAC address of the packet received on the port. If the source MAC falls within one of the Alcatel-Lucent ranges below, the Auto-QoS feature automatically sets the priority.

00-80-9F-54-xx-xx to 00-80-9F-64-xx-xx
00-80-9F-66-xx-xx to 00-80-9F-6F-xx-xx
00-80-9F-8E-xx-xx to 00-80-9F-8F-xx-xx

Third-party devices can be added to this group as well.

Note: When automatic NMS prioritization is enabled, QoS policies that specify priority are not applied to the NMS traffic. Other QoS policies, however, are applied to this type of traffic as usual.

DSCP Ranges – Configuring a range of DSCP values in a single QoS DSCP policy condition is now supported. This eliminates the need for multiple condition statements to configure multiple DSCP values for traffic

classification. In addition, specifying a mask value is no longer required; QoS automatically calculates the appropriate mask value for each DSCP value specified.

Policy-Based Mirroring - This feature enhances the current port mirroring functionality on the OmniSwitch. It allows policies to be configured to determine when traffic should be mirrored based on policies rather than being restricted to a specified port. The following policies can be configured:

- Traffic from a source address.
- Traffic to a destination address.
- Traffic to and from an address.
- Traffic between two addresses.
- Traffic with a classification criterion based on packet contents other than addresses (for example, based on protocol, priority).
- VLAN-based mirroring - mirroring of packets entering a VLAN.

Policy-Based Mirroring limitations:

- The policy mirror action must specify the same analyzer port for all policies in which the action is used.
- One policy-based mirroring session supported per switch.
- One port-based mirroring session supported per switch. Note that policy-based and port-base mirroring are both allowed on the same port at the same time.
- One remote port-based mirroring session supported per switch.
- One port-monitoring session supported per switch.
- Only ingress policy-based mirroring is supported.

Policy Based Routing (Permanent Mode) - Policy Based Routing may be used to redirect traffic to a particular gateway based on source or destination IP address, source or destination network group, source or destination TCP/UDP port, a service or service group, IP protocol, or built-in source port group.

Traffic may be redirected to a particular gateway regardless of what routes are listed in the routing table. Note that the gateway address does not have to be on a directly connected VLAN; the address may be on any network that is learned by the switch.

Ingress and Egress Bandwidth Shaping - Bandwidth shaping is configured on a per port basis by specifying a maximum bandwidth value for ingress and egress ports. On the OmniSwitch 6250 switches, configuring maximum egress bandwidth is supported on a per COS queue basis for each port

Tri-Color Marking –Tri-Color Marking (TCM) provides a mechanism for policing network traffic by limiting the rate at which traffic is sent or received on a switch interface. The TCM policer meters traffic based on user-configured packet rates and burst sizes and then marks the metered packets as green, yellow, or red based on the metering results.

TCM policer meters each packet and passes the metering result along with the packet to the Marker. Depending upon the result sent by the Meter, the packet is then marked with either the green, yellow, or red color. The marked packet stream is then transmitted on the egress based on the color-coded priority assigned.

The TCM Meter operates in Color-Blind mode (the Color-Aware mode is not supported). In the Color-Blind mode, the Meter assumes that the incoming packet stream is uncolored.
There are two types of TCM marking supported:

- Single-Rate TCM (srTCM) — Packets are marked based on a Committed Information Rate (CIR) value and two associated burst size values: Committed Burst Size (CBS) and Peak Burst Size (PBS).
- Two-Rate TCM (trTCM) — Packets are marked based on a CIR value and a Peak Information Rate (PIR) value and two associated burst size values: CBS and PBS.

Both srTCM and trTCM operate in the same basic manner. The main difference between the two types is that srTCM uses one rate limiting value (CIR) and trTCM uses two rate limiting values (CIR and PIR) to determine packet marking.

