Release Notes

OmniSwitch 6850E/6855/9000E

Release 6.4.6.R01

This release notes accompany release 6.4.6.R01 software for the OmniSwitch 6850E/6855/9000E hardware. The release notes provides important information on individual software features and hardware modules for the current release and related previous releases. Since much of the information in this 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.

Note: The OS6400 is not supported in Release 6.4.6.R01.

ATTENTION: Please refer to the 6.4.6.R01 Prerequisite section for important release specific information prior to upgrading or incorporating a switch with AOS release 6.4.6.R01.

Contents

Related Documentation

This release notes should be used in conjunction with the OmniSwitch 6850E, 6855, and 9000E user manuals. The following are the titles and descriptions of the user manuals that apply to this release.

User manuals can be downloaded at:

http://enterprise.alcatel-lucent.com/?dept=UserGuides&page=Portal

- **OmniSwitch 6850E Series Getting Started Guide**
  Describes the hardware and software procedures for getting an OmniSwitch 6850E Series switch up and running.
- **OmniSwitch 6855 Series Getting Started Guide**
  Describes the hardware and software procedures for getting an OmniSwitch 6855 Series switch up and running.
- **OmniSwitch 9000E Series Getting Started Guide**
  Describes the hardware and software procedures for getting an OmniSwitch 9000E Series switch up and running.
- **OmniSwitch 6850E Series Hardware User Guide**
  Complete technical specifications and procedures for all OmniSwitch 6850E Series chassis, power supplies, and fans.
- **OmniSwitch 6855 Series Hardware User Guide**
  Complete technical specifications and procedures for all OmniSwitch 6855 Series chassis, power supplies, and fans.
- **OmniSwitch 9000E Series Hardware User Guide**
  Complete technical specifications and procedures for all OmniSwitch 9000E Series chassis, power supplies, and fans.
- **OmniSwitch AOS Release 6 CLI Reference Guide**
  Complete reference to all CLI commands supported on the OmniSwitch. Includes syntax definitions, default values, examples, usage guidelines, and CLI-to-MIB variable mappings.
- **OmniSwitch AOS Release 6 Network Configuration Guide**
  Includes network configuration procedures and descriptive information on all the major software features and protocols included in the base software package. Chapters cover Layer 2 information (Ethernet and VLAN configuration), Layer 3 information (routing protocols), security options (Authenticated Switch Access (ASA), Quality of Service (QoS), link aggregation.
- **OmniSwitch AOS Release 6 Switch Management Guide**
  Includes procedures for readying an individual switch for integration into a network. Topics include the software directory architecture, software rollback protections, authenticated switch access, managing switch files, system configuration, using SNMP, and using web management software (WebView).
- **OmniSwitch AOS Release 6 Advanced Routing Configuration Guide**
  Includes network configuration procedures and descriptive information on all the software features and protocols included in the advanced routing software package. Chapters cover multicast routing (DVMRP and PIM), BGP, OSPF, and OSPFv3.
- **OmniSwitch AOS Release 6 Transceivers Guide**
  Includes SFP and XFP transceiver specifications and product compatibility information.

- **Upgrade Instructions for 6.4.6.R01**
  Provides instructions for upgrading the OmniSwitch 6850E, 6855, and 9000E to 6.4.6.R01 (Included in this document).
- **Technical Tips, Field Notices**
  Contracted customers can visit our customer service website at: service.esd.alcatel-lucent.com.

System Requirements

Memory Requirements

- OmniSwitch 6850E Series Release 6.4.6.R01 requires 512 MB of SDRAM and 128 MB of flash memory. This is the standard configuration shipped.
- OmniSwitch 6855 Series Release 6.4.6.R01 requires 256 MB of SDRAM and 128 MB flash memory. This is the standard configuration shipped.
- OmniSwitch 9000E Series Release 6.4.6.R01 requires 1GB of SDRAM and 256 MB of flash memory for the Chassis Management Module (CMM). 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.

UBoot, FPGA, Miniboot, BootROM, Upgrade Requirements

The software versions listed below are the MINIMUM required, except where otherwise noted. Switches running the minimum versions, as listed below, do not require any Uboot, Miniboot, or FPGA upgrades when upgrading to AOS 6.4.6.R01.

Switches not running the minimum version required should upgrade to the latest Uboot, Miniboot, FPGA that is available with the 6.4.6.R01 AOS software available from Service & Support.

Note: Refer to the **6.4.6.R01 Upgrade Instructions** section for step-by-step instructions on upgrading to Release 6.4.6.R01.

OmniSwitch 9000E

Release	Miniboot.uboot CMM	UBoot CMM	UBoot NI	FPGA CMM
CMM/NI with Old Flash 6.4.6.125.R01	6.4.3.479.R01	6.4.3.479.R01	6.4.3.479.R01	Major Revision: 2 Minor Revision: 25 (displays as 0x19; recommended)
CMM/NI with New Flash 6.4.6.125.R01	6.4.4.506.R01	6.4.4.506.R01	6.4.4.506.R01	Major Revision: 2 Minor Revision: 25 (displays as 0x19; recommended)

Note: Refer to the **Required Minimum Uboot for Modules with New Flash Component** for help with determining OS9000E module Flash components.

OmniSwitch 6850E

Release	Miniboot.uboot	UBoot	CPLD
6.4.6.125.R01	6.4.5.398.R02	6.4.5.398.R02	OS6850E-C24/P24/C48/P48 (10 or 11) OS6850E-U24X (7 or 8)

Note: CPLD version 17 is shipped for OS6850E-C24/P24/C48/P48 by factory default. CPLD version 12 is shipped for OS6850E-U24X by factory default.

OmniSwitch 6850E with OS-BPS

Release	Miniboot.uboot	UBoot	CPLD
6.4.6.125.R01	6.4.5.398.R02	6.4.5.398.R02	OS6850E-24/P24/48/P48 (17)

Note: The OS-BPS is not supported with the OS6850E-U24X.

OmniSwitch 6855-14/24/U10/U24/U24X

Release	Miniboot.uboot	UBoot	FPGA
6.4.6.125.R01	6.4.3.479.R01	6.4.3.479.R01	v2.2

OmniSwitch 6855-P14

Release	Miniboot.uboot	UBoot	FPGA
6.4.6.125.R01	6.4.4.5.R02	6.4.4.5.R02	v1.4

Prerequisites

Please verify the code version of a new switch being inserted into an existing stack. In some cases it may be required to downgrade a new switch running AOS release 6.4.6 prior to inserting it into an existing stack that is running an earlier code version. Please refer to the Downgrade Instructions.

Supported Hardware/Software Combinations

The following table shows the 6.X software releases that support each of the listed OS6850E, OS6855 and 9000E module types:

Module Type	Part No.	6.3.1.R01	6.3.2.R01	6.3.3.R01	6.3.4.R01	6.4.1.R01	6.4.2.R01	6.4.3.R01	6.4.4.R01	6.4.5.R02	6.4.6.R01
OS9700E/9702E-CMM	902668	no	no	no	no	supported	supported	supported	supported	supported	supported
OS9702E-CMM	902808	no	no	no	no	supported	supported	supported	supported	supported	supported
OS9702-CHASSIS	902727	no	no	no	supported	supported	supported	supported	supported	supported	supported
OS9-GNI-C24E	902669	no	no	no	no	supported	supported	supported	supported	supported	supported
OS9-GNI-U24E	902670	no	no	no	no	supported	supported	supported	supported	supported	supported
OS9-XNI-U2E	902671	no	no	no	no	supported	supported	supported	supported	supported	supported
OS9-XNI-U12E	902851	no	no	no	no	no	no	supported	supported	supported	supported
OS9-GNI-P24E	902927	no	no	no	no	no	no	no	supported	supported	supported
OS6855-14	902648	no	supported	no	supported	no	supported	supported	supported	supported	supported
OS6855-24	902664	no	supported	no	supported	no	supported	supported	supported	supported	supported
OS6855-U10	902647	no	supported	no	supported	no	supported	supported	supported	supported	supported
OS6855-U24	902555	no	supported	no	supported	no	supported	supported	supported	supported	supported
OS6855-U24X	902802	no	no	no	no	no	supported	supported	supported	supported	supported
OS6855-P14	902970	no	no	no	no	no	no	no	supported	supported	supported
OS6850E-24	902936	no	no	no	no	no	no	no	supported	supported	supported
OS6850E-P24	902934	no	no	no	no	no	no	no	supported	supported	supported
OS6850E-24X	902937	no	no	no	no	no	no	no	supported	supported	supported
OS6850E-P24X	902935	no	no	no	no	no	no	no	supported	supported	supported
OS6850E-48	902938	no	no	no	no	no	no	no	supported	supported	supported
OS6850E-P48	902932	no	no	no	no	no	no	no	supported	supported	supported
OS6850E-48X	902939	no	no	no	no	no	no	no	supported	supported	supported
OS6850E-P48X	902933	no	no	no	no	no	no	no	supported	supported	supported
OS6850E-U24X	902940	no	no	no	no	no	no	no	supported	supported	supported

New Hardware Supported

SFP-10G-24DWD80 Transceiver

Now supported on OS9-XNI-U12E, 6850E, 6850E-U24X.

iSFP-100-MM Transceiver

Now supported on OS9-GNI-U24E, OS6850E, OS6850E-U24X.
Note: Not supported on SFP+ ports.

iSFP-GIG-SX Transceiver

Now supported on OS9-GNI-U24E, OS9-XNI-U12E, OS6850E, OS6850E-U24X.
Note: Not supported on SFP+ ports.

iSFP-GIG-LX Transceiver

Now on OS9-GNI-U24E, OS9-XNI-U12E, OS6850E, OS6850E-U24X.
Note: Not supported on SFP+ ports.

iSFP-10G-LR Transceiver

Now supported on OS9-XNI-U12E, OS6850E , OS6850E-U24X.

iSFP-GIG-EZX Transceiver.

Now supported on OS9-GNI-U24E, OS6850E, OS6850E-U24X.

iSFP-GIG-BX-D/U Transceiver

Now supported on OS9-GNI-U24E, OS6850E, OS6850E-U24X.

iSFP-10G-ER Transceiver

Now supported on OS9-XNI-U12E, OS6850E, OS6850E-U24X.

6.4.6.R01 New Software Features and Enhancements

The following software features and enhancements are new with the 6.4.6.R01 release, subject to the feature exceptions and problem reports described later in these release notes:

6.4.6.R01 New Feature/Enhancement Summary

Feature	Platform	Software Package
Hardware/Stacking Features:		
- Split Stack Protection (SSP)	6850E OS9000E (helper function only)	Base
- LLDP PoE power negotiation	6850E/9000E	Base
Layer 3 Features:		
- ISIS-IPv6	All	Adv. Rtg.
- M-ISIS	All	Adv. Rtg.
Management Features :		
- Enabling or Disabling Console Session	All	Base
Monitoring/Troubleshooting Features :		
- Gigaword packet counter	All	Base
Multicast Features:		
- PIM Startup Delay	All	Adv. Rtg.
- Initiak multicast packet loss	All	Base
- Multicast Address Boundaries	All	Base
- L2 Star-G mode	All	Base
QoS Features :		
- Per port rate limiting	All	Base
Security Features :		
- Case sensitive MAC address	All	Base
- HIC HTTPS Web redirection	All	Base
VRF Features :		
- IP Helper per-VLAN / per-VRF	All	Base
Application Fluency :		
- mDNS Relay	All	Base
- VDI Support	All	Base

Feature	Platform	Software Package
Bring Your Own Device (BYOD)		
- Clearpass and Access Guardian Integration - Change of Authorization (CoA) - Port Bounce and URL redirect	All	Base
Additional Features:		
- 802.1q Capability on NNI ports	All	Base
- Autoboot Interruption	6850E/6855	Base
- Control packet tunneling enhancement	All	Base

6.4.6.R01 - New Feature/Enhancement Descriptions

Hardware/Stacking Features

Split Stack Protection (SSP)

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

Stack Split Protection provides the following benefits:

- Avoid network disruptions by preventing duplicate MAC and IP addresses on the network.
- The sub-stack that forms out of the stack split is able to detect that a stack split has occurred by use of a helper switch. The helper functionaltiy is supported on an OS6850E, OS9000E, or OS6450 (with the appropriate 6.6.4 maintenance release).
- Once the stack split condition has been determined, the sub-stack will put its front-panel ports into an operationally down state preventing traffic forwarding and avoiding loops and possible traffic disruption. The SSP link aggregate ports will remain up.
- A trap can be sent by the active-stack indicating the stack split state. The trap indicates that the stack split has occured and which elements are in the operationally down sub-stack.
- The entire stack will automatically recover when the sub-stacks rejoin the stack.

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

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

Note: Please contact Service & Support for information on availability for OS6855 platforms.

LLDP PoE Power Negotion

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

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

Layer 3 Features

ISIS IPv6

Intermediate System-Intermediate System (IS-IS) is a shortest path first (SPF) or link-state protocol. IS-IS is an interior gateway protocol (IGP) that distributes routing information between routers in a single autonomous system (AS) for IP (IPv4 and IPv6) as well as OSI environments. This feature allows a single routing protocol to support pure IP and OSI environments, and dual environments. Integrated IS-IS is also deployed extensively in an IP-only environment.

This release extends the support of ISIS for IPv6.

