

Release Notes

OmniSwitch 6600/7000/8800

Release 5.1.5.R04

These release notes accompany release 5.1.5.R04 software for the OmniSwitch 6600 series hardware, OmniSwitch 7000 series hardware, and OmniSwitch 8800 hardware. They provide important information on individual software features and hardware modules. Since much of the information in these 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: References to OmniSwitch 6600 series hardware include model numbers: OS6624/OS6648 (also known as OS6600-24/OS6600-48), OS6600-U24, OS6600-P24, and OS6602-24/OS6602-48. Where an item is unique to an OS6600 switch, the specific model number is used.

References to OmniSwitch 7000 series hardware include model numbers: OS7700/OS7800. Where an item is unique to an OS7000 switch, the specific model number is used.

Contents

- Related Documentation, see page 2.
- System Requirements, see page 4.
 - Memory Requirements, see page 4
 - MiniBoot and BootROM Requirements, see page 4
 - Power Supply Requirements, see page 5
 - Upgrading to 5.1.5.R04, see page 5
 - Merging OS6600 stacks, see page 5
- New Hardware Supported, see page 6
- New Software Supported, see page 10.
- Unsupported Software Features, see page 16.
- Unsupported CLI Commands, see page 17.
- Unsupported MIBs, see page 18
- AVLAN Web Authentication, see page 24
- Fixed Problem Reports, see page 25
- Open Problem Reports, and Feature Exceptions, see page 28.
 - Switch Management, see page 28.
 - Layer 2, see page 46.
 - Layer 3, see page 71.
 - Quality of Service, see page 80.
 - Advanced Routing, see page 87.
 - Security, see page 94.
 - System, see page 108.
 - OmniSwitch NIs, see page 108
- Technical Support, see page 120

Related Documentation

These Release Notes should be used in conjunction with the OmniSwitch 6600, OmniSwitch 7700/7800, and OmniSwitch 8800. The following are the titles and descriptions of the OmniSwitch 6600, OmniSwitch 7700/7800, and OmniSwitch 8800 user manuals:

- *OmniSwitch 6600 Series Getting Started Guide*

Describes the hardware and software procedures for getting an OmniSwitch 6600 Series switch up and running.
- *OmniSwitch 6600 Series Hardware User Guide*

Complete technical specifications and procedures for all OmniSwitch 6600 Series, power supplies, fans, and Network Interface (NI) modules.
- *OmniSwitch 6624/6648 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), and link aggregation.
- *OmniSwitch 6624/6648 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 6624/6648 Technical Tips, Field Notices*

Contracted customers can visit our customer service website at: <http://eservice.ind.alcatel.com>.
- *OmniSwitch 7700/7800 Getting Started Guide*

Describes the hardware and software procedures for getting an OmniSwitch 7700 or OmniSwitch 7800 up and running. Also provides information on fundamental aspects of OmniSwitch software architecture.
- *OmniSwitch 7700/7800 Hardware User Guide*

Complete technical specifications and procedures for all OmniSwitch 7700 and OmniSwitch 7800 chassis, power supplies, fans, and Network Interface (NI) modules.
- *OmniSwitch 7700/7800/8800 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-SM), and OSPF.
- *OmniSwitch 7700/7800/8800 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, such as RIP and IPX), security options (authenticated VLANs), Quality of Service (QoS), link aggregation, and server load balancing.

- *OmniSwitch 7700/7800/8800 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 7700/7800/8800 Technical Tips, Field Notices*

Includes information published by Alcatel's Customer Support group.

- *OmniSwitch 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.

- *Upgrade Instructions for 5.1.5.R04*

Provides instructions for upgrading the switch software.