QoS Egress Policy Rules
Egress policy rules allow administrators to enforce traffic controls on the egress queues as a "last resort" action. By default, QoS policy rules are applied to traffic ingressing the port. The QoS Policy List feature includes an "egress" policy list option to create a list of rules that are applied to traffic egressing a destination port(s). If a policy rule is not associated with an egress policy list, the rule will only apply to ingress traffic.

IEEE 802.1q/ad CFI/DEI Bit Stamping
When sr/trTCM ingress rate limiter is used, frames that are non-conforming to the SLA (yellow) might still be delivered to the egress port when the port is not congested. By enabling CFI/DEI bit stamping on these frames, a color-aware upstream switch would be able to treat these frames differently and drop them first when the network is congested.

QoS Policy Condition Enhancements
- VLAN IDs can be grouped together into a single VLAN group. Similar to other QoS group types such as MAC and port groups, creating a VLAN group avoids having to configure a separate policy condition for multiple VLAN IDs.
- Specifying a range of 802.1p values for an 802.1p policy condition is now supported. A condition must specify either a single 802.1p value or a range of 802.1p values; both are not supported at the same time. The ability to specify a range of 802.1p values is particularly useful when classifying Ethernet Services SAP traffic.

Map Several Inner DSCP/ToS Values to the Same Outer 802.1p Value
QoS policy rules take precedence over Ethernet Services SAP profile settings. As a result, QoS rules can be configured for advanced classification of SAP traffic, such as mapping several DSCP/ToS values to the same outer 802.1p value.

QoS Statistics Enhancements
- QoS statistics monitoring allows the gathering of egress CoS drop and transmit packet statistics for all ports by default. This also allows the user to display egress CoS queue statistics on a per port basis using existing QoS show commands.
- QoS commands used to display traffic statistics and system resource usages now include statistics for egress traffic. This applies to traffic classified using egress policy rules.

Remote Port Mirroring (802.1Q Based)
This feature provides a remote port mirroring capability where traffic from a local port can be carried across the network to an egress port where a sniffer can be attached. This feature makes use of an 802.1q tag to send the mirrored traffic over the network using tagged VLANs.

- There must not be any physical loop present in the remote port mirroring VLAN.
- Spanning Tree must be disabled for the remote port mirroring VLAN.
- BPDU mirroring will be disabled by default on all OS6250s.
- Source learning must be disabled or overridden on the ports belonging to the remote port mirroring VLAN on the intermediate and destination switches.
- On OS6250 switches the QoS redirect feature can be used to override source learning.

RIPv1/RIPv2
Routing Information Protocol (RIP) is a widely used Interior Gateway Protocol (IGP) that uses hop count as its routing metric. RIP-enabled routers update neighboring routers by transmitting a copy of their own routing table. The RIP routing table uses the most efficient route to a destination, that is, the route with the fewest hops and longest matching prefix.

OmniSwitch 6250 switches support RIP version 1 (RIPv1), RIP version 2 (RIPv2), and RIPv2 that is compatible with RIPv1. In addition, text key and MD5 authentication on an interface basis for RIPv2 is also supported. ECMP capability for up to four paths is also supported.

RIPng
The OmniSwitch 6250 switches support Routing Information Protocol next generation (RIPng) for IPv6 networks. RIPng is based on RIPv1/RIPv2 and is an Interior Gateway Protocol (IGP) best suited for moderate sized networks.

RIP Timer Configuration
- Update — The time interval between advertisement intervals.
- Invalid — The amount of time before an active route expires and transitions to the garbage state.
- Garbage — The amount of time an expired route remains in the garbage state before it is removed from the RIB.
- Holddown — The amount of time during which a route remains in the holddown state.

Redirect Policies (Port and Link Aggregate)
Two policy action commands are available for configuring QoS redirection policies: **policy action redirect port** and **policy action redirect linkagg**. A redirection policy sends traffic that matches the policy to a specific port or link aggregate instead of the originally intended destination. This type of policy may use any condition; the policy action determines which port or link aggregate to which the traffic is sent.

