Release Notes

OmniSwitch 6250/6350/6450

Release 6.7.1.R01

These release notes accompany release 6.7.1.R01 software for the OmniSwitch 6250/6350/6450 series of switches. The document provides important information on individual software and hardware features. Since much of the information in the release notes is not included in the hardware and software user manuals, it is important to read all sections of this document before installing new hardware or loading new software.

Table of Contents

Related Documentation

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

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

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

OmniSwitch 6350 Hardware Users Guide
Complete technical specifications and procedures for all OmniSwitch 6350 Series chassis, power supplies, and fans.

OmniSwitch 6250/6350/6450 CLI Reference Guide
Complete reference to all CLI commands supported on the OmniSwitch. Includes syntax definitions, default values, examples, usage guidelines, and CLI-to-MIB variable mappings.

OmniSwitch 6250/6350/6450 Network Configuration Guide
Includes network configuration procedures and descriptive information on all the major software features and protocols included in the base software package. Chapters cover Layer 2 information (Ethernet and VLAN configuration), Layer 3 information (routing protocols), security options (Authenticated Switch Access (ASA)), Quality of Service (QoS), link aggregation.

OmniSwitch 6250/6350/6450 Switch Management Guide
Includes procedures for readying an individual switch for integration into a network. Topics include the software directory architecture, software rollback protections, authenticated switch access, managing switch files, system configuration, using SNMP, and using web management software (WebView).

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

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

AOS 6.7.1.R01 Prerequisites

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

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

System Requirements

Memory Requirements

The following are the requirements for the OmniSwitch 6250/6350/6450 Series Release 6.7.1.R01:

- OmniSwitch 6250/6350/6450 Series Release 6.7.1.R01 requires 256 MB of SDRAM and 128MB of flash memory. This is the standard configuration shipped.
- Configuration files and the compressed software images—including web management software (WebView) images—are stored in the flash memory. Use the **show hardware info** command to determine your SDRAM and flash memory.

Miniboot and FPGA Requirements for Existing Hardware

The software versions listed below are the minimum required version for existing OS6250/6350/6450 models, except where otherwise noted. Switches running the minimum versions, as listed below; do not require any miniboot or CPLD upgrade.

Switches not running the minimum version required should be upgraded to the latest Uboot/Miniboot or CPLD that is available with the 6.7.1.R01 AOS software available from Service & Support.

OmniSwitch 6250 (All Models)

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

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

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

OmniSwitch 6450-24/P24/48/P48

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

OmniSwitch 6450-U24

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

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

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

OmniSwitch 6450-P10S/U24S

Release	Uboot/Miniboot	CPLD

Release	Uboot/Miniboot	CPLD
6.7.1.146.R01(GA)	6.6.5.41.R02	P10S - 4 U24S – 7

OmniSwitch 6350-24/P24/48/P48

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

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

6.7.1.R01 New Hardware Supported

New OmniSwitch 6350 Switches

The Alcatel-Lucent OmniSwitch 6350 family is a series of fixed-configuration Gigabit Ethernet switches available as 24 to 48 port, Power-over-Ethernet (PoE) and non-PoE models in a 1U form factor.

Note: The OS6350 series of switches do not support the same feature set as the OS6250 and OS6450 series. Please refer to the Unsupported Software Features section for a list of features that are not supported on the OS6350.

OS6350-24

The OmniSwitch 6350-24 is a Gigabit, non-stackable LAN switch with support for the following:

- 24 RJ-45 10/100/1000 BaseT ports
- 4 SFP 1-Gigabit ports used for uplinks
- Internal AC power supply

OS6350-P24

The OmniSwitch 6350-P24 is a Gigabit, Power Over Ethernet, non-stackable LAN switch with support for the following:

- 24 RJ-45 10/100/1000 BaseT PoE ports (all ports support 802.3at)
- 2 SFP 1-Gigabit ports used for uplinks
- Internal AC power supply supporting a 380W PoE power budget

OS6350-48

The OmniSwitch 6350-48 is a Gigabit, non-stackable LAN switch with support for the following:

- 48 RJ-45 10/100/1000 BaseT ports
- 2 SFP 1-Gigabit ports used for uplinks
- Internal AC power supply

OS6350-P48

The OmniSwitch 6350-P48 is a Gigabit, Power Over Ethernet, non-stackable LAN switch with support for the following:

- 48 RJ-45 10/100/1000 BaseT PoE ports (all ports support 802.3at)
- 4 SFP 1-Gigabit ports used for uplinks
- Internal AC power supply supporting a 780W PoE power budget

Transceivers

SFP-GIG-BX-D20/U20 and SFP-GIG-BX-D40/U40

Now supported on OS6250 SFP fixed/combo ports.