System Requirements

Memory Requirements

- OmniSwitch 6624 Release 5.1.5.R04 requires 128 MB of SDRAM and 32MB of flash memory. This is the standard configuration shipped.
- OmniSwitch 6648 Release 5.1.5.R04 requires 128 MB of SDRAM and 32MB of flash memory. This is the standard configuration shipped.
- OmniSwitch 6600-U24 Release 5.1.5.R04 requires 128 MB of SDRAM and 32MB of flash memory. This is the standard configuration shipped.
- OmniSwitch 6600-P24 Release 5.1.5.R04 requires 128 MB of SDRAM and 32MB of flash memory. This is the standard configuration shipped.
- OmniSwitch 6602-24 Release 5.1.5.R04 requires 128 MB of SDRAM and 32MB of flash memory. This is the standard configuration shipped.
- OmniSwitch 6602-48 Release 5.1.5.R04 requires 128 MB of SDRAM and 32MB of flash memory. This is the standard configuration shipped.
- OmniSwitch 7700 Release 5.1.5.R04 requires 128 MB of SDRAM and 32MB of flash memory. This is the standard configuration shipped on a Chassis Management Module (CMM).
- OmniSwitch 7800 Release 5.1.5.R04 requires 128 MB of SDRAM and 32MB of flash memory. This is the standard configuration shipped on a Chassis Management Module (CMM).
- OmniSwitch 8800 Release 5.1.5.R04 requires 128 MB of SDRAM and 32MB of flash memory. This is the standard configuration shipped on a Chassis Management Module (CMM).

Configuration files and the compressed software images—including web management software (WebView) images—are stored in flash memory. Use the **show hardware info** command to determine your SDRAM and flash memory.

Miniboot, BootROM, and FPGA Recommendations

Note: The diagnostic image version is different from the version of the operational images. The diagnostic image is derived from independent software and not tied to software features or release cycles, but to hardware production schedules.

OmniSwitch 7000/8800

- Miniboot: 5.1.5.340.R01
- BootROM: 5.1.5.340.R01
- FPGA: 44 (recommended)

OmniSwitch 6624/6648

Note: The following Miniboot and BootROM upgrades are for manufacturing purposes only. They are used to support the SST BootROM chip. A field upgrade is not needed for 5.1.5.R04. The Miniboot 5.1.2.2.R01 and BootROM 5.1.4.128.R01 are sufficient at this time.

- Miniboot: 5.1.5.115.R02
- BootROM: 5.1.5.115.R02

Power Supply Requirements

The OS7000/8800 power supply requirements vary depending on the number of Network Interface (NI) modules installed in the switch and the power redundancy requirements. Each OS7800/OS8800 chassis contains four slots for power supplies, and the OmniSwitch 7700 chassis has three slots for power supplies.

Note. In a fully loaded chassis configuration, the OS7700 requires a minimum of two power supplies, the OS7800 requires three power supplies, and the OS8800 requires three power supplies. See the *OmniSwitch 7700/7800 Hardware User Guide* and the *OmniSwitch 8800 Hardware User Manual* for more information about power supply requirements.

Upgrading to 5.1.5.R04

Instructions for upgrading to 5.1.5.R04 (image files, Miniboot, Bootrom, FPGA) are available on the Customer Support website along with the 5.1.5.R04 software (eservice.ind.alcatel.com).

Note. Failure to follow the upgrade instructions correctly can permanently damage CMM hardware.

Note. Once you have upgraded to 5.1.5.R04, downgrading the system must be done on each CMM separately.

Merging OS6600 Stacks

You cannot merge two OS6600 stacks (i.e., virtual chassis) unless they are running identical versions of software. Alcatel recommends the following steps to merge two separate stacks:

- 1 Upgrade one or both (if necessary) stacks so they are running the same software.
 - 2 Use the **copy working certified flash-syncro** command on the stacks you have upgraded.
 - 3 Confirm both stacks are running the same software with the **show microcode loaded** command.
 - 4 Confirm that all switches (modules) in both stacks have unique slot numbers by viewing the Slot Indicator LEDs. Renumber any duplicate slot numbers by using the procedures outlined in the *OmniSwitch 6600 Series Getting Started Guide*.
 - 5 Connect the two stacks together into one stack. Refer to the *OmniSwitch 6600 Series Getting Started Guide* for cabling guidelines.
 - 6 Use the **show stack topology** command to confirm that the stacks have been successfully merged.
-

New Hardware Supported

Note: No new hardware has been introduced in release 5.1.5.R04. The supported hardware below is from previous releases.