M-ISIS

Multi-topology (M-ISIS) support is necessary in IS-IS to support network domains in which non-dual stack IS-IS routers exist. The default protocol behavior of IS-IS is to construct shortest paths through the network using the routers' MAC addresses with no regard to the different IP address families supported. This behavior may result in black-holed routing when there are some IPv4-only or IPv6-only routers in an IS-IS routing domain, instead of all dual-stack routers.

M-ISIS mechanism runs multiple, independent IP topologies within a single IS-IS network domain, using separate topology-specific SPF computation and multiple Routing Information Bases (RIBs).

M-ISIS is advised in networks containing ISIS enabled routers with a combination of IPv4 and IPv6 capabilities.

Management Features

Enabling or Disabling the Console Session

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

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

It is recommended to create a back-up of the configuration file before using this feature. If remote access to the switch is lost (i.e Telnet, SSH, Webview) contact customer support to restore the access.

Note: This feature applies to the primary console port, the secondary port remains active.

Monitoring/Troubleshooting Features

Gigaword Packet Counters

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 the RADIUS standard, it can support a maximum value of 4GB (2^32 -1= 4,294.967,295). 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. 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.

Multicast Features

PIM Startup Delay

In certain networks, when PIM becomes active before the unicast applications like OSPF and BGP, multicast packet loss may be observed until the unicast routing information is updated. To overcome such packet loss due to startup latency between the PIM and unicast routing applications, a user-define startup delay has been introduced in PIM.

This feature enhancement provides the ability to configure the startup delay for PIM neighborship, so that the PIM neighborship will be formed after the delay value configured . This delay is applicable only when the switch boots up. A CLI option is added to configure the PIM startup delay, with an appropriate value, 0 being the default. If a startup delay is configured then PIM will not become globally enabled until after the delay period. This will ensure that none of the PIM interfaces become enabled until after the configured startup delay.

```
->  ip pim startup-delay <seconds>
```

The delay can be configured in the range of 0 to 120. The default value for delay is 0.

Initial Multicast Packet Routing

Multicast is often used for audio\video streaming applications where the first packet may be dropped as it is used for learning the new flow. However, some multicast applications require the initial packets sent by the multicast source to be received. The packet buffering functionality can be enabled to prevent those first multicast packets from being dropped.

Following debug CLIs can be used to modify the default values for packet buffering.

- debug ip set ipedrMaxPacketsPerSgv – to modify the number of packets that can be buffered for a particular flow. Default value is 4 packets.
- debug ip set ipedrMaxSgv – to modify the number of SGVs that can be buffered. Default value is 16 SGVs.
- debug ip set ipedrMaxBufTimeout - to modify the time up to which buffered packet can be in IPMS NI. Default value is 10 seconds.

Contact Service and Support before implementing the debug capability on an OmniSwitch.

Multicast Address Boundaries

Multicast boundaries confine multicast addresses to a particular domain. Confining multicast addresses helps to ensure that multicast data traffic passed within a multicast domain does not conflict with multicast users outside the domain.

Multicast addresses 239.0.0.0 through 239.255.255.255 have been reserved by the IANA as administratively scoped addresses for use in private multicast domains. These addresses cannot be used for any other protocol or network function. Because they are regulated by the IANA, these addresses can theoretically be used by network administrators without conflicting with networks outside of their multicast domains. However, to ensure that the addresses used in a private multicast domain do not conflict with other domains (for example, within the company network or out on the Internet), multicast address boundaries can be configured.

AOS supports configuration of multicast route boundaries for the entire multicast group including scoped multicast addresses (224.0.0.0 through 239.255.255.255).

By default, route boundary configuration is supported for the scoped addresses (239.0.0.0 to 239.255.255.255). Use "**debug ip set ipMRouteBoundaryXpand num**" command to allow multicast route boundary configuration on the complete multicast group range (224.0.0.0 to 239.255.255.255). You are required to set the debug variable to non-zero value to allow expanded range of addresses to be supported for route boundary configuration. Changing the variable value to '0' sets the route boundary configuration to its default, that is, route boundary support for only scoped multicast address range.

Configuring this feature is not standards compliant.

L2 star-G Mode for Multicast Group

When multiple hosts are a part of single multicast group, every host will have a unique entry in the IPMC table. This increases the hardware entries in IPMC table and could affect other normal multicast services. In such a scenario, configuring L2 star-G (*, G) mode for the multicast group reduces the IPMC index utilization by preventing creation of multiple multicast entries. A single star-G entry for the multicast group is created in the IPMC table.

This feature is supported both for IPv4 and IPv6 network.

Note: By default, 10 multicast groups can be configured in L2 star-G mode. This default number can be changed by modifying the global variable *ipms_maxgroup_starg* by adding the following to the AlcatelDebug.cfg file and rebooting the switch.

- debug set ipms_maxgroup_starg <num-groups>

Contact Service and Support before implementing the debug capability on an OmniSwitch.

QoS Features

Per port rate limiting

Port Group and Per Port Rate Limiting

Per port rate limiting allows configuring a policy rule that specifies a rate limiter for the group of ports or individual port. This can be achieved by configuring specific mode for the port group. The following two modes are supported:

- Non-split: This mode applies the rate limiting rule to a group of ports specified in the rule. This is the default behavior for the source port group.
- Split: This mode applies the rate limiting rule to individual ports specified in the group of ports in the rule.

Per port rate limiting is not supported for a destination port group.

Port Groups and Maximum Bandwidth

Maximum bandwidth policies are applied to source (ingress) ports and/or flows. This applies to flows that involve more than one port. Based on the rate limit mode set on the port group, the maximum bandwidth is applied.

Application Fluency Features

VDI Support

The Virtual Desktop Infrastructure (VDI) solution transforms desktops and applications into a secure on demand service which can be accessed by users anywhere. It optimizes the delivery of desktops, applications and data to users.

The Citrix XenDesktop is the desktop virtualization solution which includes all the capabilities required to deliver desktops, applications, and data securely to every user in an enterprise. With centrally deployed secure remote access to PCs on a corporate network it gives users fast, high-fidelity remote access to corporate applications and data.

The OmniSwitch identifies and gives proper QoS settings for the virtual desktop applications. The one touch QoS allows configuring and managing the Citrix VDI traffic priority and services.

A maximum of five ports can be configured for the Citrix VDI (4 TCP and 1 UDP).

Traffic type prioritization are based on the source or destination and TCP or UDP ports 16501, 2596, 2597, 2598, 2599 and user configured ports for Citrix environment. Traffic type prioritization can also be configured for non-Citrix VDI environment.

mDNS Relay

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

As an example Apple's Bonjour architecture implements the following three fundamental operations to support zero configuration networking service:

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

The Aruba AirGroup feature provides optimization that limits the unnecessary flooding of Bonjour traffic to improve Wifi performance and also allow the Bonjour services to extend across VLANs. The OmniSwitch enhancement supports an mDNS relay function by configuring a GRE tunnel interface between the WLAN controller and the OmniSwitch. The OmniSwitch can intercept and relay the mDNS frames from the wired devices advertising a service using Bonjour messages to the WLAN controller thus preventing flooding of the mDNS frames.

Note: mDNS relay is only supported for wirless clients. Wired clients are not supported.

Bring Your Own Device (BYOD)

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

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

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

Security Features

Case Sensitive MAC Address

This enhancement enables the OmniSwitch to send the MAC address of a non-supplicant client in lower case as username and password for authentication to the authentication server. Prior to this enhancement the MAC address could only be sent in uppercase for username and password.

HIC HTTPS Web Redirection

This feature enhancement provides the ability of HIC redirection when the client browser specifies a HTTPS URL on port 443. When a device is put in a HIC state, any web session will be redirected to the HIC web agent via HTTPS URL specified in the client's browser.

Prior to this enhancement HIC redirection only worked when the client browser specified a HTTP URL on port 80.

VRF

IP Helper per-VLAN and per-VRF

The per-VLAN IP helper service can now be configured on both the default VRF and non-default VRF. Prior to this enhancement the per-VLAN functionality was limited to the default VRF only. The per-VLAN paramaters such as forward delay, maximum hops, relay agent information and PXE support are all VRF-aware.

Additional Features

Boot Interruption Sequence

Prior to this enhancement pressing any key during the 2 second switch bootup interrupt window would interrupt the boot sequence causing the switch to stop at the uboot prompt. Additionally, once a key was pressed there was no way to cancel the switch bootup interrupt.

In this new implementation the boot sequence for the switch can only be interrupted by pressing the 's' key during the 2 second switch bootup interrupt window.

Once the 's' key is pressed the boot sequence will be interrupted. Another prompt will be displayed allowing the user to hit any other key to cancel the bootup interruption and continue booting the switch if desired. If no key is pressed to cancel the bootup interruption the switch will stop at the uboot prompt.

Note: This feature requires a uboot/miniboot upgrade to version 6.4.6.10.R01. Contact customer support for availability.

802.1q Capability on NNI ports

This feature enhancement allows the creation of untagged VLANs and 802.1q VLANs on a NNI port. This will allow configuring 802.1q services, QinQ service and untagged services using the same uplink NNI port. This will also allow using an untagged management VLAN to manage the switch through the NNI ports. The standard VLAN configuration (both untagged and 802.1q tagged association) is now allowed on an NNI interface binded with a service VLAN. The binding of service VLAN to NNI interface is now allowed when the interface (physical or linkagg) is already tagged with a standard VLAN.

802.1q VLAN tagging to an NNI interface will not be allowed if the interface is set with TPID other than 0x8100. Any modification with respect to TPID will not be allowed if the NNI interface is 802.1q tagged.

L2 Control Protocol Hardware Tunneling

This feature enhances the L2 control protocol tunneling feature introduced in 6.4.5.R02 by providing the ability to tunnel all the control frames in hardware for better performance.

Note : Hardware tunneling is supported only if the action (peer/tunnel/drop) is set for all the packet types pertaining to the tunnel grouping.

SNMP Traps

The following table provides a list of AOS Release 6.4.4.R01 SNMP traps managed by the switch.

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.
13	vrrpTrapNewMaster	all	The SNMP agent has transferred from the backup state to the master state.
14	vrrpTrapAuthFailure	-	This trap is not supported.
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.
18	bgpEstablished	all	The BGP routing protocol has entered the established state.
19	bgpBackwardTransition	all	This trap is generated when the BGP router port has moved from a more active to a less active state.
20	esmDrvTrapDropsLink	all	This trap is sent when the Ethernet code drops the link because of excessive errors.
21	pimNeighborLoss	all	Signifies the loss of adjacency with a neighbor device. This trap is generated when the neighbor time expires and the switch has no other neighbors on the same interface with a lower IP

No.	Trap Name	Platforms	Description
			address than itself.
22	dvmrpNeighborLoss	all	A 2-way adjacency relationship with a neighbor has been lost. This trap is generated when the neighbor state changes from “active” to “one-way,” “ignoring” or “down.” The trap is sent only when the switch has no other neighbors on the same interface with a lower IP address than itself.
23	dvmrpNeighborNotPruning	all	A non-pruning neighbor has been detected in an implementation-dependent manner. This trap is generated at most once per generation ID of the neighbor. For example, it should be generated at the time a neighbor is first heard from if the prune bit is not set. It should also be generated if the local system has the ability to tell that a neighbor which sets the prune bit is not pruning any branches over an extended period of time. The trap should be generated if the router has no other neighbors on the same interface with a lower IP address than itself.
24	risingAlarm	all	An Ethernet statistical variable has exceeded its rising threshold. The variable’s rising threshold and whether it will issue an SNMP trap for this condition are configured 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	-	Unsupported.
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	-	
33	slbTrapOperStatus	-	A change occurred in the operational status of the server load balancing entity.
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.

No.	Trap Name	Platforms	Description
36	trapAbsorptionTrap	all	The absorption trap is sent when a trap has been absorbed at least once.
37	alaStackMgrDuplicateSlotTrap	6400 6850 6850E 6855	Two or more slots claim to have the same slot number.
38	alaStackMgrNeighborChangeTrap	6400 6850 6850E 6855	Indicates whether or not the stack is in loop.
39	alaStackMgrRoleChangeTrap	6400 6850 6850E 6855	Indicates that a new primary or secondary stack is elected.
40	lpsViolationTrap	all	A Learned Port Security (LPS) violation has occurred.
41	alaDoSTrap	all	Indicates that the sending agent has received a Denial of Service (DoS) attack.
42	gmBindRuleViolation	all	Occurs whenever a binding rule which has been configured gets violated.
43	unused	-	-
44	unused	-	-
45	unused	-	-
46	unused	-	-
47	pethPsePortOnOff	-	Indicates if power inline port is or is not delivering power to the a power inline device.
48	pethPsePortPowerMaintenanceStatus	-	Indicates the status of the power maintenance signature for inline power.
49	pethMainPowerUsageOn	-	Indicates that the power inline usage is above the threshold.
50	pethMainPowerUsageOff	-	Indicates that the power inline usage is below the threshold.
51	ospfNbrStateChange	all	Indicates a state change of the neighbor relationship.
52	ospfVirtNbrStateChange	all	Indicates a state change of the virtual neighbor relationship.
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	6400 6850 6850E 6855	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	6400 6850 6850E 6855	The element identified by alaStackMgrSlotNINumber will enter the pass through mode because its operational slot was cleared with immediate effect.