Note: The ingress and egress ports that participate in redirection policies must belong to the same VLAN.

RMON
Remote Network Monitoring (RMON) is an SNMP protocol used to manage networks remotely. RMON probes can be used to collect, interpret, and forward statistical data about network traffic from designated active ports in a LAN segment to an NMS (Network Management System) application for monitoring and analyzing without negatively impacting network performance. RMON software is fully integrated in the software to acquire statistical information.

This feature supports basic RMON 4 group implementation in compliance with RFC 2819, including the **Ethernet Statistics, History** (Control & Statistics), **Alarms**, and **Events** groups.

Router Discovery Protocol (RDP)
The Router Discovery Protocol (RDP) is an extension of ICMP that allows end hosts to discover routers on their networks. The implementation of RDP supports the router requirements as defined in RFC 1256. Using RDP, hosts attached to multicast or broadcast networks send solicitation messages when they start up. Routers respond to solicitation messages with an advertisement message that contains the router IP addresses. In addition, routers send advertisement messages when their RDP interface becomes active and then subsequently at random intervals.

Routing Protocol Preference
Specifying a routing protocol preference is supported. This is done by configuring a weight for each routing protocol (including static routes) to control which entry to prefer when two entries exist from different sources. By default, local routes always have precedence.

Secure Copy (SCP)
The **scp** CLI command is available for copying files in a secure manner between hosts on the network. The **scp** utility performs encrypted data transfers using the Secure Shell (SSH) protocol. In addition, **scp** uses available SSH authentication and security features, such as prompting for a password if one is required.

Secure Shell (SSH)
The Secure Shell feature provides a secure mechanism that allows you to log in to a remote switch, to execute commands on a remote device, and to move files from one device to another. Secure Shell provides secure, encrypted communications even when your transmission is between two untrusted hosts or over an unsecure network.

The OmniSwitch includes both client and server components of the Secure Shell interface and the Secure Shell FTP file transfer protocol. SFTP is a subsystem of the Secure Shell protocol. All Secure Shell FTP data are encrypted through a Secure Shell channel.

When used as an SSH Server, the following SSH Software is supported on the indicated operating systems:

SSH Software	Supported Operating Systems
OpenSSH	Sun Solaris, Mac OSX, Linux Red Hat
F-Secure	Sun Solaris, Win 2000, Win XP
SSH-Communication	Sun Solaris, Win 2000, Win XP, Linux Red Hat
PuTTY	Win 2000, Win XP
MAC-SSH	Mac OSX

When used as an SSH Client, the following SSH Software is supported on the indicated operating systems:

SSH Software	Supported Operating Systems
OpenSSH	Sun Solaris, Linux Red Hat, AOS
F-Secure	Sun Solaris, Win 2000
SSH-Communication	Sun Solaris, Win 2000, Win XP, Linux Red Hat

Secure Shell (SSH) Public Key Authentication
DSA public key authentication is supported when using PuTTY SSH software to generate the private and public key for the client and to access the switch. It is now possible to enforce the use of public key authentication only on the switch. By default, both password and public key authentication are allowed.

Service Assurance Agent (SAA)
With SAAs, users can verify service guarantees, increase network reliability by validating network performance and proactively identify network issues. SAA uses active monitoring to generate traffic in a continuous, reliable, and predictable manner, thus enabling the measurement of network performance and health.

SAA - Ethernet OAM
ETH-LB/DMM can be used to measure delay and jitter by sending frames with DM information to the peer MEP and receiving frames with DM information from the peer MEP.

SAA - IP ping
IP SAAs enhances the service level monitoring to become IP application-aware by measuring both end-to-end and at the IP layer. It allows performance measurement against any IP addresses in the network (example Switch, Server, PC).