New Network Interface Modules (NIs)

Note: The following hardware became available in release 5.1.5.R01:

OmniSwitch 7700/7800 NIs

OS7-ENI2-C24

Second-generation version of the OmniSwitch 7700/7800 24-port 10/100 copper Ethernet NI module. Each port uses RJ-45 connectors and supports category 5 Twisted pair cable 100 ohm.

OS7-ENI-C24-UPG

First-generation version of the OmniSwitch 7700/7800 24-port 10/100 copper Ethernet NI module upgraded for Release 5.1.5. Each port uses RJ-45 connectors and supports category 5 Twisted pair cable 100 ohm.

OS7-ENI-P24

The Ethernet Network Interface (ENI) module is a Power over Ethernet (PoE) module that provides 24 twisted-pair inline power ports, individually configurable as 10BaseT or 100BaseTX. In addition, powered Devices (PDs) such as IP phones, wireless LAN stations, Ethernet hubs, and other access points can be plugged directly into the Ethernet ports. From these RJ-45 ports, the devices receive both electrical power and data flow.

OS7-GNI-U2-UPG

First-generation version of the OmniSwitch 7700/7800 two-port wire-rate 1 Gbps fiber Gigabit module upgraded for Release 5.1.5. The OS7-GNI-U2-UPG provides two GBIC slots.

OS7-GNI2-C12

Second-generation version of the OmniSwitch 7700/7800 12-port 10/100/1000 high-density copper Gigabit Ethernet NI module.

OS7-GNI-C12-UPG

First-generation version of the OmniSwitch 7700/7800 12-port 10/100/1000 high-density copper Gigabit Ethernet NI module upgraded for release 5.1.5.

OS7-GNI2-U12

Second-generation version of the OmniSwitch 7700/7800 12-port 1 Gbps high-density fiber Gigabit Ethernet NI module. The OS7-GNI2-U12 provides 12 MiniGBICs slots.

OS7-GNI-U12-UPG

First-generation version of the OmniSwitch 7700/7800 12-port 1 Gbps high-density fiber Gigabit Ethernet NI module. The OS7-GNI-U12-UPG provides 12 MiniGBICs slots.

OmniSwitch 8800 NIs

OS8-10GNI-UR1

The Gigabit Network Interface (GNI) module is a wire-rate 10 Gbps module that provides two redundant Xenpak slots acting as one port. (Only one port may be active at a time.)

OS8-GNI2-C24

Second-generation version of the OmniSwitch 8800 12-port 10/100/1000 high-density copper Gigabit Ethernet NI module.

OS8-GNI-C24-UPG

First-generation version of the OmniSwitch 8800 12-port 10/100/1000 high-density copper Gigabit Ethernet NI module upgraded for Release 5.1.5.

OS8-GNI2-U24

Second-generation version of the OmniSwitch 8800 24-port 1 Gbps high-density fiber Gigabit Ethernet NI module. The OS8-GNI2-U24 provides 24 MiniGBICs slots.

OS8-GNI-U24-UPG

First-generation version of the OmniSwitch 8800 24-port 1 Gbps high-density fiber Gigabit Ethernet NI module upgraded for Release 5.1.5. The OS8-GNI-U24-UPG provides 24 MiniGBICs slots.

New Fan Tray

OS7000-FTTC

OmniSwitch 7700/7800 fan tray with power-controlled fans (less power, less RPM).