No.	Trap Name	Platforms	Description
56	alaStackMgrOutOfSlotsTrap	6400 6850 6850E 6855	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	6400 6850 6850E 6855	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	6400 6850 6850E 6855	There are no pass through slots avail able to be assigned to an element that is supposed to enter the pass through mode.
59	gmHwVlanRuleTableOverloadAlert	all	An overload trap occurs whenever a new entry to the hardware VLAN rule table gets dropped due to the overload of the table.
60	lnkaggAggUp	all	Indicates the link aggregate is active. This trap is sent when any one port of the link aggregate 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	-	A File Written Trap is sent when the amount of data requested by the user has been written by the port monitoring instance.
67	alaVrrp3TrapProtoError	all	Indicates that a TTL, checksum, or version error was encountered upon receipt of a VRRP advertisement.
68	alaVrrp3TrapNewMaster	all	The SNMP agent has transferred from the backup state to the master state.
69	gmHwMixModeSubnetRuleTableOverloadAlert	all	A subnet overload trap occurs in mixed mode whenever a new entry to the HW subnet rule table gets dropped 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.
73	vRtrIsisDatabaseOverload	all	This notification is generated when the system

No.	Trap Name	Platforms	Description
			enters or leaves the Overload state.
74	vRtrIsisManualAddressDrops	all	Generated when one of the manual area addresses assigned to this system is ignored when computing routes.
75	vRtrIsisCorruptedLSPDetected	all	This notification is generated when an LSP that was stored in memory has become corrupted.
76	vRtrIsisMaxSeqExceedAttempt	all	Generated when the sequence number on an LSP wraps the 32 bit sequence counter
77	vRtrIsisIDLenMismatch	all	Need Desc. A notification sent when a PDU is received with a different value of the System ID Length.
78	vRtrIsisMaxAreaAddrsMismatch	all	A notification sent when a PDU is received with a different value of the Maximum Area Addresses.
79	vRtrIsisOwnLSPPurge	all	A notification sent when a PDU is received with an OmniSwitch systemID and zero age
80	vRtrIsisSequenceNumberSkip	all	When we recieve an LSP is received without a System ID and different contents.
81	vRtrIsisAutTypeFail	all	A notification sent when a PDU is received with the wrong authentication type field.
82	vRtrIsisAuthFail	all	A notification sent when a PDU is received with an incorrent authentication information field.
83	vRtrIsisVersionSkew	all	A notification sent when a a Hello PDU is received from an IS running a different version of the protocol.
84	vRtrIsisAreaMismatch	all	A notification sent when a Hello PDU is received from an IS which does not share any area address.
85	vRtrIsisRejectedAdjacency	all	A notification sent when a Hello PDU is received from an IS, but does not establish an adjacency due to a lack of resources.
86	vRtrIsisLSPTooLargeToPropagate	all	A notification sent when an attempt to propagate an LSP which is larger than the dataLinkBlockSize for a circuit.
87	vRtrIsisOrigLSPBufSizeMismatch	all	A notification sent when a Level 1 LSP or Level 2 LSP is received which is larger than the local value for the originating L1LSP BufferSize or originating L2LSPBufferSize respectively. Also when a Level 1 LSP or Level2 LSP is received containing the originating LSPBufferSize option and the value in the PDU option field does not match the local value for originating L1LSP BufferSize or originatingL2LSP BufferSize respectively.
88	vRtrIsisProtoSuppMismatch	all	A notification sent when a non-pseudonode segment 0 LSP is received that has no matching protocols supported.
89	vRtrIsisAdjacencyChange	all	A notification sent when an adjacency changes state, entering or leaving state up. The first 6 bytes of the vRtrIsisTrapLSPID are the SystemID of the adjacent IS.

No.	Trap Name	Platforms	Description
90	vRtrIsisCircIdExhausted	all	A notification sent when ISIS cannot be started on a LAN interface because a unique circId could not be assigned due to the exhaustion of the circId space.
91	vRtrIsisAdjRestartStatusChange	all	A notification sent when an adjancency's graceful restart status changes.
92	dot1agCfmFaultAlarm	all	A MEP has lost contact with one or more MEPs. A notification (fault alarm) is sent to the management entity with the OID of the MEP that has detected the fault.
93	Unused	all	-
94	lldpRemTablesChange	all	A lldpRemTablesChange notification is sent when the value of lldpStatsRemTableLastChangeTime changes.
95	chassisTrapsPossibleDuplicateMac	6400 6850 6850E 6855	The old PRIMARY element cannot be detected in the stack. There is a possiblity of a duplicate MAC address in the network
96	unused	all	-
97	alaPimInvalidRegister	all	An alaPimInvalidRegister notification signifies that an invalid PIM Register message was received by this device
98	alaPimInvalidJoinPrune	all	A alaPimInvalidJoinPrune notification signifies that an invalid PIM Join/Prune message was received by this device.
99	alaPimRPMappingChange	all	An alaPimRPMappingChange notification signifies a change to the active RP mapping on this device.
100	alaPimInterfaceElection	all	An alaPimInterfaceElection notification signifies that a new DR or DR has been elected on a network.
101	lpsLearnTrap	all	Generated when an LPS port learns a bridged MAC.
102	gvrpVlanLimitReachedEvent	all	Generated when the number of vlans learned dynamically by GVRP has reached a configured limit.
103	alaNetSecPortTrapAnomaly	all	Trap for an anomaly detected on a port.
104	alaNetSecPortTrapQuarantine	all	Trap for an anomalous port quarantine.
105	udldStateChange	all	Generated when the state of the UDLD protocol changes.
106	healthMonIpcTrap	all	This trap is sent when IPC Pools exceed usage.
107	bcmHashCollisionTrap	all	-
108	healthMonCpuShutPortTrap	all	This trap is sent when port is shut down because of a CPU spike.
109	arpMaxLimitReached	all	This IP Trap is sent when the hardware table has reached the maximum number of entries supported. The OS6400 will not generate new ARP request for new nexthops.
110	ndpMaxLimitReached	all	This IPv6 Trap is sent when the hardware table has reached the maximum number of entries supported. The OS6400 will not generate new

No.	Trap Name	Platforms	Description
			ARP request for new nexthops.
111	ripRouteMaxLimitReached	all	This trap is sent when the RIP database reaches the supported maximum number of entries. When the maximum number is reached, RIP discards any new updates.
112	ripngRouteMaxLimitReached	all	This trap is sent when the RIPng database reaches the supported maximum number of entries. When the maximum number is reached, RIPng discards any new updates.
113	aaaHicServerTrap	all	This trap is sent when the HIC server is down.
114	alaErpRingStateChanged	all	This trap is sent when the ERP Ring State has changed from “Idle” to “Protection”.
115	alaErpRingMultipleRpl	all	This trap is sent when multiple RPLs are detected in the Ring.
116	alaErpRingRemoved	all	This trap is sent when the Ring is removed dynamically.
117	e2eGvrpVlanMatch	all	This trap is sent when GVRP recieves a registration for a VLAN that is configured for End-to-End Flow Control.
118	e2eStackTopoChange	all	This trap is sent when the stack topology changes.
119	dot3OamThresholdEvent	all	This trap is sent when a local or remote threshold crossing event is detected. A local threshold crossing event is detected by the local entity, while a remote threshold crossing event is detected by the reception of an Ethernet OAM Event Notification OAMPDU that indicates a threshold event.
120	dot3OamNonThresholdEvent	all	This trap is sent when a local or remote non-threshold crossing event is detected. A local event is detected by the local entity, while a remote event is detected by the reception of an Ethernet OAM Event Notification OAMPDU that indicates a non-threshold crossing event.
121	alaDot3OamThresholdEventClear	all	This trap is sent when is sent when a local or remote threshold 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	ntpMaxAssociation	all	This trap is generated when the maximum number of peer and client associations configured for the switch is exceeded.
124	alaLicenseExpired	9000E	This trap is sent when the value of aluLicenseTimeRemaining becomes 0 (zero) for a demo licensed application. This notification is

No.	Trap Name	Platforms	Description
			applicable only for temporary licenses. This trap can be utilized by an NMS to inform user about an application license expiration.
125	vRtrLdpInstanceStateChange	all	This trap is sent when the LDP module changes state either administratively or operationally.
126	vRtrLdpGroupIdMismatch	all	This trap is sent when there is a mismatch of local and remote group IDs.
127	mplsXCup	9000E	This trap is generated when one of the configured cross-connect entries is about to leave the down state and transition into some other state (but not into the “Not Present” state).
128	mplsXCdown	9000E	This trap is sent when one of the configured cross-connect entries is about to enter the down state from some other state (but not from the “Not Present” state).
129	vRtrMplsStateChange	9000E	This trap is sent when the MPLS module changes state.
130	vRtrMplsIfStateChange	9000E	This trap is sent when is generated when the MPLS interface changes state.
131	vRtrMplsLspUp	9000E	This trap is sent when an LSP transitions to the 'inService' state from any other state.
132	vRtrMplsLspDown	9000E	This trap is sent when an LSP transitions out of 'inService' state to any other state.
133	svcStatusChanged	9000E	This trap is sent when there is a change in the administrative or operating status of a service.
134	sapStatusChanged	9000E	This trap is sent when there is a change in the administrative or operating status of an SAP.
135	sdpBindStatusChanged	9000E	This trap is sent when there is a change in the administrative or operating status of an SDP Binding.
136	sdpStatusChanged	9000E	This trap is sent when there is a change in the administrative or operating status of an SDP.
137	sapPortStateChangeProcessed	9000E	This trap is sent when the agent has finished processing an access port state change event, and that the operating status of all the affected SAP's has been updated accordingly.
138	sdpBindSdpStateChangeProcessed	9000E	This trap is sent when the agent has finished processing an SDP state change event, and that the operating status of all the affected SDP Bindings has been updated accordingly.
139	unused	-	-
140	unused	-	-
141	unused	-	-

No.	Trap Name	Platforms	Description
142	ddmTemperatureThresholdViolated	all	This trap is sent when an SFP/ XFP/SFP+ temperature has crossed any threshold or reverted from previous threshold violation for a port represented by ifIndex. It also provides the current realtime value of SFP/ XFP/SFP+ temperature.
143	ddmVoltageThresholdViolated	all	This trap is sent when SFP/XFP/ SFP+ supply voltage has crossed any threshold or reverted from previous threshold violation for a port represented by ifIndex. It also provides the current realtime value of SFP/XFP/SFP+ supply voltage.
144	ddmCurrentThresholdViolated	all	This trap is sent when if an SFP/ XFP/SFP+ Tx bias current has crossed any threshold or reverted from previous threshold violation for a port represented by ifIndex. It also provides the current realtime value of SFP/XFP/SFP+ Tx bias current.
145	ddmTxPowerThresholdViolated	all	This trap is sent when an SFP/ XFP/SFP+ Tx output power has crossed any threshold or reverted from previous threshold violation for a port represented by ifIndex. It also provides the current realtime value of SFP/XFP/SFP+ Tx output power.
146	ddmRxPowerThresholdViolated	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 realtime value of SFP/XFP/SFP+ Rx optical power.
147	halHashCollisionTrap	all	-
148	alaLbdStateChangeToShutdown	all	This trap is sent when the port state changes to “shutdown”.
149	alaLbdStateChangeForClearViolationA	all	This trap is sent when the port state changes from “shutdown” due “to clear-violation-all”.
150	alaLbdStateChangeForAutoRecovery	all	This trap is sent when the port state changes from shutdown due to auto-recovery mechanism
151	pimBsrElectedBSRLostElection	all	This trap is sent when the current E-BSR loses an election to a new Candidate-BSR.
152	pimBsrCandidateBSRWinElection	all	This trap is sent when a C-BSR wins a BSR Election.
153	alaErpRingPortStatusChanged	all	This trap is sent whenever the ring port status changes.
154	lnkaggPortReserve	all	This trap is sent when given port of the link aggregation goes to reserved state.
155	esmViolationRecoveryTimeout	all	This trap is sent when a user port is re-enabled after an esm viola-tion recovery timeout.

No.	Trap Name	Platforms	Description
156	alaMvrpVlanLimitReachedEvent	all	This trap is sent when the num-ber of VLANs learned dynami-cally by MVRP reaches the configured limit.
157	alaMvrpE2eVlanConflict	all	This trap is sent when MVRP receives a registration for a VLAN that is configured for End To End Flow Control.
158	alaDhcpSrvLeaseUtilizationThreshold	all	This trap is sent when the lease utilization on a subnet exceeds or falls below the configured threshold value.
159	alaDhcpClientAddressAddTrap	all	This trap is sent when a new IP address is assigned to DHCP Cli-ent interface.
160	alaDhcpClientAddressExpiryTrap	all	This trap is sent when the lease time expires or when the DHCP client is not able to renew/rebind an IP address
161	alaDhcpClientAddressModifyTrap	all	This trap is sent when the DHCP client is unable to obtain the existing IP address and a new IP address is assigned to the DHCP client.
162	alaDyingGaspTrap/ esmDrvTrapDropsLink.3	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	Reserved40	-	-
167	Reserved41	-	-
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		-
171	aaaHicServerChangeTrap	all	This trap is sent when the active HIC server is changed from.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.