6.7.1.R01 New Software Features and Enhancements

The following software features are new with the 6.7.1.R01 release, subject to the feature exceptions and problem reports described later in these release notes:

Feature	Platform	License
Chassis / System		
Monitor Interswitch Stack Connections	OS6250/6450	
Layer 2		
Prioritization of ERP Packets	OS6250/6450	
Layer 3		
IPv6 Supported RFC / IPv6 Phase 2	OS6250/6350/6450	
IPv6 Security Source Guard	OS6250/6350/6450	
IPv6 Security RA Guard	OS6250/6350/6450	
IPv6 DHCP Relay	OS6250/6350/6450	
IPv6 DHCP Snooping and Remote Circuit ID	OS6250/6350/6450	
Management		
RCL – DHCP Server Priority	OS6250/6350/6450	
Metro		
CPE Test Head enhancements	OS6250/6450	Metro
Security		
Critical Voice VLAN when Radius is Down	OS6250/6350/6450	

Feature Summary Table

Chassis / System

Monitor Interswitch Stacking Connections

Prior to this enhancement port status, statistics, and counters were only available for non-stacking ports. This enhancement adds the ability to display port status, statistics, and counters for stacking ports.

Layer 2

Prioritization of ERP Packets

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

The processing of IPV6 protocol packets is determined by the presence of an IPv6 interface. If an iPv6 interface exists then the packets are processed by the CPU otherwise the packets are transparently forwarded.

To control the processing of IPv4 protocol packets the following command is introduced.

```
-> ip multicast dynamic-control drop-all status {enable | disable}
```

With high multicast traffic in a network the switch could have issues managing the ERP ring, which could result in a loop in the network. This feature allows restricting the L3 multicast protocol packets from being processed by the CPU. The feature allows two types of configuration:

- Configuration excluding well-know protocols, this allows only the well-known IPV4 protocols like OSPF, VRRP, RIPv2, PIM and DVMRP which will continue to be processed by the CPU.
- Configuration including well-know protocols, this controls all the multicast control frames including the IPV4 protocols from being processed by the CPU.

Layer 3

IPv6 Supported RFCs / IPv6 Phase 2 Logo

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

IPv6 Security - Source Guard

IPv6 Source Filtering is an IPv6 security feature. When IPv6 source guard is enabled on an interface, all unknown IPv6 traffic coming in on the interface is sent to the CPU. The software looks up the IPv6 source address to source MAC address in a binding table learned on the device. If the mapping is not found the flow is discarded.

IPv6 source filtering applies to DHCPv6 Snooping ports, link aggregates, and VLANs and restricts port traffic to only packets that contain the client source MAC address, IPv6 address, and VLAN combination. The DHCPv6 Snooping binding table is used to verify the client information for the port/VLAN that is enabled for IPv6 source filtering.

IPv6 Security – Router Advertisement (RA) Guard

RA filtering can be used to prevent the spread of rogue RAs from unauthorized systems. If enabled on an interface, any received RAs will be dropped without being forwarded on to any other connected IPv6 clients. One or more trusted ports or linkaggs can be specified for an interface. RAs received on those trusted ports or linkaggs will be allowed to continue on to all other IPv6 clients reached via the interface.

IPv6 DHCP Relay/snooping/circuit-id

The Alcatel-Lucent OmniSwitch implementation of RFC 3315 provides DHCPv6 Relay support and stateless address auto configurations to IPv6 hosts connected to the switch.

DHCPv6 is used to acquire global IPv6 address in Stateful mode and DHCPv6 messages are exchanged between IPv6 hosts and IPv6 router similar to client-server model. The IPv6 addresses are assigned by DHCPv6 server in Stateful mode The DHCPv6 server maintains the client information.

DHCPv6 Relay on OmniSwitch processes and forwards all DHCPv6 messages triggered by DHCPv6 client to the configured DHCPv6 relay agent as a unicast packet.