Generic L2 SAA
L2 SAAs enhance the service level monitoring by enabling performance measurement against any L2 address within the provider network.

sFlow
sFlow is a network monitoring technology that gives visibility to the activity of the network, by providing network usage information. It provides the data required to effectively control and manage the network usage. sFlow is a sampling technology that meets the requirements for a network traffic monitoring solution. sFlow is a sampling technology embedded within switches/routers. It provides the ability to monitor the traffic flows. It requires a sFlow agent software process running as part of the switch software and a sFlow collector, which receives and analyses the monitored data. The sFlow collector makes use of SNMP to communicate with a sFlow agent in order to configure sFlow monitoring on the device (switch).

SNMP
The Simple Network Management Protocol (SNMP) is an application-layer protocol that allows communication between SNMP managers and SNMP agents on an IP network. Network administrators use SNMP to monitor network performance and to solve network problems. SNMP provides an industry standard communications

model used by network administrators to manage and monitor their network devices. The OmniSwitch supports SNMPv1, SNMPv2, and SNMPv3.

Source Learning
Source Learning builds and maintains the MAC address table on each switch. New MAC address table entries are created in one of two ways: they are dynamically learned or statically assigned. Dynamically learned MAC addresses are those that are obtained by the switch when source learning examines data packets and records the source address and the port and VLAN it was learned on. Static MAC addresses are user defined addresses that are statically assigned to a port and VLAN.

In addition, Source Learning also tracks MAC address age and removes addresses from the MAC address table that have aged beyond the configurable aging timer value.

Accessing MAC Address Table entries is useful for managing traffic flow and troubleshooting network device connectivity problems.

L2 Static Multicast Addresses - Static multicast MAC addresses are used to send traffic intended for a single destination multicast MAC address to multiple switch ports within a given VLAN. A static multicast address is assigned to one or more switch ports for a given VLAN. The ports associated with the multicast address are then identified as egress ports. When traffic received on ports within the same VLAN is destined for the multicast address, the traffic is forwarded on the egress ports that are associated with the multicast address. One of the benefits of using static multicast addresses is that multicast traffic is switched in hardware and no longer subject to flood limits on broadcast traffic.

Disable Learning on a per port basis
Provides the option to disable source learning on a per port basis. This feature is only supported on "hardware learning" ports and is not supported on mobile ports, LPS ports or Access Guardian ports. The feature is also supported for Link Aggregation where all ports in the aggregate are set to disable source learning. Configuration of static mac-addresses on such ports is still allowed.

Disable MAC learning on a per VLAN basis
Provides the option to disable source learning for all the ports of a VLAN. This feature is meant to be used on a ring topology where a VLAN only contains two ports.

It is recommended to have only 2 ports in a VLAN that has source learning disabled.

Software Rollback
The directory structure inherent in an OmniSwitch switch allows for a switch to return to a previous, more reliable version of image or configuration files.

Changes made to the configuration file may alter switch functionality. These changes are not saved unless explicitly done so by the user. If the switch reboots before the configuration file is saved, changes made to the configuration file prior to the reboot are lost.

New image files should be placed in the working (non-certified) directory first. New image or configuration files can be tested to decide whether they are reliable. Should the configuration or image files prove to be less reliable than their older counterparts in the certified directory, then the switch can be rebooted from the certified directory, and "rolled back" to an earlier version.

Once the contents of the working directory are established as good files, then these files can be saved to the certified directory and used as the most reliable software to which the switch can be rolled back to in an emergency situation.

Spanning Tree
In addition to the Q2005 version of MSTP, the Alcatel-Lucent Spanning Tree implementation also provides support for the 802.1w Rapid Spanning Tree Algorithm and Protocol (RSTP) and the 802.1D Spanning Tree

Algorithm and Protocol (STP). All three supported protocols ensure that there is always only one data path between any two switches for a given Spanning Tree instance to prevent network loops.