No.	Trap Name	Platforms	Description
174	alaStackMgrIncompatibleModeTrap	all	-
175	alaEsmDBChange	all	-
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	stpLoopGuardError	all	This trap is sent by a bridge when a port enters the Loop inconsistent state (ERR state).
179	stpLoopGuardRecovery	all	This trap is sent by a bridge when a port leaves the Loop inconsistent state (ERR state).
180	alaTestOamGroupTxDoneTrap	all	This trap is sent from the Generator DUT, once the test-duration for the Test OAM Group has expired on it. Once the test-duration has expired, the Generator DUT sends the trap after some time interval (around 5 to 10 seconds).
181	alaTestOamGroupRxReadyTrap	all	This trap is sent once the DUT with Analyzer or Loopback Role is ready to receive the test traffic. Once this trap is received, the Generator is activated for generating the test traffic for the Test OAM Group.
182	alaTestOamGroupAbortTrap	all	This trap is sent from the DUT if the Test is aborted for the Test OAM Group during takeover or if any of the NIs go down
183	alaDhcpBindingDuplicateEntry	all	This trap is sent to in response to MAC Movement in the DHCP-Binding Table, MAC Address, VLAN, Previous ifIndex, Current ifIndex.
184	esmStormThresholdViolationStatus	all	This trap is sent when a User Port receives ingress traffic above the configured value.
185	Reserved42	-	-
186	Reserved43	-	-
187	Reserved44	-	-
188	poePowerBudgetChange	all	This trap is sent when any further temperature increase will cause POE power budget rampdown.
189	alaDBChange	all	TBD
190	alaStackMgrIncompatibleLicenseTrap	all	This trap is snt when the license information for a slot is not the same as the primary element license information

No.	Trap Name	Platforms	Description
191	chassisTrapsLowFlashSpace	all	This trap is sent when the free flash space falls below the set minimum level.
192	aaaAuthenticationFalureTrap	all	This trap is sent when user authientication fails
193	alaKerberosReqTimeoutTrap	all	TBD
194	alaKerberosInactivityTimerExpiryTrap	all	TBD
195	alaKerberosRateLimitExceed	all	TBD
196	unpMcLagMacIgnored	OS9000E	This trap is sent when a MAC/User is dropped because the VLAN does not exist or UNP is not enabled on the MCLAG.
197	unpMcLagConfigInconsistency	OS9000E	This trap is sent when a configuration becomes “Out of Sync".
198	Reserved45	-	-
199	Reserved46	-	-
200	Reserved47	-	-
201	Reserved48	-	-
202	Reserved49	-	-
203	Reserved50	-	-
204	multiChassisIpcVlanUp	OS9000E	Indicates the operational status for the multi-chassis communication VLAN is Up.
205	multiChassisIpcVlanDown	OS9000E	Indicates the operational status for the multi-chassis communication VLAN is Down.
206	multiChassisMisconfigurationFailure	OS9000E	This trap is sent when there is a multi-chassis misconfiguration possibly due to inconsistent Chassis ID, Hello-Interval or IPC VLAN.
207	multiChassisHelloIntervalConsisFail		This trap is sent when there is an inconsistency between the local and peer hello interval.
208	multiChassisStpModeConsisFailure	OS9000E	This trap is sent when there is an inconsistency between local and peer spanning tree path cost mode.
209	multiChassisStpPathCostModeConsisFa	OS9000E	This trap is sent when ther is an STP path cost mode consistency falure.
210	multiChassisVflinkStatusConsisFailure	OS9000E	This trap is sent when there is an MCM Virtual Fabric Link status consistency falure.
211	multiChassisStpBlockingStatus	OS9000E	This trap is sent when the STP status for some VLANs on the Virtual Fabric Link is in a blocking state.
212	multiChassisLoopDetected	OS9000E	This trap is sent when a loop is detected over the multi-chassis aggregates.

No.	Trap Name	Platforms	Description
213	multiChassisHelloTimeout	OS9000E	This trap is sent when the Hellow Timer expires
214	multiChassisVflinkDown	OS9000E	This trap is sent when the Virtual Fabric Link goes down
215	multiChassisVFLMemberJoinFailure	OS9000E	This trap is sent when a port configured as a virtual fabric member is unable to join the virtual fabric link
216	multiChassisGroupConsisFailure	OS9000E	This trap is sent when there is an inconsistency between local and peer chassis group.
217	multiChassisTypeConsisFailure	OS9000E	This trap is sent when there is an inconsistency between local and peer chassis type.
218	alaSIPSnoopingACLPreemptedBySOSCall	all	This trap is sent when a SIP snooping RTP/RTCP ACL entry is preempted by an SOS call.
219	alaSIPSnoopingRTCPOverThreshold	all	This trap is sent when one or more RTCP parameters exceeds the threshold limit.
220	alaSIPSnoopingRTCPPktsLost	all	This trap is sent when RTCP packets are lost due to rate limiting.
221	alaSIPSnoopingSignallingLost	all	This trap is sent when when SIP signalling messages are lost due to rate limiting.
222	chassisTrapNiBPSLessAllocatedSytemPower	OS6850E	This trap is sent when insufficient system power is provided by the BPS.
223	chassisTrapsBPSStateChange	OS6850E	This trap is sent when the BPS is inserted or removed.
224	chassisTrapsNiBPSFETStateChange	OS6850E	This trap is sent when the BPS FET state changes.
225	alaSIPSnoopingCallRecordsFileMoved	all	This notification is generated when SIP SNOOPING ended call records flash file is moved from /flash/switch/sip_call_record.txt to /flash/switch/sip_call_record.txt.old. This happens when the configured call record storage limit is reached and possibly at boot-up if /flash/switch/sip_call_record.txt from previous run exists at the first check. Please configure aluSIPSnoopingThresholdNumberOfCalls appropriately to control frequency of file movement and this notification.
226	Reserved51	-	-
227	esmPollBasedLinkScanTrap	all	Started polling based link scanning on the slot. Suspected spurious link change interrupts.
228	multiChassisConsisFailureRecovered	OS9000E	Trap indicating the system has recovered from a multi-chassis inconsistency between the local and peer switches.

No.	Trap Name	Platforms	Description
229	chassisTrapsFabricError	OS9000E	NI was reset due to unrecoverable fabric link errors.
230	alaStackSplitProtectionTrap	OS6850E	This trap is sent when an element of the stack enters into Protection state.
231	alaStackSplitRecoveryTrap	OS6850E	This trap is sent when an element of the stack recovers from the Protection state.

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 in AOS Release 6.4.6.R01:

Feature	Platform	Software Package
OSPF Database Overflow (RFC 1765)	all	base
Authenticated VLANs	OS9000E	base
Legacy VLAN Stacking Mode	all	base
Binding Rules	OS9000E	base

Unsupported CLI Commands

The following CLI commands are not supported in AOS Release 6.4.4.R01:

Software Feature	Unsupported CLI Commands
BGP	ip bgp redist-filter status ip bgp redist-filter ip bgp redist-filter community ip bgp redist-filter local-preference ip bgp redist-filter metric ip bgp redist-filter effect ip bgp redist-filter subnets
BFD	ip bfd-std mode demand
Chassis Mac Server	mac-range local mac-range duplicate-eeprom mac-range allocate-local-only show mac-range status
Chassis Supervision	show fabric
DHCP Relay	ip helper traffic-suppression ip helper dhcp-snooping port traffic-suppression
Ethernet Interfaces	10gig slot [slot] phy-a|phy-b interfaces long interfaces runt interfaces runtsize interfaces flood rate interfaces hybrid preferred-copper interfaces hybrid forced-copper interfaces hybrid forced-fiber
Flow Control	Flow flow wait time interfaces flow
Hot Swap	reload ni [slot] # [no] power ni all
Source IP Management	aaa radius agent preferred ntp src-ip preferred snmp source ip preferred
NTP	no ntp server all
PIM	ip pim cbsr-masklength ip pim static-rp status ip pim rp-candidate ip pim crp-address ip pim crp-expirytime ip pim crp-holdtime ip pim crp-interval ip pim crp-priority ip pim data-timeout ip pim joinprune-interval ip pim source-lifetime ip pim interface mode ip pim interface cbsr-prefernce ip pim interface max-graft-retries

Software Feature	Unsupported CLI Commands
	ip pim interface sr-ttl-threshold show ip pim rp-candidate show ip pim rp-set show ip pim nexthop show ip pim mroute
QoS	qos classify fragments qos flow timeout show policy classify destination interface type show policy classify source interface type
RIP	ip rip redist status ip rip redist ip rip redist metric ip rip redist-filter ip rip redist-filter effect ip rip redist-filter metric ip rip redist-filter route-tag ip rip redist-filter redist-control
System	install show microcode history
VLANs	vlan router mac multiple enable|disable vlan binding mac-port-protocol vlan binding mac-ip vlan binding ip-port show vlan ipmvlan port-binding
VRF	ip service http ip service all
Tunneling L2 Protocols	ethernet-service uni-profile P l2-protocol [STP | GVRP]peer

Open Problem Reports and Feature Exceptions in Release 6.4.6.R01

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.

LAYER 2

Autoneg

PR	Description	Workaround
186066	When a combo fiber port on an OmniSwitch 6850E (with auto-negotiation disabled) is connected to any other OmniSwitch which also has auto-negotiation disabled, the port does not come up even after reloading the OmniSwitch 6850E.	Disable auto negotiation for both fiber and copper combo ports instead of just the fiber port.

Multicast

PR	Description	Workaround
187957	Mulitcast source entries are missing on receiver side after admin down of primary member port of a linkagg. The issue is observed only if the linkagg member ports are on different NIs and the admin down of the primary port is done which is closer to the multicast source. In a cable fault scenario (Physical cable pull) issue is not seen.	Disable and re-enable the linkagg.

QoS

QoS

PR	Description	Workaround
186114	Traffic gets dropped when QoS port ingress bandwidth is configured during run-time after policy rule for UNP profile .	There is no known workaround at this time.

SIP

PR	Description	Workaround
177082/184466	DSCP marking based on local SIP QoS rule is not carried on egress packets towards EDGE endpoint when call server reachability (uplink port) and edge port is on different NI. Also statistics are not updated when endpoints are	Configure the edge port as part of Linkagg.

	on different NIs.	
177063	SIP traffic classification based on source VLAN is not classified as expected, if the UDP SIP packet is fragmented and the call server or the endpoints are on a different NI.	There is no known workaround at this time.

UNP

Rate Limiting

PR	Description	Workaround
186124	Rate-limiting granularity varies on a port where the rate-limiting configuration is present both in UNP profile and in QOS policy list configuration.	Use UNP ingress bandwidth configuration or QoS rate limiting policy list rule but not both.

Stacking

PR	Description	Workaround
187265	In a stack with more than 4 switches with Stack Split Protection enabled and no SSP LAG member port on primary (NI-1) and secondary NI(NI-2). After the event of a stack split and stack recovery between NI2 and NI3, when a subsequent takeover is issued, the LAG member port present in NI3 does not join the SSP LAG.	There is no known workaround at this time.

System

General

PR	Description	Workaround
186093	DDM display may show receive value as being higher than transmit value even when the SFP is connected back to back.	This is an expected behavior. There may be a variance between actual and reported values for both the transmit and receive side.
187711	When an OmniSwitch 6855 is synched between working and certified directories, the USB flash drive is not detected when ‘usb enable’ command is issued during USB hot swap.	Disable USB on the switch using the command ‘usb disable’. Insert flash drive and then enable the USB by using the command ‘usb enable’.
185994	When OmniSwitch 6850Es are connected with dual speed SFP on combo ports back to back and the port speed is configured to 100mbps. After saving the configuration and rebooting the port speed returns to 1-Gig.	There is no known workaround at this time.

Hot Swap / Redundancy

Feature Exceptions

CMM and Power Redundancy Feature Exceptions for OmniSwitch

- Manual invocation of failover (by user command or Primary pull) should only be done during times 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.
- Hot standby redundancy or failover to a secondary module without significant loss of traffic is only supported if all the remaining units in the stack are 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 configuration, different images, etc.). In this case, upon failover, all the NIs will reset and might go to "down" state, and to recover, need to power down the switch and power it back up.
- Primary and Redundant power supplies must be of the same type. For example, having a primary 510W power supply with a redundant 360W power supply is not supported.

Hot Swap Feature Exceptions for OmniSwitch 9000E

- Hot swap of NIs needs to be preceded by the removal of all cables connected to the NI.
- Hot swap of unlike modules is not supported.
- The **reload ni** command is not supported. Please use **no power ni**/**power ni** as an alternative.
- All insertions of NI modules cannot be followed by another hot swap activity until the OK2 LED on the inserted NI blinks green.

Hot Swap Feature Exceptions for OmniSwitch 6850E/6855

- 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 loop back has to be broken. Full redundancy is not guaranteed until the loop back is restored.
- Hot swap of unlike chassis is not supported.

Hot Swap Time Limitations for OmniSwitch

- All removals of NI modules must have a 30 seconds interval before initiating another hot swap activity.
- All insertions of NI modules must have a 3 minutes interval before initiating another hot swap activity.
- All hot swaps of CMM modules must have a 10 minutes interval before initiating another hot swap, reload or takeover activity.
- All takeovers must have a 10 minutes interval before following with another hot swap, reload or takeover activity.

- All insertions 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.

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	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484

Email: esd.support@alcatel-lucent.com

Web: service.esd.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 6.4.6.R01 Upgrade Instructions

OmniSwitch Upgrade Overview

This section documents the 6.4.6.R01 upgrade requirements for the following OmniSwitch models:

- OmniSwitch 6850E
- OmniSwitch 6850E with OmniSwitch BPS
- OmniSwitch 6855
- OmniSwitch 9000E

Prerequisites

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

- Read and understand the entire upgrade procedure before performing any steps.
- The person performing the upgrade must:
  - Be the responsible party for maintaining the switch’s configuration.
  - Be aware of any issues that may arise from a network outage caused by improperly loading this code.
  - Understand that the switch must be rebooted and network users will be affected by this procedure.
  - Have a working knowledge of the switch to configure it to accept an FTP connection through the Network Interface (NI) Ethernet port.
- Read the Release Notes prior to performing any upgrade for information specific to this release.
- All FTP transfers MUST be done in binary mode.