Currently the following modes of DHCPv6 Relay are available:

DHCPv6 L3 Relay - Switch acts as a pure Layer 3 relay agent when client facing interface has an IPv6 interface associated. The DHCPv6 Layer 3 Relay configuration has the following modes similar to DHCP relay:

- Global mode - Up to 256 configurable IPv6 relay addresses
- Per-VLAN mode - Up to 256 vlans with up to 8 IPv6 relay addresses Per-VLAN

This can be configured using the ipv6 helper address command family.

DHCPv6 LDRA - Switch acts as a Lightweight DHCPv6 Relay Agent (LDRA) when client facing interface or port has no IPv6 interface and only VLAN is configured on it.

The LDRA uses the following messages for DHCP Snooping and relay-forwarding:

- Relay-Forward
  - The link-address is set to the unspecified address
  - The peer-address is copied from the client link local address
  - The Interface-ID option is inserted

- Relay-Reply

Messages received on clients ports are only forwarded to trusted ports and not to other client ports. On client ports, the following messages are discarded as server violations:

- Advertise
- Reply
- Reconfigure
- Relay-Reply

A client port can also be configured as client-only-trusted or client-only-untrusted. When a client port is client-only-untrusted, the Relay-Forward message is discarded. The LDRA intercepts any DHCPv6 message received on client ports.

Management

RCL- DHCP Server Priority

This feature modifies the Automatic Remote Configuration DHCP client process on an OmniSwitch to give priority to a DHCP response from the OV Client server. If a DHCP response is received on VLAN 1 from a DHCP server other than OmniVista, the response will be temporarily stored. The DHCP client will continue to wait for the 30 second window to see if a DHCP response is received from the higher priority OmniVista DHCP server.

Priority 1 – OmniVista DHCP server (VSI = alcatel.nms.ov2500)
Priority 2 – OXO DHCP Server – (VSI = alcatel.a.a4400.0)
Priority 3 – All other DHCP servers

If no DHCP response is received from the OmniVista DHCP server within the 30 second window, the stored response will be applied.

If a DHCP response is received from the OmniVista DHCP server it will be immediately applied.

Metro

CPE Test Head enhancements

The L2 SAA test allows to measure the RTT and Jitter during the test head operation. The L2 SAA test is performed between two OmniSwitches. The test can be run in parallel with the other CPE tests.

The L2 SAA also allows continuous monitoring of the network performance between the devices. The network performance is monitored by continuous injections of L2 SAA packets throughout the tests which generates and analyze traffic performance.

On receiving the SAA reply for every frame, the minimum RTT, maximum RTT, total RTT, minimum Jitter, maximum Jitter, total Jitter and number of packets received will be calculated and stored in a global buffer for reference.

Security

Critical Voice VLAN when RADIUS is Down

The critical Voice VLAN allows classifying the IP phone traffic from the data traffic when the authentication server is down.

A user-network-profile (UNP) is configured to classify packets that cannot be authenticated when auth-server is down or unreachable. An additional user-network-profile must be configured to be assigned to voice traffic to keep it separate from other data traffic. The user-network-profile is associated to the Voice policy and the UNP is applied to the detected IP phone traffic.

In the presence of an authentication server, the IP phone MAC address is authenticated against the authentication server and the traffic is classified into a voice domain VLAN that is returned from the RADIUS server.

When the RADIUS server is down, the MAC address is first classified as IP phone traffic or non-IP Phone traffic. The MAC address is verified against the LLDP database for classification.

Unsupported Software Features

CLI commands and Web Management options may be available in the switch software for the following features. These features are not supported:

Feature	Platform
BGP	OS6250/6350/6450
DVMRP	OS6250/6350/6450
IS-IS	OS6250/6350/6450
Multicast Routing	OS6250/6350/6450
OSPF, OSPFv3	OS6250/6350/6450
PIM	OS6250/6350/6450
Traffic Anomaly Detection	OS6250/6350/6450
IPv6 Sec	OS6250/6350/6450
IP Tunnels (IPIP, GRE, IPv6)	OS6250/6350/6450
Server Load Balancing	OS6250/6350/6450
CPE Testhead	OS6350
VLAN Stacking / Ethernet Services	OS6350
Ethernet/Link/Test OAM	OS6350
PPPoE	OS6350
ERP	OS6350
GVRP	OS6350
IPv4/ IPv6 RIP	OS6350
VRRP	OS6350
HIC/ BYOD / Captive Portal	OS6350
mDNS Relay	OS6350
IPMVLAN (VLAN Stacking Mode)	OS6350
IPMC Receiver VLAN	OS6350
OpenFlow	OS6350
License Management	OS6350
Loopback Detection	OS6350
SAA	OS6350
Ethernet Wire-rate Loopback Test	OS6350
Dying Gasp	OS6350
Stacking	OS6350

