Release Notes

OmniSwitch 6350/6450

Release 6.7.2.R05

These release notes accompany release 6.7.2.R05 software for the OmniSwitch 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.

Note: The OmniSwitch 6250 is not supported in this release.

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: https://businessportal2.alcatel-lucent.com

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 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 Transceivers Guide
Includes transceiver specifications and product compatibility information.

Technical Tips, Field Notices, Upgrade Instructions
Contracted customers can visit our customer service website at: https://businessportal2.alcatel-lucent.com.

AOS 6.7.2.R05 Prerequisites

N/A

System Requirements

Memory Requirements

The following are the requirements for the OmniSwitch6350/6450 Series Release 6.7.2.R05:

- OmniSwitch 6350/6450 Series 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 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 CPLDthat is available with the 6.7.2.R05 AOS software available from Service & Support.

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

Release	Uboot/Miniboot	CPLD
6.7.2.113.R05(GA)	6.6.3.259.R01	6

OmniSwitch 6450-24/P24/48/P48

Release	Uboot/Miniboot	CPLD
6.7.2.113.R05(GA)	6.6.3.259.R01	11

OmniSwitch 6450-U24

Release	Uboot/Miniboot	CPLD
6.7.2.113.R05(GA)	6.6.3.259.R01	6

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

Release	Uboot/Miniboot	CPLD
6.7.2.113.R05(GA)	6.6.4.54.R01	11

OmniSwitch 6450-P10S/U24S

Release	Uboot/Miniboot	CPLD
6.7.2.113.R05(GA)	6.6.5.41.R02	P10S - 4 U24S – 7

OmniSwitch 6450-M/X Models

Release	Uboot/Miniboot	CPLD
6.7.2.113.R05(GA)	6.7.1.54.R02	10M – 6 24X/24XM/P24X/48X/P48X – 11 U24SXM/U24X - 7

OmniSwitch 6350-24/P24/48/P48

Release	Uboot/Miniboot	CPLD
6.7.2.113.R05(GA)	6.7.1.69.R01/6.7.1.103.R01 6.7.1.30.R04 (optional)	12 (minimum) 16 (optional)
Note: The optional uboot/miniboot and CPLD is only needed for stacking support. Standalone units		

Release	Uboot/Miniboot	CPLD
can remain at the previous versions.		

OmniSwitch 6350-10/P10

Release	Uboot/Miniboot	CPLD
6.7.2.113.R05(GA)	6.7.1.30.R04	4

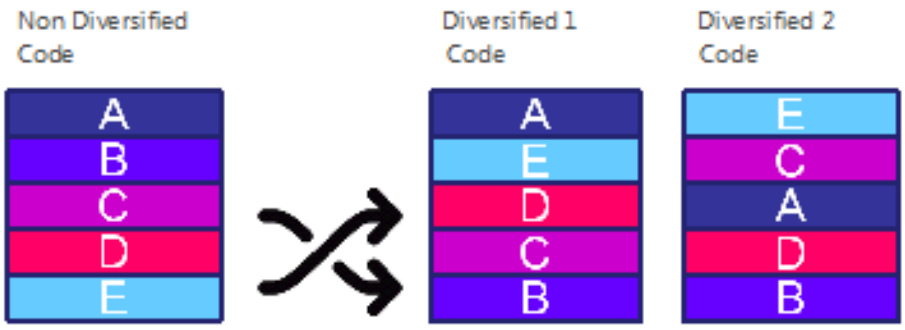
Note: Refer to the Upgrade Instructions section for upgrade instructions and additional information on Uboot/Miniboot and CPLD requirements.

CodeGuardian

Alcatel-Lucent Enterprise and LGS Innovations have combined to provide the first network equipment to be hardened by an independent group. CodeGuardian promotes security and assurance at the network device level using independent verification and validation of source code, software diversification to prevent exploitation and secure delivery of software to customers.