WARNING: Do not proceed until all the above prerequisites have been met and understood. Any deviation from these upgrade procedures could result in the malfunctioning of the switch. All steps in these procedures should be reviewed before beginning.

OmniSwitch Upgrade Requirements

These tables list the required Uboot/Miniboot, FPGA, and AOS combinations for upgrading an OmniSwitch. The Uboot/Miniboot versions for the associated AOS Release must at least be the miminum versions listed below to support AOS 6.4.6.R01.

NOTE: In most cases an FPGA/CPLD or miniboot/uboot upgrade is not required when upgrading to 6.4.6.R01. Please review the following table carefully to determine upgrade requirements.

NOTE: These tables list the MINIMUM Uboot/Miniboot and FPGA required to upgrade to 6.4.6.R01. Downgrading from a more recent version is not required or supported.

Minimum Version Requirements to Upgrade to AOS 6.4.6.R01

	AOS	Uboot	Miniboot	FPGA Version
OmniSwitch 6850E[1]	6.4.6.125.R01 GA	6.4.5.398.R02	6.4.5.398.R02	OS6850E-C24/C48/P24/P48 (v10 or v11) OS6850E-U24X (v7or v8)
OmniSwitch 6850E with OS-BPS	6.4.6.125.R01 GA	6.4.5.398.R02	6.4.5.398.R02	OS6850E-C24/P24/C48/P48(v17) OS6850E-U24X (not supported with OS-BPS)
OmniSwitch 6855 (except P14)	6.4.6.125.R01 GA	6.4.3.479.R01	6.4.3.479.R01	v2.2
OmniSwitch 6855-P14	6.4.6.125.R01 GA	6.4.4.5.R02	6.4.4.5.R02	v1.4
OmniSwitch 9000E **(New Flash Component)**	6.4.6.125.R01 GA	6.4.4.506.R01	6.4.4.506.R01	Major Revision: 2 Minor Revision: 25 (displays as 0x19)
OmniSwitch 9000E **(Previous Flash Component)**	6.4.6.125.R01 GA	6.4.3.479.R01	6.4.3.479.R01	Major Revision: 2 Minor Revision: 25 (displays as 0x19)

1. Factory CPLD default version for OS6850E-C24/P24/C48/P48 is version 17. Factory CPLD default version for OS6850E-U24X is version 12. Customers using FPGA/CPLD version 10 or 11 (for OS6850E-C24/P24/C48/P48) and version 7 or 8 (for OS6850E-U24X) need not upgrade FPGA/CPLD version when upgrading to AOS 6.4.6.RO1.

Note: A minimum uboot/miniboot version is required to support the autoboot interupt feature in 6.4.6 R01, contact customer support for more details.

Version Requirements – Upgrading to AOS Release 6.4.6.R01

AOS 6.4.6.R01 Upgrade Files			
	AOS	**Uboot/Miniboot**	**FPGA**
OmniSwitch 6850E	K2os.img, Kadvrout.img Kbase.img, Kencrypt.img, Keni.img, Ksecu.img	kuboot.bin kminiboot.uboot	K2Efpga.upgrade_kit
OmniSwitch 6855	K2Ios.img, Kadvrout.img, Kbase.img, Kencrypt.img, Keni.img, Ksecu.img	kuboot.bin kminiboot.uboot	N/A
OmniSwitch 9000E	Jadvrout.img, Jbase.img, Jencrypt.img Jeni.img, Jos.img, Jsecu.img	miniboot.uboot u-boot.bin	Jfpga.upgrade_kit

Upgrading to AOS 6.4.6.R01

Upgrading OmnSwitch to 6.4.6.R01 consists of the following steps. The steps must be performed in order. Observe the following prerequisites before performing the steps as described below:

- In most cases upgrading the FPGA/CPLD is not required when upgrading to AOS Release 6.4.6.R01. If an FPGA/CPLD upgrade is required, two reboots of the switch or stack being upgraded will be required. The first reboot will happen automatically after upgrading the FPGA/CPLD. A second reboot is required after upgrading the Uboot/Miniboot and AOS.
- If a unit has been received from the factory with a newer FPGA/CPLD version it is not required to upgrade the existing units to the newer version. Having a mix of FPGA/CPLD in the same stack or chassis is supported.
- An OmniSwitch 6850E-U24X with CPLD version 8 will require a hard reboot (the switch must be physically powered down and back up) for any CPLD upgrade to take affect.
  NOTE: That an OmniSwitch 6850E-U24X with CPLD version 7 or version 8 does not require a CPLD upgrade when upgrading to 6.4.6.R01.
- CPLD must be upgraded to version 17 for OmniSwitch 6850E with OS-BPS models.
- For OS6850E-C24/P24/C48/P48 models without OS-BPS models, CPLD upgrade to version 17 is not mandatory.
- Refer to the Version Requirements table to determine the proper code versions.
- Download the appropriate AOS images, Uboot/Miniboot, and FPGA files from the Service & Support website.

Summary of Upgrade Steps

1. Upgrade the FPGA/CPLD, if required. (switch/stack automatically reboots)
2. Upgrade the Uboot/Miniboot (If required) and AOS images (Reboot required)
3. Verify the upgrade and remove the upgrade uboot/miniboot and CPLD files from the switch.

Upgrading - Step 1. Upgrade the FPGA/CPLD (If required)

Follow the steps below to FTP the FPGA/CPLD upgrade kit to the switch and perform the FPGA/CPLD upgrade. Note the following:

- The CMMs must be certified and synchronized and running from Working directory.
- This procedure will automatically reboot the switch or stack.
- 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.

1. Download and extract the 6.4.6.R01 Upgrade archive from the Service & Support website. The archive will contain the FPGA/CPLD upgrade kit to be used for the upgrade.
2. FTP (Binary) the FPGA/CPLD upgrade kit listed above to the **/flash** directory on the primary CMM.
3. Follow the steps below to upgrade the FPGA/CPLD.

WARNING: During the FPGA/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

Enter the following to begin the FPGA/CPLD upgrade:

```
-> update fpga cmm
```

The switch will upgrade the FPGA/CPLD and reboot.

Stack Procedure

Updating a stack requires all elements of the stack to be upgraded. The FPGA/CPLD upgrade can be completed for all the elements of a stack using the '**all**' parameter as shown below.

Enter the following to begin the FPGA upgrade for all the elements of a stack.

```
-> update fpga ni all
```

The stack will upgrade the FPGA and reboot.

Upgrading - Step 2. Upgrade Uboot/Miniboot and AOS

Follow the steps below to upgrade the Uboot/Miniboot and AOS. This step will upgrade both Uboot/Miniboot and AOS once the switch or stack is rebooted. Note the following:

- The CMMs must be certified and synchronized and running from Working directory.
- This procedure will require a reboot of the switch or stack.
- 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.

1. Download and extract the 6.4.6.R01 Upgrade archive from the Service & Support website. The archive will contain the files to be used for the upgrade.

    - Uboot/Miniboot Files (if required)
    - AOS Files – (required)

2. FTP (Binary) the Uboot/Miniboot files listed above to the **/flash** directory on the primary CMM, if required.

3. FTP (Binary) the image files listed above to the **/flash/working** directory on the primary CMM.

4. 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.

5. Reboot the switch. **This will update both the Uboot/Miniboot and AOS.**

    ```
    -> reload working no rollback-timeout
    ```

6. 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
    ```

Proceed to Verify The Update to verify the upgrade procedure.

Verifying the Update

The following examples show what the code versions should be after upgrading to AOS Release 6.4.6.R01. These names and files will differ based on the type of switch and upgrade requirements.

Verifying the Software Upgrade

To verify that the AOS software was successfully upgraded to 6.4.6.R01, use the **show microcode** command as shown below. The display below shows a successful image file upgrade.

```
-> show microcode

Package      Release         Size     Description
------------+---------------+--------+-----------------------------

Kbase.img    6.4.6.125.R01   15510736 Alcatel-Lucent Base Software
K2os.img     6.4.6.125.R01    2511585 Alcatel-Lucent OS
Keni.img     6.4.6.125.R01    5083931 Alcatel-Lucent NI software
Ksecu.img    6.4.6.125.R01     597382 Alcatel-Lucent Security Management
```

Verifying the U-Boot/Miniboot and FPGA Upgrade

To verify that the FPGA was successfully upgraded on a CMM, use the **show hardware info** command as shown below. These names and files will differ based on the type of switch and upgrade requirements.

```
-> show hardware info
CPU Type                          : Motorola MPC8248,
Flash Manufacturer                : Wintek CF128MB,
Flash size                        : 131203072 bytes (125 MB),
RAM Manufacturer                  : 0x00000000 - Other,
RAM size                          : 536870912 bytes (512 MB),
NVRAM Battery OK ?                : YES,
Uboot Version                     : 6.4.5.398.R02,
Miniboot Version                  : 6.4.5.398.R02,
Product ID Register               : ff
Hardware Revision Register        : 30
CPLD Revision Register            : 12
XFP Module ID                     : 02
```

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:                    OS6850E-24X,
  Description:                   24 G  2 10G,
  Current Switch mode :          OS6850E,
  Saved Switch mode :            OS6850E,
  Part Number:                   902937-90,
  Hardware Revision:             07,
  Serial Number:                 L408029P,
  Manufacture Date:              MAR 15 2011,
  Firmware Version:              ,
  Admin Status:                  POWER ON,
  Operational Status:            UP,
  Power Consumption:             0,
  Power Control Checksum:        0x66b7,
  CPU Model Type   :             Motorola MPC8248,
  MAC Address:                   00:e0:b1:d3:09:01,
  ASIC - Physical 1:             BCM56514_A0,
  FPGA - Physical 1:             0012/00,
  UBOOT Version :                6.4.5.398.R02,
  UBOOT-miniboot Version :       6.4.5.398.R02,
  POE SW Version :               n/a
```

Remove the FPGA and Uboot/Miniboot Upgrade Files

After the switch/stack has been upgraded and verified the upgrade files can be removed from the switch. These names and files will differ based on the type of switch and upgrade requirements.

Issue the following command to remove the upgrade files.

```
-> rm K2Efpga.upgrade_kit
-> rm kuboot.bin
-> rm kminiboot.uboot
```

Appendix B: AOS 6.4.6.R01 Auto-FPGA Upgrade Instructions (OS6850E Only)

OS6850E Auto-FPGA Upgrade Overview

This section documents the Automatic FPGA upgrade procedure on OS6850E models for AOS release 6.4.6.R01. The Automatic FPGA upgrade procedure can be be used on the OS6850E models to reduce the number of reboots to just one when upgrading the FPGA.

Note: The Auto-FPGA upgrade procedure is not supported on OS6850E-U24X units with CPLD v7. Please refer to Appendix A for the alternate upgrade procedure.

Prerequisites

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

- Read and understand the entire upgrade procedure before performing any steps.
- The person performing the upgrade must:
  - Be the responsible party for maintaining the switch's configuration.
  - Be aware of any issues that may arise from a network outage caused by improperly loading this code.
  - Understand that the switch must be rebooted and network users will be affected by this procedure.
  - Have a working knowledge of the switch to configure it to accept an FTP connection through the Network Interface (NI) Ethernet port.
- Read the Release Notes prior to performing any upgrade for information specific to this release.
- All FTP transfers MUST be done in binary mode.

WARNING: Do not proceed until all the above prerequisites have been met and understood. Any deviation from these upgrade procedures could result in the malfunctioning of the switch. All steps in these procedures should be reviewed before beginning.

OS6850E Auto-FGPA Upgrade Requirements

These tables list the required Uboot/Miniboot, FPGA, and AOS combinations for upgrading an OmniSwitch 6850E. The Uboot/Miniboot versions for the associated AOS Release must at least be the miminum versions listed below.

NOTE: In most cases an FPGA/CPLD or miniboot/uboot upgrade is not required when upgrading to 6.4.6.R01. Please review the following table carefully to determine upgrade requirements.

NOTE: These tables list the MINIMUM Uboot/Miniboot and FPGA required to upgrade to 6.4.6.R01. Downgrading from a more recent version is not required or supported.

Minimum Version Requirements to Upgrade to AOS 6.4.6.R01

	AOS	Uboot	Miniboot	FPGA Version
OmniSwitch 6850E[1]	6.4.6.125.R01 GA	6.4.5.398.R02	6.4.5.398.R02	OS6850E-C24/C48/P24/P48 (v10 or v11) OS6850E-U24X (v8)
OmniSwitch 6850E with OS-BPS	6.4.6.125.R01 GA	6.4.5.398.R02	6.4.5.398.R02	OS6850E-C24/P24/C48/P48(v17) OS6850E-U24X (not supported with OS-BPS)

1. Factory CPLD default version for OS6850E-C24/P24/C48/P48 is version 17. Factory CPLD default version for OS6850E-U24X is version 12. Customers using FPGA/CPLD version 10 or 11 (for OS6850E-C24/P24/C48/P48) and version7 or 8 (for OS6850E-U24X) need not upgrade FPGA/CPLD version when upgrading to AOS 6.4.6.RO1.

2. The Auto-FPGA upgrade procedure is not supported on an OS6850E-U24X with CPLD v7. Please refer to Appendix A for the alternate upgrade procedure.

Version Requirements – Upgrading to AOS Release 6.4.6.R01

AOS 6.4.6.R01 Auto-FPGA Upgrade Files

	AOS	Uboot/Miniboot	FPGA	Debug File
OmniSwitch 6850E	K2os.img, Kadvrout.img Kbase.img, Kencrypt.img, Keni.img, Ksecu.img	kuboot.bin kminiboot.uboot	K2Efpga.upgrade_kit	AlcatelDebug.cfg

Auto-FPGA Upgrade to AOS 6.4.6.R01

Upgrading an OS6850E to 6.4.6.R01 consists of the following steps. The steps must be performed in order. Observe the following prerequisites before performing the steps as described below:

- This procedure assumes an FPGA/CPLD upgrade is required. If an FPGA/CPLD upgrade is not required refer to Appendix A for the alternate upgrade procedure.
- An OmniSwitch 6850E-U24X with CPLD version 8 will require a hard reboot (the switch must be physically powered down and back up) for any CPLD upgrade to take affect.
  NOTE: That an OmniSwitch 6850E-U24X with CPLD version 7 or version 8 does not require a CPLD upgrade when upgrading to 6.4.6.R01.
- CPLD must be upgraded to version 17 for OmniSwitch 6850E with OS-BPS models.
- For OS6850E-C24/P24/C48/P48 models without OS-BPS models, CPLD upgrade to version 17 is not mandatory.
- Refer to the Version Requirements table to determine the proper code versions.
- Download the appropriate AOS images, Uboot/Miniboot, FPGA files from the Service & Support website and manualy create the AlcatelDebug.cfg file .

Summary of Upgrade Steps

1. Manually create the AlcatelDebug.cfg file
2. Upgrade the Uboot/Miniboot and AOS images (Reboot required)
3. The OmniSwith automatically upgrades the FPGA/CPLD.
4. Verify the upgrade and remove the upgrade uboot/miniboot and CPLD files from the switch.

Auto-Upgrading - Step 1. Create the AlcatelDebug.cfg file

A file named AlcatelDebug.cfg must be created and FTPd to the /flash/working directory on the switch. This file will be read after the uboot/miniboot and AOS image upgrade to determine which FPGA/CPLD version to use to perform the automatic FGPA/CPLD upgrade.

- The CMMs must be certified and synchronized and running from Working directory after transferring the AlcatelDebug.cfg file to the switch.
- This procedure will require a reboot of the switch or stack.
- 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.

1. Use the editor on the OmniSwitch or any text editor create and FTP the AlcatelDebug.cfg file to the **/flash/working** directory on the switch.
2. Certify and synchronize the CMMs.

Contents of AlcatelDebug.cfg file:

```
debug set auto_update_fpga_copper 17
debug set auto_update_fpga_u24x 12
debug set auto_update_fpga_retry 1
```

Auto-Upgrading - Step 2. Upgrade Uboot/Miniboot and AOS

Follow the steps below to upgrade the Uboot/Miniboot and AOS. This step will upgrade both Uboot/Miniboot and AOS once the switch or stack is rebooted. Note the following:

- The CMMs must be certified and synchronized and running from Working directory.
- This procedure will require a reboot of the switch or stack.
- 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.

1. Download and extract the 6.4.6.R01 Upgrade archive from the Service & Support website. The archive will contain the files to be used for the upgrade.
   - FPGA/CPLD Files
   - Uboot/Miniboot Files (if required)
   - AOS Files – (required)
2. FTP (Binary) the Uboot/Miniboot and FPGA/CPLD files listed above to the **/flash** directory on the primary CMM.
3. FTP (Binary) the image files listed above to the **/flash/working** directory on the primary CMM.
4. 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.

5. Reboot the switch. **This will update both the Uboot/Miniboot and AOS.**

   ```
   -> reload working no rollback-timeout
   ```

Auto-Upgrading - Step 3. Upgrade the FPGA/CPLD

After the switch reboots during the uboot/miniboot and AOS image upgrade it will read the contents of the AlcatelDebug.cfg file to determine the proper FPGA/CPLD upgrade version. The switch/stack will then automatically upgrade the FPGA/CPLD. Once complete enter the following to complete the upgrade:

If you have **a single CMM** enter:

```
      -> copy working certified
```

If you have **redundant CMMs** enter:

```
       -> copy working certified flash-synchro
```

Verifying the Update

The following examples show what the code versions should be after upgrading to AOS Release 6.4.6.R01. These names and files will differ based on the type of switch and upgrade requirements.

Verifying the Software Upgrade

To verify that the AOS software was successfully upgraded to 6.4.6.R01, use the **show microcode** command as shown below. The display below shows a successful image file upgrade.

```
-> show microcode

Package      Release         Size     Description
------------+--------------+--------+------------------------------

Kbase.img    6.4.6.125.R01   15510736 Alcatel-Lucent Base Software
K2os.img     6.4.6.125.R01    2511585 Alcatel-Lucent OS
Keni.img     6.4.6.125.R01    5083931 Alcatel-Lucent NI software
Ksecu.img    6.4.6.125.R01     597382 Alcatel-Lucent Security Management
```

Verifying the U-Boot/Miniboot and FPGA Upgrade

To verify that the FPGA was successfully upgraded on a CMM, use the **show hardware info** command as shown below. These names and files will differ based on the type of switch and upgrade requirements.

```
-> show hardware info
CPU Type                          : Motorola MPC8248,
Flash Manufacturer                : Wintek CF128MB,
Flash size                        : 131203072 bytes (125 MB),
RAM Manufacturer                  : 0x00000000 - Other,
RAM size                          : 536870912 bytes (512 MB),
NVRAM Battery OK ?                : YES,
Uboot Version                     : 6.4.5.398.R02,
Miniboot Version                  : 6.4.5.398.R02,
Product ID Register               : ff
Hardware Revision Register        : 30
CPLD Revision Register            : 12
XFP Module ID                     : 02
```

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:                    OS6850E-24X,
  Description:                   24 G  2 10G,
  Current Switch mode :          OS6850E,
  Saved Switch mode :            OS6850E,
  Part Number:                   902937-90,
  Hardware Revision:             07,
  Serial Number:                 L408029P,
  Manufacture Date:              MAR 15 2011,
  Firmware Version:              ,
  Admin Status:                  POWER ON,
  Operational Status:            UP,
  Power Consumption:             0,
  Power Control Checksum:        0x66b7,
  CPU Model Type   :             Motorola MPC8248,
  MAC Address:                   00:e0:b1:d3:09:01,
  ASIC - Physical 1:             BCM56514_A0,
  FPGA - Physical 1:             0012/00,
  UBOOT Version :                6.4.5.398.R02,
  UBOOT-miniboot Version :       6.4.5.398.R02,
  POE SW Version :               n/a
```

Remove the FPGA and Uboot/Miniboot Upgrade Files

After the switch/stack has been upgraded and verified the upgrade files can be removed from the switch. These names and files will differ based on the type of switch and upgrade requirements.

Issue the following command to remove the upgrade files.

```
-> rm K2Efpga.upgrade_kit
-> rm kuboot.bin
-> rm kminiboot.uboot
-> rm /flash/working/AlcatelDebug.cfg
-> rm /flash/certified/AlcatelDebug.cfg
```

Appendix C: AOS 6.4.6.R01 Downgrade Instructions

OmniSwitch Downgrade Overview

This section documents the downgrade procedure for the following OmniSwitch models:

- OmniSwitch 6850E
- OmniSwitch 6855
- OmniSwitch 9000E

Note: Please verify the code version of a new switch being inserted into an existing stack. In some cases it may be required to downgrade a new switch prior to inserting it into an existing stack that is running an earlier code version.

Prerequisites

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

- Read and understand the entire downgrade procedure before performing any steps.
- The person performing the downgrade must:
  - Be the responsible party for maintaining the switch’s configuration.
  - Be aware of any issues that may arise from a network outage caused by improperly loading this code.
  - Understand that the switch must be rebooted and network users will be affected by this procedure.
  - Have a working knowledge of the switch to configure it to accept an FTP connection through the Network Interface (NI) Ethernet port.
- Read the Release Notes prior to performing any downgrade for information specific to this release.
- All FTP transfers MUST be done in binary mode.

WARNING: Do not proceed until all the above prerequisites have been met and understood. Any deviation from these downgrade procedures could result in the malfunctioning of the switch. All steps in these procedures should be reviewed before beginning.

OmniSwitch Downgrade Requirements

This table lists the Uboot/Miniboot, FPGA, and AOS downgrade files. Downgrading to previous AOS releases from AOS release 6.4.6.R01 may require the FPGA/CPLD or uboot/miniboot to be downgraded. Please refer to the table below, previous release notes, or installed units for the proper versions and download the appropriate files from the Service & Support website.

Version Requirements to Downgrade from AOS 6.4.6				
	AOS	**Uboot**	**Miniboot**	**FPGA Version**
OmniSwitch 6850E[1]	6.4.4.R01	6.4.4.213.R01	6.4.4.213.R01	OS6850E-C24/C48/P24/P48 (v10 or v11) OS6850E-U24X (v8)
OmniSwitch 6855/9000E	6.4.4.R01	No uboot/miniboot or FPGA/CPLD downgrade required.		
OmniSwitch 6850E/6855/9000E	6.4.5.R02	No uboot/miniboot or FPGA/CPLD downgrade required.		

1. Factory CPLD default version for OS6850E-C24/P24/C48/P48 is version 17. Factory CPLD default version for OS6850E-U24X is version 12. Uboot/Miniboot is 6.4.5.398.R02. If downgrading an OS6850E to 6.4.4.R01 the Uboot/Miniboot and FPGA will need to be downgraded to the versions above. If downgrading an OS6805E to AOS release 6.4.5.R02 a uboot/miniboot and FPGA downgrade is not required.

Version Requirements – Downgrading to a previous AOS release

AOS 6.X.X Downgrade Files			
	AOS	**Uboot/Miniboot**	**FPGA**
OmniSwitch 6850E	K2os.img, Kadvrout.img Kbase.img, Kencrypt.img, Keni.img, Ksecu.img	kuboot.bin kminiboot.uboot	K2Efpga.upgrade_kit
OmniSwitch 6855	K2Ios.img, Kadvrout.img, Kbase.img, Kencrypt.img, Keni.img, Ksecu.img	N/A	N/A
OmniSwitch 9000E	Jadvrout.img, Jbase.img, Jencrypt.img Jeni.img, Jos.img, Jsecu.img	N/A	N/A

Downgrading From AOS 6.4.6.R01

Downgrading an OmnSwitch to an earlier AOS release consists of the following steps. The steps must be performed in order. Observe the following prerequisites before performing the steps as described below:

- Downgrading to previous AOS releases from AOS release 6.4.6.R01 may require the FPGA/CPLD or uboot/miniboot to be downgraded. Please refer to the version requirements table, previous version release notes or the existing installed units for the proper versions.
- If an FPGA/CPLD downgrade is required, two reboots of the switch or stack being downgraded will be required. The first reboot will happen automatically after downgrading the FPGA/CPLD. A second reboot is required after downgrading the Uboot/Miniboot and AOS.
- Once the proper versions are confirmed, download the appropriate AOS images, Uboot/Miniboot, and FPGA files from the Service & Support website.

Summary of Downgrade Steps

1. Downgrade the FPGA/CPLD, if required. (switch/stack automatically reboots)
2. Downgrade the Uboot/Miniboot (if required) and AOS images (Reboot required)
3. Verify the downgrade and remove the downgrade uboot/miniboot and CPLD files from the switch.

Downgrading - Step 1. Downgrade the FPGA/CPLD (If required)

Follow the steps below to FTP the FPGA/CPLD downgrade kit to the switch and perform the FPGA/CPLD downgrade. Note the following:

- The CMMs must be certified and synchronized and running from Working directory.
- This procedure will automatically reboot the switch or stack.
- 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.

1. Download and extract the downgrade archive from the Service & Support website. The archive will contain the FPGA/CPLD downgrade kit to be used for the downgrade.
2. FTP (Binary) the FPGA/CPLD downgrade kit listed above to the **/flash** directory on the primary CMM.
3. Follow the steps below to downgrade the FPGA/CPLD.

WARNING: During the FPGA/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

Enter the following to begin the FPGA/CPLD downgrade:

```
-> update fpga cmm
```

The switch will downgrade the FPGA/CPLD and reboot.

Stack Procedure

Downgrading a stack requires all elements of the stack to be downgraded. The FPGA/CPLD downgrade can be completed for all the elements of a stack using the '**all**' parameter as shown below.

Enter the following to begin the FPGA downgrade for all the elements of a stack.

```
-> update fpga ni all
```

The stack will downgrade the FPGA and reboot.

Downgrading - Step 2. Downgrade Uboot/Miniboot and AOS

Follow the steps below to downgrade the Uboot/Miniboot and AOS. This step will downgrade both Uboot/Miniboot and AOS once the switch or stack is rebooted. Note the following:

- The CMMs must be certified and synchronized and running from Working directory.
- This procedure will require a reboot of the switch or stack.
- 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.

1. Download and extract the downgrade archive from the Service & Support website. The archive will contain the files to be used for the downgrade.