802.1Q 2005 (MSTP) - 802.1Q 2005 (Q2005) is a version of Multiple Spanning Tree Protocol (MSTP) that is a combination of the 802.1D 2004 and 802.1S protocols. This implementation of Q2005 also includes improvements to edge port configuration and provides administrative control to restrict port role assignment and the propagation of topology change information through bridge ports.
Q2005 (MSTP) is only available when the flat mode is active for the switch. The flat mode applies a single spanning tree instance across all VLAN port connections on a switch. MSTP allows the configuration of Multiple Spanning Tree Instances (MSTIs) in addition to the CST instance. Each MSTI is mapped to a set of VLANs. As a result, flat mode can now support the forwarding of VLAN traffic over separate data paths.

Automatic VLAN Containment (AVC)
In a 802.1s Multiple Spanning Tree (MST) configuration, it is possible for a port that belongs to a VLAN, which is not a member of an instance, to become the root port for that instance. This can cause a topology change that could lead to a loss of connectivity between VLANs/switches. Enabling Automatic VLAN Containment (AVC) helps to prevent this from happening by making such a port an undesirable choice for the root.

When AVC is enabled, it identifies undesirable ports and automatically configures them with an infinite path cost value.
Balancing VLANs across links according to their Multiple Spanning Tree Instance (MSTI) grouping is highly recommended to ensure that there is not a loss of connectivity during any possible topology changes. Enabling AVC on the switch is another way to prevent undesirable ports from becoming the root for an MSTI.

802.1D STP and 802.1w RSTP - STP and RSTP are available in both the flat and 1x1 mode. However, when using 802.1D or 802.1w in the flat mode, the single spanning tree instance per switch algorithm applies. Note that 802.1w is the default Spanning Tree protocol for the switch regardless of which mode is active. This default value will apply to future releases as well.

PVST+ Interoperability - The current Alcatel-Lucent 1x1 Spanning Tree mode has been extended to allow all user ports on an OmniSwitch to transmit and receive either the standard IEEE BPDUs or proprietary PVST+ BPDUs. An OmniSwitch can have ports running in either 1x1 modes when connecting to another OmniSwitch, or PVST+ mode simultaneously.

- It is mandatory that all the Cisco switches have the MAC Reduction Mode feature enabled.
- Priority values can only be assigned in multiples of 4096 to be compatible with the Cisco MAC Reduction mode.
- In a mixed OmniSwitch and Cisco environment, it is highly recommended to enable PVST+ mode on all OmniSwitches in order to maintain the same root bridge for the topology.
- Alcatel-Lucent's PVST+ interoperability mode is not compatible with a switch running in PVST mode.
- The same default path cost mode, long or short, must be configured the same way on all switches.

RRSTP - Ring Rapid Spanning Tree Protocol (RRSTP) is complimentary to either the Rapid Spanning Tree (RSTP) or the Multiple Spanning Tree Protocol (MSTP) but is designed to enhance convergence time in a ring configuration when a link failure occurs. Note that RRSTP is supported only in a ring topology where switches are connected point to point. In addition, there can be no alternate connections for the same instance between any two switches within a ring topology.

RRSTP reduces convergence time by finding the bridge that hosts the alternate (ALT) port and immediately changing the ALT port state to forwarding without altering the port state. This process quickly enables the data path. The RRSTP frame travels from the point of failure to the ALT port in both directions. The MAC addresses corresponding to the ports in the ring are flushed to make the data path convergence time much faster. While RRSTP is already reacting to the loss of connectivity, the standard BPDU carrying the information about the link failure is processed in normal fashion at each hop. When this BPDU reaches the bridge whose ALT port is now in the "ALT FWD" state, due to RRSTP frame processing, it updates the state of the two ports in the ring as per the STP standard.

RRSTP is only supported when the switch is configured in Flat mode (RRSTP or MSTP).