CodeGuardian employs multiple techniques to identify vulnerabilities such as software architecture reviews, source code analysis (using both manual techniques and automated tools), vulnerability scanning tools and techniques, as well as analysis of known vulnerabilities in third party code.
Software diversification

Software diversification randomizes the executable program so that various instances of the same software, while functionally identical, are arranged differently. The CodeGuardian solution rearranges internal software while maintaining the same functionality and performance and modifies the deliverable application to limit or prevent/impede software exploitation. There will be up to 3 different diversified versions per GA release of code.



CodeGuardian AOS Releases

Chassis	Standard AOS Releases	AOS CodeGuardian Release	LGS AOS CodeGuardian Release
OmniSwitch 6450	AOS 6.7.2.R05	AOS 6.7.2.RX5	AOS 6.7.2.LX5

X=Diversified image 1-3
ALE will have 3 different diversified images per AOS release (R14 through R34)
Our partner LGS will have 3 different diversified images per AOS release (L14 through L34)

6.7.2.R05 New Hardware Supported

SFP-10G-ZR
This release adds support for the SFP-10G-ZR transceiver on the OS6450 SFP+ chassis ports and XNI plug-in modules for both stacking and uplink.

6.7.2.R05 New Software Features and Enhancements

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

Feature	Platform	License
Wire rate loopback	OS6450	N/A
Interface status details	OS6350/OS6450	N/A
Enhanced DDM Display	OS6350/OS6450	N/A
Stronger key exchange for 6450	OS6350/OS6450	N/A
Multiple MAC range port security	OS6350/OS6450	N/A
Policy List in CoA Packet Processing Enhancement.	OS6350/OS6450	N/A
OV Cirrus - Change the default admin password when switch becomes OV managed	OS6350/OS6450	N/A
OV Cirrus Troubleshooting Enhancements • Switch /AP must perform actions issued by OV Cirrus user, for better troubleshooting • OV Cirrus user must be able to view Switch/AP logs on OV (Activation Server) UI even before it becomes OV Managed.	OS6350/OS6450	N/A
NTP Burst/iBurst Support	OS6350/OS6450	N/A
Add new DHCP VSO for "Vendor specific string"	OS6350/OS6450	N/A
NAS IP address to be modified from VPN IP to default IP	OS6350/OS6450	N/A
Support of Applying QoS Policy when two or more policy servers are configured	OS6350/OS6450	N/A
BYOD Support for 6350	OS6350/OS6450	N/A
AAA Authentication to search local database	OS6350/OS6450	N/A
OV Cirrus - PKI Enhancement	OS6350/OS6450	N/A

Feature Summary Table

New Feature Descriptions

Wire-Rate Loopback
The loopback test capability allows the use of an external test head to send traffic at wire-rate speed to a specific switch port which then loops the traffic back to the test head. The test head measures and collects statistics on frame loss, delay, and latency of the loopback traffic. Two types of loopback tests are supported, Inward loopback and Outward loopback. In previous releases for the loopback test to work, source MAC address, destination MAC address, source VLAN, loopback port and type of re-direction either inward or outward was required.
In the current release, AOS supports Inward loopback tests with only the destination MAC address and loopback port, and Outward loopback test with destination MAC address, source VLAN, and loopback port.

Interface Status Details
The **show interfaces** command displays the operational status of the port (up/down) with other parameters such as port type, MAC address, and so on. The operational status of the port may be down due to admin action and software reasons such as violations caused due to STP, LFP, LLDP, LPS, and so on.

In this release, whenever the port is down, the **show interfaces** command displays the reason due to which the operational status of the port is down, so that the user is aware of the fault and can proceed with corrective measures. For example, if the violation is caused due to Learned Port Security, the operational status is displayed as 'down, LPS'. If the violation caused is due to Spanning Tree Protocol, operational status is displayed as down, STP'. This feature is supported only to display the software reasons that cause the operational status of the port to go to down state. If the port is down due to physical fault, 'none' will be printed in the corresponding place.