Unsupported CLI Commands

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

Software Feature	Unsupported CLI Commands
AAA	aaa authentication vlan single-mode aaa authentication vlan multiple-mode aaa accounting vlan show aaa authentication vlan show aaa accounting vlan
CPE Test Head	test-oam direction bidirectional test-oam role loopback
Chassis Mac Server	mac-range local mac-range duplicate-eeprom mac-range allocate-local-only show mac-range status

Software Feature	Unsupported CLI Commands
DHCP Relay	ip helper traffic-suppression ip helper dhcp-snooping port traffic-suppression
Ethernet Services	ethernet-services sap-profile bandwidth not-assigned
Flow Control	flow
Hot Swap	reload ni [slot] # [no] power ni all
Interfaces	show interface slot/port hybrid copper counter errors show interface slot/port hybrid fiber counter errors
QoS	qos classify fragments qos flow timeout
System	install power ni [slot]

Open Problem Reports and Feature Exceptions

The problems listed here include problems known at the time of the product's release. Any problems not discussed in this section should be brought to the attention of the Alcatel-Lucent Technical Support organization as soon as possible. Please contact customer support for updates on problem reports (PRs) where no known workaround was available at the time of release.

QoS

PR	Description	Workaround
208297	If link aggregate member ports are configured to be part of a port group and a QoS rule has that port group as a condition with an action to forward to another port, the LACP frames from these ports are redirected to the target port specified in the action. This causes the LACPDU packets to not be processed, which brings the link aggregate down.	Do not configure link aggregate member ports as part of a port group.

System

PR	Description	Workaround
208433	After a takeover, on the new primary "show stacking interfaces" output for the "Number of Status Change" field gets reset to 1 for all the stacking ports.	There is no known workaround at this time.
205986	On an OS6450-10 the combo port LED will sometimes remain on even though the link is down.	Administratively disable and re-enable the port to fix the issue.

Redundancy/ Hot Swap

CMM (Primary Stack Module) and Power Redundancy Feature Exceptions

- Manual invocation of failover (by user command or Primary pull) must be done when traffic loads are minimal.
- Hot standby redundancy or failover to a secondary CMM without significant loss of traffic is only supported if the secondary is fully flash synchronized with the contents of the primary's flash.
- Failover/Redundancy is not supported when the primary and secondary CMMs are not synchronized (i.e., unsaved configs, different images etc.).
- When removing modules from the stack (powering off the module and/or pulling out its stacking cables), the loop back stacking cable must be present at all times to guarantee redundancy. If a module is removed from the stack, rearrange the stacking cables to establish the loopback before attempting to remove a second unit.
- When inserting a new module in the stack, the loopback has to be broken. Full redundancy is not guaranteed until the loopback is restored.

Stack Element Insert/Removal Exceptions

All insertions and removals of stack elements must be done one at a time and the inserted element must be fully integrated and operational as part of the stack before inserting another element.

Hot Swap / Insert of 1G/10G Modules on OS6450

- Inserting a 10G module into a slot that was empty does not require a reboot.
- Inserting a 10G module into a slot that had a 10G module does not require a reboot.
- Inserting a 10G module into a slot that had a 1G module requires a reboot.
- Inserting a 1G module into a slot that was empty requires a reboot.
- Inserting a 1G module into a slot that had a 1G module does not require a reboot.
- Inserting a 1G module into a slot that had a 10G module requires a reboot.

- Note: PTP is not supported when the OS6450-U24S is in stacking mode. If the OS6450-U24S is in stacking mode, or one of the hot swap scenarios above causes it to boot up in stacking mode, PTP will be disabled.