    - Uboot/Miniboot Files (if required)
    - AOS Files – (required)

2. FTP (Binary) the Uboot/Miniboot files listed above to the **/flash** directory on the primary CMM, if required.

3. FTP (Binary) the image files listed above to the **/flash/working** directory on the primary CMM.

4. 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 downgraded version.

WARNING: DO NOT INTERRUPT the downgrade process until it is complete. Interruption of the process will result in an unrecoverable failure condition.

5. Reboot the switch. **This will update both the Uboot/Miniboot and AOS.**

    ```
    -> reload working no rollback-timeout
    ```

6. Once the switch reboots, certify the downgrade:

    If you have **a single CMM** enter:

    ```
    -> copy working certified
    ```

    If you have **redundant CMMs** enter:

    ```
    -> copy working certified flash-synchro
    ```

Verifying the Downgrade

The following examples show what the code versions may be after downgrading. These names and files will differ based on the type of switch and downgrade requirements.

Verifying the Software Downgrade

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

```
-> show microcode

Package      Release         Size     Description
------------+---------------+--------+-----------------------------

Kbase.img    6.4.5.402.R02   15510736 Alcatel-Lucent Base Software
K2os.img     6.4.5.402.R02    2511585 Alcatel-Lucent OS
Keni.img     6.4.5.402.R02    5083931 Alcatel-Lucent NI software
Ksecu.img    6.4.5.402.R02     597382 Alcatel-Lucent Security Management
```

Verifying the U-Boot/Miniboot and FPGA Downgrade

To verify that the FPGA was successfully downgraded on a CMM, use the **show hardware info** command as shown below. These names and files will differ based on the type of switch and downgrade requirements.

```
-> show hardware info
CPU Type                          : Motorola MPC8248,
Flash Manufacturer                : Wintek CF128MB,
Flash size                        : 131203072 bytes (125 MB),
RAM Manufacturer                  : 0x00000000 - Other,
RAM size                          : 536870912 bytes (512 MB),
NVRAM Battery OK ?                : YES,
Uboot Version                     : 6.4.5.398.R02,
Miniboot Version                  : 6.4.5.398.R02,
Product ID Register               : ff
Hardware Revision Register        : 30
CPLD Revision Register            : 08
XFP Module ID                     : 02
```

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:                    OS6850E-24X,
  Description:                   24 G  2 10G,
  Current Switch mode :          OS6850E,
  Saved Switch mode :            OS6850E,
  Part Number:                   902937-90,
  Hardware Revision:             07,
  Serial Number:                 L408029P,
  Manufacture Date:              MAR 15 2011,
  Firmware Version:              ,
  Admin Status:                  POWER ON,
  Operational Status:            UP,
  Power Consumption:             0,
  Power Control Checksum:        0x66b7,
  CPU Model Type   :             Motorola MPC8248,
  MAC Address:                   00:e0:b1:d3:09:01,
  ASIC - Physical 1:             BCM56514_A0,
  FPGA - Physical 1:             0008/00,
  UBOOT Version :                6.4.5.398.R02,
  UBOOT-miniboot Version :       6.4.5.398.R02,
  POE SW Version :               n/a
```

Remove the FPGA and Uboot/Miniboot Downgrade Files

After the switch/stack has been downgraded and verified the downgrade files can be removed from the switch. These names and files will differ based on the type of switch and downgrade requirements.

Issue the following command to remove the downgrade files.

```
-> rm K2Efpga.upgrade_kit
-> rm kuboot.bin
-> rm kminiboot.uboot
```

Appendix D: Required Minimum Uboot for Modules with New Flash Component

The modules listed below are being manufactured with a new flash component that requires a minimum Uboot version. The new modules will be shipped with the proper Uboot installed and should not be downgraded when deploying them into an existing network. These modules are fully compatible with all previous AOS Releases in which they were initially supported.

The modules listed below have different uboot/miniboot requirements than modules with the previous flash components. Please review the upgrade instructions prior to upgrading to AOS Release 6.4.6.R01.

Note: If one of the modules listed below is downgraded to an unsupported Uboot version it must be returned to Alcatel-Lucent for repair.

Identifying the New Modules:

1. New 9000 level part number as listed below.
2. Minimum Uboot revision sticker on the module when shipped.

Module Type	Part No.	Minimum Uboot
OS9700E/9702E-CMM	903182-60	6.4.4.506.R01
OS9702E-CMM	903187-90	6.4.4.506.R01
OS9700E-CMM	903182-90	6.4.4.506.R01
OS9800E-CMM	903183-90	6.4.4.506.R01
OS9-GNI-C24E	903184-90	6.4.4.506.R01
OS9-GNI-U24E	903185-90	6.4.4.506.R01
OS9-XNI-U2E	903186-90	6.4.4.506.R01
OS9-XNI-U12E	903188-90	6.4.4.506.R01
OS9-GNI-P24E	903189-90	6.4.4.506.R01

Module Identification Example using CLI

```
-> show ni 1
Module in slot 1
  Model Name:                     OS9700-24E,
  Description:                    C24 10/100/1000,
  Part Number:                    903184-90,
  Hardware Revision:              C15,
  Serial Number:                  G25Q0772,
  Manufacture Date:               JUN 28 2012,
  Firmware Version:               ,
  Admin Status:                   POWER ON,
  Operational Status:             UP,
  Power Consumption:              51,
  Power Control Checksum:         0xd872,
  CPU Model Type   :              Motorola MPC8540 ADS,
  MAC Address:                    00:d0:95:ec:d1:c8,
  ASIC - Physical 1:              BCM56504_A1,
  FPGA - Physical 1:              0005/00,
  UBOOT Version :                 6.4.4.506.R01,
  UBOOT-miniboot Version :        No Miniboot,
  POE SW Version :                n/a
```

Identifying a module with an incorrect uboot

In the event that a module is mistakenly downgraded use the error log information below to help identify it. The module must be returned to Alcatel-Lucent for repair.

OK1/OK2 LEDs

The OK1 and OK2 LEDs will be off.

Console Display

```
OmniSwitch->
FRI AUG 17 12:38:16 : INTERFACE (6) info message:
+++ Excessive wait for connection to NI 6 NISUP
FRI AUG 17 12:38:16 : HSM-CHASSIS (101) info message:
+++ == HSM == HSM: NI DOWN received, BOARD RESET NI# 6
FRI AUG 17 12:38:16 : SYSTEM (75) info message:
+++ i2cNiBoardReset: task tCS_HSM slot 6 device 0x7a state 0 data 0xff
FRI AUG 17 12:38:16 : HSM-CHASSIS (101) info message:
+++ == HSM == HSM: NI: 6 BOARD RESET
FRI AUG 17 12:38:16 : SYSTEM (75) info message:
+++ i2cNiBoardReset: task tCS_HSM slot 6 device 0x7a state 1 data 0xfe
```

Switch Log

```
at Aug 18 09:28:47 2012       HSM-CHASSIS       info T8: Ni(6) insertion
detected

Sat Aug 18 09:28:48 2012       HSM-CHASSIS       info == HSM == Power ON NI
niSlot=6

Sat Aug 18 09:28:48 2012          SYSTEM         info i2cNiBoardReset: task
tCS_HSM slot 6 device 0x7a state 1 data 0xfe

Sat Aug 18 09:28:48 2012       HSM-CHASSIS       info == HSM ==
csHsmUtilNiCtxBrdSend() nsm CS_HSM_NSM_ST_OP, poweroff 0 Ni6

Sat Aug 18 09:28:48 2012         IPC-DIAG        info ipctPipeReceived:
IPCT_OPEN_CONNECTION slot 6

Sat Aug 18 09:28:48 2012         IPC-DIAG        info priv_ipctOpenConnection:
CONNECTING to 7f020601:10001

Sat Aug 18 09:29:18 2012         IPC-DIAG        info ipctOutgoingDisconnected:
Disconnection from address 7f020601

Sat Aug 18 09:29:18 2012         IPC-DIAG        info priv_ipctOpenConnection:
CONNECTING to 7f020601:10001