Enhanced DDM Display
Digital Diagnostics Monitoring (DDM) allows the switch to monitor the status of a transceiver by monitoring the threshold values and generate a trap message when the operating value crosses the delimited values.
In this release, the support is extended to display the DDM information for all the ports irrespective of operational status of the port, either remote or local.

SSH Stronger Key Exchange
AOS SSH functionality generates and uses DSA 1024 bit keys and RSA 2048 keys and the Diffie-Hellman key exchange algorithm. As part of SSH Strong Key Exchange, AOS also supports ECDSA public keys and ECDH key exchange algorithm. ECDSA 256-bit public/private key pair is generated when a switch reboot is done. The keys are generated during boot up only if the respective key pairs files are not present in the "/flash/network" directory. AOS shall support ECDH 256, ECDH 384 and ECDH521 key algorithm along with diffie-hellman in common criteria and default mode.

Multiple MAC Range Port Security
The LPS MAC range allows to restrict the source learning of the host MAC addresses. The MAC range command supported only one MAC range configuration. In this release AOS enhances the capability to configure up to eight MAC ranges per port. The multiple MAC ranges can be configured using the port-security mac-range CLI command.

Policy List in CoA Packet Processing Enhancement.
During CoA packet processing, if the UNP returned in both levels of authentication is from the same VLAN the re-authentication mechanism was not triggered.
The following enhancement is done in the current release:
During CoA packet processing, if the UNP returned in both levels of authentication is from the same VLAN then the Policy-List returned from the server is processed.
If the server returned Policy-List is not available on the switch then the Policy-List associated with the UNP is not applied.

BYOD and External Captive Portal support on OS6350

The OmniSwitch implementation of BYOD leverages the OmniVista-UPAM (Unified Policy Access Manager) /Aruba ClearPass Policy Manager (CPPM) and Access Guardian features on the OmniSwitch. It allows guest access or on boarding of both wired or wireless devices such as employee, guest, employee owned or silent devices through an OmniSwitch edge device with UPAM/ClearPass as a RADIUS server. This feature is now supported on OS6350.

OV Cirrus - Change the default admin password when switch becomes OV managed
In the process of getting an OmniSwitch managed by OmniVista, we now have the ability to change the default password of admin user. This is useful to avoid the security threat of leaving the switch running with the default admin password. Password change will happen only when admin user has the password as switch.

OV Cirrus - OV Cirrus Troubleshooting Enhancement
This is to facilitate troubleshooting of network devices by remote operators, even when a device fails to get managed by OV Cirrus. To enable remote troubleshooting, OV Cirrus operators will be provided with a user interface in Device Catalog application, and can choose one or more troubleshooting commands. These commands are sent one by one to the device whenever the device tries to go through the Activation procedure.

NTP Burst/iBurst Support
In this release, NTP supports burst/iburst mode of operation. This enables faster synchronization of configured NTP pool servers, and periodic resolution of NTP servers present in the pending list.

New DHCP VSO to help customer protect their devices from unauthorized use
A new DHCP VSO (Network ID) is added to allow a customer to protect their devices from unauthorized use. They do this by specifying a DHCP option that identifies their Network ID and by registering the same value in their OmniVista Cirrus. By doing this, the customer ensures that anyone who doesn't know this Network ID value cannot add/manage the switches from OmniVista Cirrus. The switch or AP will send this option's value in the Call-Home request message to the Activation server. The Call-Home request will be answered only if the network ID of the tenant matches the value registered in OV.

NAS IP address modified from VPN Client IP to local LAN IP
In OV Cirrus Environment, when UPAM uses "IP Range" to verify the Authentication/Accounting packages, UPAM needs to get the local LAN IP of AP/Switch from the packet. So AP and Switch needs to set NAS IP address, an attribute in the Authentication and Accounting package, to be the local LAN IP instead of the VPN Client IP. OmniSwitch now supports NAS IP Attribute in RADIUS packet to use the local LAN IP instead of the VPN Client IP.