Technical Support

Alcatel-Lucent technical support is committed to resolving our customer's technical issues in a timely manner. Customers with inquiries should contact us at:

Region	Phone Number
North America	800-995-2696
Latin America	877-919-9526
Europe Union	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484

Email: esd.support@alcatel-lucent.com

Internet: Customers with Alcatel-Lucent service agreements may open cases 24 hours a day via Alcatel-Lucent's support web page at: service.esd.alcatel-lucent.com.

Upon opening a case, customers will receive a case number and may review, update, or escalate support cases on-line. Please specify the severity level of the issue per the definitions below. For fastest resolution, please have telnet or dial-in access, hardware configuration—module type and revision by slot, software revision, and configuration file available for each switch.

Severity 1 Production network is down resulting in critical impact on business—no workaround available.
Severity 2 Segment or Ring is down or intermittent loss of connectivity across network.
Severity 3 Network performance is slow or impaired—no loss of connectivity or data.
Severity 4 Information or assistance on product feature, functionality, configuration, or installation.

Appendix A: AOS 6.7.1.R01 Upgrade Instructions

OmniSwitch Upgrade Overview

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

- OmniSwitch 6250 models being upgraded to AOS 6.7.1.R01.
- OmniSwitch 6450 models being upgraded to AOS 6.7.1.R01.

Prerequisites

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

- Read and understand the entire Upgrade procedure before performing any steps.
- The person performing the upgrade must:
  - Be the responsible party for maintaining the switch's configuration.
  - Be aware of any issues that may arise from a network outage caused by improperly loading this code.
  - Understand that the switch must be rebooted and network users will be affected by this procedure.
  - Have a working knowledge of the switch to configure it to accept an FTP connection through the Network Interface (NI) Ethernet port.
- Read the 6.7.1.R01 Release Notes prior to performing any upgrade for information specific to this release.
- All FTP transfers MUST be done in binary mode.

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

OmniSwitch Upgrade Requirements

These tables list the required Uboot/Miniboot, CPLD and AOS combinations for upgrading an OmniSwitch. The Uboot/Miniboot and CPLD may need to be upgraded to the versions listed below to support AOS Release 6.7.1.R01.

Version Requirements - Upgrading to AOS Release 6.7.1.R01

Version Requirements to Upgrade to AOS Release 6.7.1.R01			
	AOS	**Uboot/Miniboot**	**CPLD**
6250-24/P24/8M/24M	6.7.1.146.R01 GA	6.6.3.259.R01 (minimum) 6.6.4.158.R01 (optional)	12 (minimum) 14 (optional)
6450-10/10L/P10/P10L	6.7.1.146.R01 GA	6.6.3.259.R01	6
6450-24/P24/48/P48	6.7.1.146.R01 GA	6.6.3.259.R01	11
6450-U24	6.7.1.146.R01 GA	6.6.3.259.R01	6
6450-24L/P24L/48L/P48L	6.7.1.146.R01 GA	6.6.4.54.R01	11

- The OS6450 "L" models were introduced in AOS Release 6.6.4.R01 and ship with the correct minimum versions, no upgrade is required.
- Uboot/Miniboot versions 6.6.4.158.R01 and 6.6.4.54.R01 were newly released versions in 6.6.4.R01.
- CPLD versions 14, 6, and 11 were newly released versions in 6.6.4.R01.
- Uboot/Miniboot version 6.6.3.259.R01 was previously released with 6.6.3.R01.
- CPLD version 12 was previously released with 6.6.3.R01.
- IMPORTANT NOTE: If performing the optional upgrade BOTH Uboot/Miniboot and CPLD MUST be upgraded.

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

Upgrading to AOS Release 6.7.1.R01

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

- Upgrading an OmniSwitch to AOS Release 6.7.1.R01 may require two reboots of the switch or stack being upgraded. One reboot for the Uboot/Miniboot or AOS and a second reboot for the CPLD.
- Refer to the Version Requirements table to determine the proper code versions.
- Download the appropriate AOS images, Uboot/Miniboot, and CPLD files from the Service & Support website.

Summary of Upgrade Steps

1. FTP all the required files to the switch
2. Upgrade the Uboot/Miniboot and AOS images as required. (A reboot is required).
3. Upgrade the CPLD as required. (Switch automatically reboots).
4. Verify the upgrade and remove the upgrade files from the switch.