Sat Aug 18 09:29:18 2012         IPC-DIAG        info priv_ipctOpenConnection:
connect failed, errno 67
```

Appendix E: Previous Release Features and Enhancements

The following software features and enhancements were introduced in previous AOS Releases. Please refer to the Release Notes for the respective release for additional information.

6.4.5 New Feature/Enhancement Summary

Feature	Platform	Software Package
Hardware/Stacking Features:		
- OmniSwitch Backup Power Shelf (BPS)	6850E	base
- IEEE 802.3ah Dying Gasp	6855/6850E	base
- ISSU in Stacking Configuration	6400/6850E/6855	base
Layer 2 Features :		
- Ethernet Ring Protection v2 (ERPv2)	all	base
- Multi-Chassis Link Aggregation (MC-LAG)	9000E	base
Layer 3 Features:		
- IPv6DHCP Relay	all	base
- Session Initiated Protocol (SIP) Snooping	6850E/6855-U24X/9000E	base
- IP interface name up to 32 character	all	base
- show ip route	all	base
- Bind physical port with IP interface directly excluding vlan assignment	all	base
- Convert local interfaces into OSPF passive interfaces using route map	6850E/6855/9000E	adv rtg
- Increased number of BFD sessions per NI	6850E/6855/9000E	adv. rtg.
- UDP port relay to specific ip-address	all	base
- Automatic OSPF P2P static neighbors	all	adv. rtg.
Management Features :		
- Auto Remote Confguration - Tagged Management VLAN support	6400/6850E/6855	base
- Additional SWLOG message when link up/down event SNMP trap is sent	all	base
- BNPP:Ping and traceroute for read only users	all	base
- Option to build a default user profile for admins	all	base
- Per command authorization for TACACS	all	base
- ssh for read only user	all	base
- Increase system name to 254	all	base
- Improved Captive Portal Performance	6850E/6855/9000E	base
Metro Ethernet Features:		
- L2 control protocol (SW version) enhancement	all	base
- CPE Test Head	6400/6850E/6855-	base

Feature	Platform	Software Package
	U24X/9000E	
- SAA interval timer to 5 minutes	all	base
- Control Frame Tunnelling	all	base
- PPPoE-IA	all	base
Monitoring/Troubleshooting Features :		
- Additional Storm Control option on AOS	all	base
- Loopback Detection	6400/6850E	base
Multicast Features:		
- PIM-BFD Multicast Subsecond Convergence	6850E/6855/9000E	Adv. Rtg.
- Layer 2 Multicast VLAN Replication	all	base
- IGMP v1/v2 to PIM-SSM Static Mapping	all	base
- L2/L3 Convergence Enhancements	all	base
QoS Features :		
Ingress/Egress Bandwidth via RADIUS	all	base
Security Features :		
- Allow policy list definition for HIC	all	base
- SNMPv3 FIPS 140-2 Encryption Modules	all	base
- RADIUS Test Tool	all	base
- User Detection and domain-based profiles/kerberos snooping	all	base
- Virtual Network Profile	6400,/6850E/ 6855	base
- Add additional information to "show 802.1x users" command	all	base
- ARP poisoning protection AOS command	all	base
- Radius Calling station ID	all	base
- Merge HIC to 9000E platform	9000E	secu
- 802.1X on IPMVLAN	all	secu
- Configurable reauthentication / refresh timer	all	secu
- LPS sticky mode without learning windows	6850E/6855/9000E	secu
VRF Features :		
- VRF Route Leak	6850E/6855/9000E	base
- PIM SSM static map	6850E/6855/9000E	base

6.4.4 Feature/Enhancement Summary

Feature	Platform	Software Package
Access Guardian		
- Accounting for Non-supplicants	All	secu
- Captive Portal Enhancements	All	secu
- Control Over Access Guardian	All	secu
- Dynamic User Network Profiles	All	secu
- Host Integrity Check (HIC) Redundancy	All	secu
Out of the Box Auto-Configuration with Dynamic Management VLAN	All	base
DHCP Option-82 CVLAN	All	base
Dual-Home Links		
- Dual-Home Link (DHL) – Active-Active	All	base
Ethernet OAM		
- Virtual MEP – UNI Loopback	all	base
- Fault Propogation Enhancement	All	base
Link Monitoring/Diagnostics/Recovery		
- Link Monitoring/Flapping Detection	All	base
- Link Fault Propogation	all	base
- Interface Violation Recovery	all	base
- Time Domain Reflectometry	all	base
Learned Port Security Enhancements	all	base
Link Aggregation		
- Minimum LAG size	all	base
LLDP		
- Rogue Detection	all	base
OmniSwitch 6850E Stack Mode	6850E	base
- In 6850 Mode – Supports same software features as OS6850 - In 6850E Mode – Supports same software features as 6855-U24X (VRF/egress policies)		
Power Over Ethernet		
- Auto Negotiation of PoE Class	6850E/9000E	base
- 802.3at support	6850E/9000E	base

Feature	Platform	Software Package
Spanning Tree		
- STP Loop Guard	all	base
VLAN-based Ingress Source Filtering / Dynamic ARP Inspection	all	base
Web Cache Communication Protocol (WCCP)	all	base

6.4.3 Feature/Enhancement Summary

Feature	Platform	Software Package
AAA/802.1x		
- Service Type information in RADIUS Access Request	all	base
- Capture Client IP in RADIUS Accounting Message	all	base
Access Guardian		
- Javaless Captive Portal and MAC OS Support	all	encrypt
Out of the Box Auto-Configuration	all	base
DHCP		
- Internal DHCP Server	all	base
- DHCP Client with configurable option 60	all	base
- DHCP Option 82 ASCII support	all	base
Ethernet OAM		
- IEEE 802.1ag Version 8.1	all	base
- ITU Y.1731	all	base
- Service Assurance Agent (SAA) for OAM and IP SLA Measurements	all	base
Ethernet Services		
- L2 Control Protocol Tunneling (L2CP)	6400/6850/6855/9000	base
- Wire-Speed Ethernet Loopback	6400/6850/6855/9000	base
- SVLAN Routing	all	base
IP Enhancements		
- Extended Ping & Traceroute	all	base
- Selectable IP Interface for Management Services	all	base
- IP Loopback0 Address In the Same Range of Existing Subnet	all	base
Link Aggregation		
- Non-unicast Load Balancing on Link Aggregation	all	base
- Active-Stand by Dual Home LinkAgg	all	base
LLDP Network Policies	all	base
- Voice Vlan Support	all	base
- Voice Application Support	all	base
MAC-Forced Forwarding (RFC 4562)	all	base

Feature	Platform	Software Package
Multiple VLAN Registration Protocol (MVRP)	all	base
Multicast Switching and Routing		
- VRF Aware Multicast Routing (PIM)	6855-U24X/9000E	advanced routing
QoS		
- Egress Policy Rules	6400/6855-U24X/9000E	base
- sr-TCM and tr-TCM (RFC 2697/2698)	all	base
- IEEE 802.1q/ad CFI/DEI Bit Stamping	all	base
- Policy Condition Enhancements (VLAN group, 802.1p Range)	all	base
- Flexible Inner DSCP/ToS Mapping to Outer 802.1p	all	base
- QOS Statistics	all	base
Recursive Static Route	all	base
Security		
- BPDU Shutdown Auto-Recovery Timer	all	base
- Admin User Remote Access Restriction Control	all	base
Storm Control		
- Extended Flood Control Metering for Unknown Unicast, Multicast and Broadcast	all	base
USB Support	all	base

6.4.2 Feature/Enhancement Summary

Feature	Platform	Software Package
10Km Stacking	OS6855-U24X	base
802.1x Radius-down Fail-Open	all	base
DDM - Transceiver Digital Diagnostic Monitoring	all	base
DHCP Snooping Option 82 – Port-based format	OS6400/OS6850/OS6855	base
ECMP – Support for up to 16 paths	OS6850/OS9000/OS9000E	base
Ethernet Services		
- L2 Tunneling Enhancements	all	base
- Egress Rate Limiting	OS6400/OS6855-U24X/OS9000E	base
Ethernet OAM 802.3ah – EFM	OS6400/OS6850/OS6855	base
Ethernet Ring Protection (ERP) – Shared VLAN	all	base
IGMP Relay - Forward to Specific Host in L3 Environment	OS6850/OS9000/OS9000E	base
IPMVLAN Group Address and Mask	OS6400/OS6850/OS6855	base
MPLS		
- VPLS Support	OS9000E	mpls
- MPLS Static Fast Re-Route	OS9000E	mpls
- MPLS License	OS9000E	mpls
- MPLS OAM-LSP Ping/Traceroute	OS9000E	mpls
- MPLS Traps	OS9000E	mpls
NTP Server	all	base
Server Load Balancing – Weight Round Robin	OS6850/OS9000/OS9000E	base
Hashing Control	OS6850/OS6855/OS9000/OS9000E	base
Source Learning		
- Disable MAC learning per VLAN	OS6400/OS6855-U24X/OS9000E	base
- Disable MAC learning per port	all	base
VRF		
- BFD Support	OS9000E/OS6855-U24X	base
- VRRP Support	OS9000E/OS6855-U24X	base
- Switch Authentication (ASA)	OS9000E/OS6855-U24X	base
- Switch Access and Utilities	OS9000E/OS6855-U24X	base
- Qos Enhancements	OS9000E/OS6855-U24X	base
- UDP/DHCP Relay	OS9000E/OS6855-U24X	base
Ported features for OS9000E		
- BFD	OS9000E	base
- Configure more than one sFlow receiver	OS9000E	base
- G.8032 Ethernet Ring Protection	OS9000E	base
- IPsec Support for IPv6	OS9000E	base/encrypt
- IPsec Support for OSPF3	OS9000E	base/encrypt
- IPsec Support for RIPng	OS9000E	base/encrypt
- IPv6 Unique Local IPv6 Unicast	OS9000E	base

Feature	Platform	Software Package
- IPv6 Scoped Multicast Addresses	OS9000E	base
- Pause Control	OS9000E	base

6.4.1 and Earlier Feature/Enhancement Summary

Feature	Platform	Software Package
10Km Stacking	OS6855-U24X	base
31-bit Network Mask Support	all	base
802.1AB MED Extensions	all	base
802.1Q	all	base
802.1Q 2005 (MSTP)	all	base
Access Guardian		base
- 802.1x Device Classification	all	base
- 802.1x RADIUS Failover	all	base
- Captive Portal	all	base
- Captive Portal Web Pages	all	base
- Host Integrity Check (HIC)	6400/6850/6855	base
- User Network Profiles (UNP)	all	base
- QoS Policy Lists	6400/6850/6855	base
Access Control Lists (ACLs)	all	base
- ACLs for IPv4	all	base
- ACLs for IPv6	all	base
- ACL & Layer 3 Security	all	base
- ACL Manager (ACLMAN)	all	base
Account & Password Policies	all	base
ARP Defense Optimization	all	base
ARP Poisoning Detect	all	base
Authenticated Switch Access	all	base
Authenticated VLANs	OS6400/OS6850/OS6855/OS9000	base
Automatic VLAN Containment (AVC)	all	base
Auto-Qos Prioritization of IP Phone Traffic	all	base
Auto-Qos Prioritization of NMS Traffic	all	base
Bi-Directional Forwarding Detection (BFD)	OS6850/OS6855/OS9000/OS9000E	base
BGP Graceful Restart	OS6850/OS6855/OS9000/9000E	advanced routing
BGP4	OS6850/OS6855/OS9000/9000E	advanced routing
BPDU Shutdown Ports	all	base
Command Line Interface (CLI)	all	base
DDM	all	
DHCP		
- Option-82	all	base
- Option 82 – Port-based format	OS6400/OS6850/OS6855	base
- DHCP Relay	all	base

Feature	Platform	Software Package
- DHCP Snooping	all	base
- DHCP Snooping Option-82 Data Insertion Format	all	base
DNS Client	all	base
DSCP Range Condition	all	base
DVMRP	OS6850/OS6855/OS9000/OS9000E	advanced routing
Dynamic VLAN Assignment (Mobility)	all	base
Ethernet Ring Protection (G.8032)	**all**	**base**
- Ethernet Ring Protection (ERP) - Shared VLAN	all	base
Ethernet Services		
- L2 Tunneling Enhancements	all	base
- Egress Rate Limiting	OS6400/OS6855-U24X/OS9000E	base
ECMP RIP Support	**OS6850/OS6855/OS9000/9000E**	**base**
- Support for up to 16 paths	OS6850/OS9000/OS9000E	base
End User Partitioning	all	base
Ethernet Interfaces	all	base
Ethernet OAM	**all**	**base**
- Ethernet OAM 802.3ah – EFM	all	base
Flood/Storm Control	all	base
Generic Routing Encapsulation (GRE)	all	base
GVRP	all	base
Hashing Control	OS6850/OS6855/OS9000/OS9000E	base
Health Statistics	all	base
HTTP/HTTPS Port Configuration	all	base
IGMP Multicast Group Configuration Limit	OS6400/OS6850/OS6855/OS9000	base
IGMP Relay - Forward to Specific Host in L3 Environment	OS6850/OS9000/OS9000E	base
Interface Admin Down Warning	OS6400/OS6850/OS6855	base
Interswitch Protocols (AMAP)	All	base
IPMVLAN Multicast Group Overlapping	**all**	**base**
- Group Address and Mask	OS6400/OS6850/OS6855	base
IPMS Flood Unknown Option	all	base
IPsec Support for IPv6	OS6850//OS6855/OS9000/OS9000E	base / encrypt
IPsec Support for OSPF3	OS6850/OS6855/OS9000/OS9000E	base / encrypt
IPsec Support for RIPng	OS6850/OS6855/OS9000/OS9000E	base / encrypt
IPv6		
-Unique Local IPv6 Unicast Addresses	OS6850/OS6855/OS9000/OS9000E	advanced routing
-IPv6 Scoped Multicast Addresses	OS6850/OS6855/OS9000/OS9000E	advanced routing

Feature	Platform	Software Package
-IPv6 Multicast Routing	OS6850/OS6855/OS9000/OS9000E	advanced routing
-IPv6 Multicast Switching (MLD)	all	base
-IPv6 Multicast Switching (Proxying)	all	base
- IPv6 Client and/or Server Support	all	base
- IPv6 Routing	OS6850/OS6855/OS9000/OS9000E	base
IP DoS Filtering	all	base
IP MC VLAN – Support for multiple sender ports	all	base
IP Multinetting	all	base
IP Route Map Redistribution	all	base
IP-IP Tunneling	all	base
IPv4 Multicast Switching (IPMS)	all	base
IPv4 Multicast Switching (Proxying)	all	base
IPv4 Routing	all	base
IS-IS	OS6850/OS9000/OS9000E	advanced routing
ISSU	OS9000E	base
L2 Static Multicast Address	all	base
L4 ACLs over IPv6	all	base
Learned MAC Address Notificaton	all	base
Learned Port Security (LPS)	all	base
Link Aggregation (static & 802.3ad)	all	base
MAC Address Mode	OS9000/OS9000E	base
Mac Authentication for Supplicant/Non-Supplicant	all	base
MAC Retention	OS6400/OS6850/OS6855-U24X	base
Multiple Virtual Routing & Forwarding (Multiple VRF)	OS9000E/OS6855U24X	base
MPLS		
- VPLS Support	OS9000E	mpls
- MPLS Static Fast Re-Route	OS9000E	mpls
- MPLS License	OS9000E	mpls
- MPLS OAM-LSP Ping/Traceroute	OS9000E	mpls
- MPLS Traps	OS9000E	mpls
Network Time Protocol (NTP)		
- Client	all	base
- Server	all	base
OSPFv2	OS6850/OS6855/OS9000/9000E	advanced routing
OSPFv3	OS6850/OS6855/OS9000/9000E	advanced routing
Pause Control/Flow Control	all	base
Port Mapping – Unknown Unicast Flooding	all	base
Partitioned Switch Management	all	base
Pause Control/Flow Control	all	base

Feature	**Platform**	**Software Package**
Per-VLAN DHCP Relay	all	base
PIM PIM-SSM (Source-Specific Multicast)	OS6850/OS6855/OS9000/9000E	advanced routing
Policy Based Mirroring	all	base
Policy Based Routing (Permanent Mode)	all	base
Policy Server Management	all	base
Port Mapping	all	base
Port Mirroring (128:1)	all	base
Port Monitoring	all	base
Port-based Ingress Limiting	all	base
Power over Ethernet (PoE)	OS6400/OS6850/OS6855/OS9000	base
PVST+	all	base
Quality of Service (QoS)	all	base
Quarantine Manager and Remediation	all	base
Redirection Policies (Port and Link Aggregate)	all	base
Remote Port Mirroring	all	base
RIPng	OS6850/OS6855/OS9000/OS9000E	base
RIPv1/RIPv2	all	base
RMON	all	base
Router Discovery Protocol (RDP)	all	base
Routing Protocol Preference	all	base
RRSTP	all	base
Secure Copy (SCP)	all	base
Secure Shell (SSH)	all	base
Server Load Balancing	**OS6400/OS6850/OS9000**	**base**
- WRR	OS6850/OS9000/OS9000E	base
sFlow	all	base
Smart Continuous Switching Hot Swap Management Module Failover Power Monitoring Redundancy	all	base
SNMP	all	base
Software Rollback	all	base
Source Learning	all	base
- Disable MAC learning per VLAN	OS6400/OS6855-U24X/OS9000E	base
- Disable MAC learning per port	all	base
Spanning Tree	all	base
SSH Public Key Authentication	all	base
Switch Logging	all	base
Syslog to Multiple Hosts	all	base
Text File Configuration	all	base

Feature	Platform	Software Package
TFTP Client for IPv4	all	base
Traffic Anomaly Detection (Network Security)	OS6850/OS6855/OS9000/OS9000E	base
UDLD	all	base
User Definable Loopback Interface	all	base
User Network Profile (UNP)	all	base
VLAN Stacking and Translation	all	base
VLAN Stacking Eservices	all	base
VLANs	all	base
VRF – Multiple VRF Routing and Forwarding	OS9000E/OS6850-U24X	base
- BFD Support	OS9000E/OS6855-U24X	base
- VRRP Support	OS9000E/OS6855-U24X	base
- Switch Authentication (ASA)	OS9000E/OS6855-U24X	base
- Switch Access and Utilities	OS9000E/OS6855-U24X	base
- Qos Enhancements	OS9000E/OS6855-U24X	base
- UDP/DHCP Relay		
VRRP Global Commands	OS6850/OS6855/OS9000/OS9000E	base
VRRPv2	OS6850/OS6855/OS9000/OS9000E	base
VRRPv3	OS6850/OS6855/OS9000/OS9000E	base
Web-Based Management (WebView)	all	base
Webview/SNMP support for BGP IPv6 Extensions	OS6850/OS6855/OS9000/OS9000E	advanced routing
Windows Vista for WebView	all	base