Policy reload does not work if there are 2 or more policy server configured.
When an OmniSwitch is having more than two policy servers configured, the highest precedence server will be identified and the configuration of the highest precedence server will be loaded to avoid the policy recache.

OV Cirrus PKI Update Enhancement
This enhancement facilitates updating of device PKI objects like device certificate, private key, public key, certificate signing request and CA certificate chain from OV Cirrus.

The AAA authentication to search local database
In this enhancement, local authentication is allowed as the first authentication method, after which switch authentication can be done with external servers. In this way, local authentication can be configured as either first or last server. Local authentication could be either first or last for FTP/SSH/HTTP/Telnet/Console. In case when the authenticated user name is not available in local database, then authentication retry is made with the next configured external server. SNMP and default is not supported with local as first followed by external server.

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	6350/6450
DVMRP	6350/6450
IS-IS	6350/6450
Multicast Routing	6350/6450
OSPF	6350/6450
PIM	6350/6450
Traffic Anomaly Detection	6350/6450
IPv6 Sec	6350/6450
IP Tunnels (IPIP, GRE, IPv6)	6350/6450
Server Load Balancing	6350/6450
VLAN Stacking / Ethernet Services	OS6350
Ethernet/Link/Test OAM	OS6350
PPPoE	OS6350
ERP	OS6350
GVRP	OS6350
IPv4/ IPv6 RIP	OS6350
VRRP	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

Unsupported CLI Commands

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

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

Open Problem Reports and Feature Exceptions

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

CR	Description	Workaround
CRAOS6X-1308	While configuring outward service on port 1/52 (XNI-U2 fiber port) loopback functionality is not working as expected.	Workaround: 1. Disable and Enable the loopback test using CLI command: *loopback-test testname* 2. Admin down/up using CLI. 3. Physical Port toggle.
CRAOS6X-1619	Appropriate error message is not displayed while creating loopback profile with profile name of characters above 32.	There is no known workaround at this time.
CRAOS6X-1292	Error message is not appropriate while creating loopback profile with profile name of characters above 32.	There is no known workaround at this time.
CRAOS6X-1150	Device got stuck up while initiating call home when OmniSwitch is in common criteria mode.	There is no known workaround at this time.
CRAOS6X-672	OVCloud: Device console hangs during call-home restart once VPN failed.	Login through Management IP through telnt or SSH.
CRAOS6X-68	Star symbol is missing in show erp command when ERP member port NI is not present in stack.	There is no known workaround at this time.

Redundancy/ Hot Swap

CMM (Primary Stack Module) and Power Redundancy Feature Exceptions

- Manual invocation of failover (by user command or Primary pull) must be done when traffic loads are minimal.
- Hot standby redundancy or failover to a secondary CMM without significant loss of traffic is only supported if the secondary is fully flash synchronized with the contents of the primary's flash.
- Failover/Redundancy is not supported when the primary and secondary CMMs are not synchronized (i.e., unsaved configurations, 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.

- When hot-swapping any element of the stack it must be replaced by the same model. For example, anOS6450-P24 model can only be hot-swapped with another OS6450-P24 model.

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: Precision Time Protocol (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:ebg_global_supportcenter@al-enterprise.com

Internet: Customers with Alcatel-Lucent service agreements may open cases 24 hours a day via Alcatel-Lucent Enterprise support web page at: https://businessportal2.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 6.7.2.R05 Upgrade Instructions

OmniSwitch Upgrade Overview

This section documents the upgrade requirements for an OmniSwitch. These instructions apply to the following:

- OmniSwitch 6450 models being upgraded to AOS 6.7.2.R05.
- OmniSwitch 6350 models being upgraded to AOS 6.7.2.R05.

See also Specific Upgrade Instructions For OS6350 for more upgrade instructions for OmniSwitch6350.

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.

NOTE: 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 6.7.2.R05.