Upgrading - Step 1. FTP the 6.7.1.R01 Files to the Switch

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

1. Download and extract the 6.7.1.R01 Upgrade archive from the Service & Support website. The archive will contain the following files to be used for the upgrade:
   - Uboot/Miniboot Files – kfu-boot.bin, kfminiboot.bs
   - AOS Files – KFbase.img, KFeni.img, KFos.img, KFsecu.img
   - CPLD File - KFfpga_upgrade_kit
2. FTP (Binary) the 6.7.1.R01 Uboot/Miniboot files listed above to the **/flash** directory on the primary CMM, if required.
3. FTP (Binary) the CPLD upgrade kit listed above to the **/flash** directory on the primary CMM, if required.
4. FTP (Binary) the 6.7.1.R01 image files listed above to the **/flash/working** directory on the primary CMM.
5. Proceed to Step 2.

Note: Make sure the destination paths are correct when transferring the files. Also, when the transfer is complete, verify the file sizes are the same as the original indicating a successful binary transfer.

Upgrading - Step 2. Upgrade Uboot/Miniboot and AOS

Follow the steps below to upgrade the Uboot/Miniboot (if required) and AOS. This step will upgrade both Uboot/Miniboot and AOS once the switch/stack is rebooted. If a Uboot/Miniboot upgrade is not required skip to rebooting the switch to upgrade the AOS.

1. Execute the following CLI command to update the Uboot/Miniboot on the switch(es) (can be a standalone or stack).
   ```
   -> update uboot all
   -> update miniboot all
   ```
   - If connected via a console connection update messages will be displayed providing the status of the update.
   - If connected remotely update messages will not be displayed. After approximately 10 seconds issue the '**show ni**' command, when the update is complete the **UBOOT-Miniboot Version** will display the upgraded version.

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

2. Reboot the switch. **This will update both the Uboot/Miniboot (if required) and AOS**.
   ```
   -> reload working no rollback-timeout
   ```
3. Once the switch reboots, certify the upgrade:
   - If you have **a single CMM** enter:
   ```
   -> copy working certified
   ```
   - If you have **redundant CMMs** enter:
   ```
   -> copy working certified flash-synchro
   ```
4. Proceed to Step 3 (Upgrade the CPLD).

Upgrading - Step 3. Upgrade the CPLD

Follow the steps below to upgrade the CPLD (if required). Note the following:

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

WARNING: During the CPLD upgrade, the switch will stop passing traffic. When the upgrade is complete, the switch will automatically reboot. This process can take up to 5 minutes to complete. Do not proceed to the next step until this process is complete.

Single Switch Procedure

1. Enter the following to begin the CPLD upgrade:

   ```
   -> update fpga cmm
   ```

The switch will upgrade the CPLD and reboot.

Stack Procedure

Updating a stack requires all elements of the stack to be upgraded. The CPLD upgrade can be completed for all the elements of a stack using the ‘all’ parameter as shown below.

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

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

The stack will upgrade the CPLD and reboot.

Proceed to Verifying the Upgrade to verify the upgrade procedure.

Verifying the Upgrade

The following examples show what the code versions should be after upgrading to AOS Release 6.7.1.R01.

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

Verifying the Software Upgrade

To verify that the AOS software was successfully upgraded to 6.7.1.R01, use the show microcode command as shown below. The display below shows a successful image file upgrade.

```
-> show microcode

Package          Release        Size       Description
-----------------+---------------+----------+------------------------------------------
KFbase.img       6.7.1.R01    15510736  Alcatel-Lucent Base Software
KFos.img         6.7.1.R01    2511585   Alcatel-Lucent OS
KFeni.img        6.7.1.R01    5083931  Alcatel-Lucent NI software
KFsecu.img       6.7.1.R01    597382  Alcatel-Lucent Security Management
```

Verifying the U-Boot/Miniboot and CPLD Upgrade

To verify that the CPLD was successfully upgraded on a CMM, use the show hardware info command as shown below.

```
-> show hardware info

CPU Type                          : Marvell Feroceon,
Flash Manufacturer                : Numonyx, Inc.,
Flash size                        : 134217728 bytes (128 MB),
RAM Manufacturer                  : Samsung,
RAM size                          : 268435456 bytes (256 MB),
Miniboot Version                  : 6.6.4.158.R01,
Product ID Register               : 05
Hardware Revision Register        : 30
FPGA Revision Register            : 014
```