Switch Logging
The Switch Logging feature is designed to provide a high-level event logging mechanism that can be useful in maintaining and servicing the switch. Switch Logging uses a formatted string mechanism to process log requests from applications. When a log request is received, Switch Logging verifies whether the Severity Level included with the request is less than or equal to the Severity Level stored for the appropriate Application ID. If it is, a log message is generated using the formatting specified by the log request and placed on the Switch Log Queue, and Switch Logging returns control back to the calling application. Otherwise, the request is discarded. The default output device is the log file located in the Flash File System. Other output devices can be configured via Command Line Interface. All log records generated are copied to all configured output devices.

Command Line Interface can be used to display and configure Switch Logging information. Log information can be helpful in resolving configuration or authentication issues, as well as general errors.

Syslog to Multiple Hosts - Sending syslog files to multiple hosts is allowed. It is possible to specify up to a maximum of four servers.

Trivial File Transfer Protocol (TFTP) Client
TFTP, a client-server protocol, is used to transfer files between a TFTP server and client. TFTP client functionality on the OmniSwitch is used to download files from or upload files to a TFTP server.

Text File Configuration
The text file configuration feature allows you to configure the switch using an ASCII-based text file. You may type CLI commands directly into a text document to create a configuration file. This file resides in the switch's file system. You can create configuration files in the following ways.

- You may create, edit, and view a file using a standard text editor (such as Microsoft NotePad) on a workstation. The resulting configuration file is then uploaded to the switch.
- You can invoke the switch's CLI **snapshot** command to capture the switch's current configuration into a text file.
- You can use the switch's text editor to create or make changes to a configuration file.

UDLD - Fiber and Copper
The unidirectional link detection protocol is a protocol that can be used to detect and disable malfunctioning unidirectional Ethernet fiber or copper links. Errors due to improper installation of fiber strands, interface malfunctions, media converter faults, etc can be detected and the link can be disabled. It operates at Layer 2 in conjunction with IEEE 802.3's existing Layer 1 fault detection mechanisms.

User Definable Loopback Interface
Loopback0 is the name assigned to an IP interface to identify a consistent address for network management purposes. The Loopback0 interface is not bound to any VLAN, therefore it always remains operationally active. This differs from other IP interfaces, such that if there are no active ports in the VLAN, all IP interfaces associated with that VLAN are not active. In addition, the Loopback0 interface provides a unique IP address for the switch that is easily identifiable to network management applications.

User Network Profiles
This feature provides the capability to have "Roles" assigned to users during authentication. This allows for a VLAN to be associated to a role, users matching the role will automatically be assigned to that VLAN. The role should be configured to match the Filter-ID attribute being returned by the RADIUS server.

VLANs
One of the main benefits of using VLANs to segment network traffic is that VLAN configuration and port assignment is handled through switch software. This eliminates the need to physically change a network device connection or location when adding or removing devices from the VLAN broadcast domain.
The VLAN management software handles the following VLAN configuration tasks:

- Creating or modifying VLANs.

- Assigning or changing default VLAN port associations (VPAs).
- Enabling or disabling VLAN participation in the current Spanning Tree algorithm.
- Enabling or disabling classification of mobile port traffic by 802.1Q tagged VLAN ID.
- Enabling or disabling VLAN authentication.
- Enabling or disabling unique MAC address assignments for each router VLAN defined.
- Displaying VLAN configuration information.

Up to 4094 VLANs for Flat Spanning Tree mode and 252 VLANs for 1x1 Spanning Tree mode are supported. In addition, it is also possible to specify a range of VLAN IDs when creating or deleting VLANs and/or configuring VLAN parameters, such as Spanning Tree bridge values.

Web-Based Management (WebView)
The switch can be monitored and configured using WebView, Alcatel-Lucent's web-based device management tool. The WebView application is embedded in the switch and is accessible through the following web browsers:

- Internet Explorer 6.0 and later for Windows NT, 2000, XP, 2003, Vista
- Firefox 2.0 and later for Windows and Solaris SunOS 5.10