Version Requirements – Upgrading to AOS Release 6.7.2.R05

Version Requirements to Upgrade to AOS Release 6.7.2.R05			
	AOS	**Uboot/Miniboot**	**CPLD**
6450-10/10L/P10/P10L 6450-24/P24/48/P48 6450-U24 6450-24L/P24L/48L/P48L 6450-P10S 6450-U24S 6450-10M 6450-24X 6450- 24XM,24X,P24X,P48X,	6.7.2.112.R05 GA	6.6.3.259.R01 6.6.3.259.R01 6.6.3.259.R01 6.6.4.54.R01 6.6.5.41.R02 6.6.5.41.R02 6.7.1.54.R02 6.7.1.54.R02 6.7.1.54.R02	6 11 6 11 4 7 6 7 11
6350-24/P24/48/P48 6350-10/P10	6.7.2.112.R05 GA	6.7.1.69.R01/6.7.1.103.R01 (minimum) 6.7.1.30.R04 (optional) 6.7.1.30.R04	12 (minimum) 16 (optional) 4
• 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.
- The 6.7.1.30.R04 uboot/miniboot and CPLD 16 for the 6350-24/48 models is only needed for stacking support. Standalone units can remain at the previous version.

Upgrading to AOS Release 6.7.2.R05

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 6.7.2.R05 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. Rebootthe switch.
3. Upgrade the CPLD as required. (Switch automatically reboots).
4. Verify the upgrade and remove the upgrade files from the switch.

Specific Upgrade Instructions for OS6350

This section documents the specific upgrade requirements for an OmniSwitch6350.

Dynamic Rules supported in 672R04 is 193 whereas in 6.7.2.R05 it is 173. So when the switches are upgraded from pre 6.7.2.R05 (6.7.2.R01/2/3/4) to 6.7.2.R05 it is recommended to check the “show qos slice ingress” command and confirm the Dynamic Rules usage. The Dynamic Rules usage should not be more than 173 rules.

Note that If the Dynamic usage rule is more than 173 rules, the behaviour of the OmniSwitch post upgrade is not as expected.

For a smooth upgrade to 6.7.2.R05 in OS6350, the user has to manually confirm prior to upgrade, that existing QoS configuration / TCAM entries usage is not more than 173 rules.

Upgrading - Step 1. FTP the 6.7.2.R05 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 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 (optional)
   - AOS Files (6450) – KFbase.img, KFeni.img, KFos.img, KFsecu.img
   - AOS Files (6350) – KF3base.img, KF3eni.img, KF3os.img, KF3secu.img
   - CPLD File - KFfpga_upgrade_kit (optional)
2. FTP (Binary) the 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 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 an 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 fpgacmm

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 fpgani 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 6.7.2.R05.

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, 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       6.7.2.112.R05   18130755 Alcatel-Lucent Enterprise Base Softw
KFos.img         6.7.2.112.R05    3562484 Alcatel-Lucent Enterprise OS
KFeni.img        6.7.2.112.R05    6152493 Alcatel-Lucent Enterprise NI softwar
KFsecu.img       6.7.2.112.R05     648189 Alcatel-Lucent Enterprise Security M
KFdiag.img       6.7.2.112.R05    2411898 Alcatel-Lucent Enterprise Diagnostic
```

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:                 OS6450-24,
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.
```

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.
   ->rmKFfpga.upgrade_kit
   ->rmkfu-boot.bin
   ->rm kfminiboot.bs

Appendix B: AOS 6.7.2.R05 Downgrade Instructions

OmniSwitch Downgrade Overview

This section documents the downgrade requirements for the OmniSwitchmodels. These instructions apply to the following:

- OmniSwitch 6450 models being downgraded from AOS 6.7.2.R05.
  OmniSwitch 6350 models being downgraded from AOS 6.7.2.R05.

  Note: The OmniSwitch 6350-10/P10 require a minimum of AOS Release 6.7.1.R04 and cannot be downgraded to any earlier release.