You can also view information for each switch in a stack (if applicable) using the show ni command as shown below.

```
-> show ni

Module in slot 1
  Model Name:                  OS6250-24,
  Description:                 24 10/100 + 4 G,
  Part Number:                 902736-90,
  Hardware Revision:           05,
  Serial Number:               K2980167,
  Manufacture Date:            JUL 30 2009,
  Firmware Version:            ,
  Admin Status:                POWER ON,
  Operational Status:          UP,
  Power Consumption:           30,
  Power Control Checksum:      0xed73,
  CPU Model Type   :           ARM926 (Rev 1),
  MAC Address:                 00:e0:b1:c6:b9:e7,
  ASIC - Physical 1:           MV88F6281 Rev 2,
  FPGA - Physical 1:           0014/00,
  UBOOT Version :              n/a,
  UBOOT-miniboot Version :     6.6.4.158.R01,
  POE SW Version :             n/a
```

Note: It is OK for the 'UBOOT Version' to display "n/a". The 'UBOOT-miniboot' version should be the upgraded version as shown above.

Remove the CPLD and Uboot/Miniboot Upgrade Files

After the switch/stack has been upgraded and verified the upgrade files can be removed from the switch.

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

Appendix B: AOS 6.7.1.R01 Downgrade Instructions

OmniSwitch Downgrade Overview

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

- OmniSwitch 6250 models being downgraded from AOS 6.7.1.R01.
- OmniSwitch 6450 models being downgraded from AOS 6.7.1.R01.

Note: The OmniSwitch 6350 requires a minimum of AOS Release 6.7.1.R01 and cannot be downgraded.

Prerequisites

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

- Read and understand the entire downgrade procedure before performing any steps.
- The person performing the downgrade must:
  - Be the responsible party for maintaining the switch's configuration.
  - Be aware of any issues that may arise from a network outage caused by improperly loading this code.
  - Understand that the switch must be rebooted and network users will be affected by this procedure.
  - Have a working knowledge of the switch to configure it to accept an FTP connection through the Network Interface (NI) Ethernet port.
- Read the 6.7.1.R01 Release Notes prior to performing any downgrade for information specific to this release.
- All FTP transfers MUST be done in binary mode.

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

OmniSwitch Downgrade Requirements

Downgrading the Uboot/Miniboot or CPLD is not required when downgrading AOS from 6.7.1.R01. Previous AOS releases are compatible with the Uboot/Miniboot and CPLD versions shipping from the factory.

Summary of Downgrade Steps

1. FTP all the required AOS files to the switch
2. Downgrade the AOS images as required. (A reboot is required).
3. Verify the downgrade.

Downgrading - Step 1. FTP the 6.6.5 Files to the Switch

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

1. Download and extract the appropriate 6.6.X archive from the Service & Support website. The archive will contain the following files to be used for the downgrade:
   - AOS Files – KFbase.img, KFeni.img, KFos.img, KFsecu.img

2. FTP (Binary) the 6.6.X image files listed above to the **/flash/working** directory on the primary CMM.

3. Proceed to Step 2.

Note: Make sure the destination paths are correct when transferring the files. Also, when the transfer is complete, verify the file sizes are the same as the original indicating a successful binary transfer.

Downgrading - Step 2. Downgrade the AOS

Follow the steps below to downgrade the AOS. This step will downgrade the AOS once the switch/stack is rebooted.

1. Reboot the switch. **This will downgrade the AOS**.
   -> reload working no rollback-timeout

2. Once the switch reboots, certify the downgrade:
   - If you have **a single CMM** enter:

   -> copy working certified
   - If you have **redundant CMMs** enter:

   -> copy working certified flash-synchro

Proceed to Verifying the Downgrade.

Verifying the Downgrade

To verify that the AOS software was successfully downgraded use the show microcode command as shown below. The example display below shows a successful image file downgrade. The output will vary based on the model and AOS version.

```
-> show microcode

Package          Release        Size       Description
-----------------+---------------+----------+------------------------------------------
KFbase.img       6.6.5.R02   15510736  Alcatel-Lucent Base Software
KFos.img         6.6.5.R02   2511585   Alcatel-Lucent OS
KFeni.img        6.6.5.R02    5083931  Alcatel-Lucent NI software
KFsecu.img       6.6.5.R02     597382  Alcatel-Lucent Security Management
```