  Note: The OmniSwitch PoE models with the new PoE controller require a minimum of AOS Release 6.7.2.R01 and cannot be downgraded to any earlier release.

- OS6350-P10 (903966-90)
- OS6350-P24 (903967-90)
- OS6350-P48 (903968-90)

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 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 6.7.2.R05. Previous AOS releases are compatible with the Uboot/Miniboot and CPLD versions shipping from the factory.

Summary of Downgrade Steps

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

Downgrading - Step 1. FTP the 6.6.5 or 6.7.1 Files to the Switch

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

1. Download and extract the appropriate archive from the Service & Support website. The archive will contain the following files to be used for the downgrade:
   - AOS Files (OS6450) – KFbase.img, KFeni.img, KFos.img, KFsecu.img
   - AOS Files (OS6350) – KF3base.img, KF3eni.img, KF3os.img, KF3secu.img

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

3. Proceed to Step 2.

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

Downgrading - Step 2. Downgrade the AOS

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

1. Reboot the switch. **This will downgradethe 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.R0    25083931  Alcatel-Lucent NI software
KFsecu.img      6.6.5.R02     597382  Alcatel-Lucent Security Management
```

Appendix C: Fixed Problem Reports

The following table lists the previously known problems that were fixed in this release.

CR/PR NUMBER	SUMMARY
CRAOS6X-36	OS6450 stack - Intermittent ping loss in IPMVLAN.
CRAOS6X-50	SFP is detected, however the links fails to come up.
CRAOS6X-51	Randomly the communication between OS6450-U24S and OS6450-P10S is getting failed.
CRAOS6X-650	TUT: OS6450-24 IP entry capacity & QOS error logs.
CRAOS6X-866	Need clarification regarding fix for PR 222602.
CRAOS6X-872	Stellar AP 1231 in aaa blocking policy (not classified in built-in defaultWLANProfile policy).
CRAOS6X-913	CMI: OS6450: Switch crashed while upgrading.
CRAOS6X-958	6450 stack get stuck in Pending state after the ERP failed link is up.
CRAOS6X-959	The IP interface is not UP.
CRAOS6X-967	Switch Radius attributes.
CRAOS6X-969	OS6450-P10: Authrized failed: Unable to execute any command.
CRAOS6X-981	KDC: Need Authentication log output on syslog for OS6450 switch.
CRAOS6X-1026	All user confirm the log file when connect to http and https in OS6350-P10.
CRAOS6X-1087	OS6450 - DDM warnings during link status changes.
CRAOS6X-1151	CPE test OAM giving throughput as negative when duration longer than 2146.
CRAOS6X-1176	Regarding specific logs output continuously.
CRAOS6X-1211	Issue with DHL connectivity (PR 212857).
CRAOS6X-1256	SODEXO PARENT: OS6450: switch ports moved to blocked mode with QoS violation.
CRAOS6X-1306	6350 - Stacking leds behavior.
CRAOS6X-1312	System Info messge: timerWdHandler: kill failed - logs every 20s.
CRAOS6X-1339	High CPU load on Omniswitch 6450 stacks.
CRAOS6X-1370	5XOS6450: Daughter board doesn't show up in the stack units 3,4,5.
CRAOS6X-1480	OS6350-24: SFP ports are not working.
CRAOS6X-1507	EC: ADANA BÜYÜKŞEHİR BELEDİYESİ : Vulnerability- NTP mode 6.
CRAOS6X-1547	LLDP link issue between AOS switch and Stellar AP in Enterprise mode.
CRAOS6X-1594	OS6450/OS6350(6.7.2.107.R03): Need time info to be updated in the commands output "show system hardware-self-test/show system process-self-test".
CRAOS6X-1596	OS6350: "ERROR: Invalid policy. Captive Portal is not supported in this hardware platform while trying to configure auth-server-down policy.
CRAOS6X-1611	How to suppress the logs "RadprocessNext" AAA.