New Chassis

OS6600-U24

The OS6600-U24 is a stackable edge/workgroup switch offering 24 fiber 100 Mbps Ethernet SFP ports. The switch may be equipped with up to four Gigabit Ethernet ports for connections to a high-speed backbone or server.

Note: The following new hardware became available in release 5.1.5.R02 and is supported subject to the feature exceptions and problem reports described later in these release notes:

New Chassis

OS6600-P24

The OS6600-P24 (OS6600-P24) is a stackable edge/workgroup switch offering 24 Power over Ethernet (PoE) 10/100 Ethernet ports. The OS6600-P24 can also be equipped with up to four Gigabit Ethernet ports for connections to a high speed backbone or server.

In addition to working as an individual, stand-alone switch, the OS6600-P24 can also be linked together with any other member of the OmniSwitch 6600 Family of switches to form a single, high-density virtual chassis known as a *stack* consisting of up to eight (8) switches in *any combination* within the stack.

OS6602-24

The OS6602-24 is a stackable edge/workgroup switch offering 24 10/100 Ethernet ports. The OS6602-24 has two Gigabit Ethernet SFP ports for connections to a high speed backbone or server and two ports for stacking switches.

In addition to working as an individual, stand-alone switch, the OS6602-24 can also be linked together with any other member of the OmniSwitch 6600 Family of switches to form a single, high-density virtual chassis known as a *stack* consisting of up to eight (8) switches in *any combination* within the stack.

OS6602-48

The OS6602-48 is a stackable edge/workgroup switch offering 48 10/100 Ethernet ports. The OS6602-48 has two Gigabit Ethernet SFP ports for connections to a high speed backbone or server and two ports for stacking switches.

In addition to working as an individual, stand-alone switch, the OS6602-48 can also be linked together with any other member of the OmniSwitch 6600 Family of switches to form a single, high-density virtual chassis known as a *stack* consisting of up to eight (8) switches in *any combination* within the stack.

New Backup Power Supplies (BPSs)

Note: The following BPSs became available in release 5.1.5.R02:

OS6600-BPS-P

The OS6600-BPS-P unit is the OS6600-P24's backup power supply, which provides backup electrical current used for switch functions and PoE ports. The OS6600-BPS-P contains two built-in power supplies—one supplying 55 Watts (100 Watts maximum) for switch functions and the other supplying 210 watts for PoE functions.

OS6602-BPS

The OS6602-BPS is an AC backup power supply for OS6602-24 and OS6602-48 switches. The backup power supply bay is located on the chassis rear panel of OS6602-24 and OS6602-48 switches.

OS6602-BPS-DC

The OS6600-BPS is a DC backup power supply for OS6602-24 and OS6602-48 switches. The backup power supply bay is located on the chassis rear panel of OS6602-24 and OS6602-48 switches.

New Software Supported

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

Feature Summary

Feature	Platform	Software Package
10 Gigabit Enhancements	OS8800	base
4 to 1 Port Mirroring	all	base
802.1x Sygate Phase 1	all	base
Ability to log in when the identity field is greater than or equal to 32 bytes	all	security
ACL for Traffic Management	OS7700/OS7800/OS8800	base
AVLAN Enhancements	all	base optional security
AVLAN Users Increased from 1024 to 2048	all	security
CLI Command to Disable PoE Capacitor Detector	OS6600/OS7700/OS7800	base
Destination TCP Port ACL Enhancements	all	base
DOS Attacks and Port Security	OS7700/OS7800/OS8800	base
Dynamic Link Aggregation across OS6600 Stacks	OS6600	base
Ethernet Enhancements	OS7700/7800	base
Generic UDP Relay	OS7700/OS7800/OS8800	base
High Availability Vlans	OS7000 / OS8800	base
Increased IPX Routing Table Size	OS7700/7800/OS8800	base
IPMS Enhancements	all	base
IP Routing Enhancements	all	base
LACP Port Down Traps	all	base
NTP Client Enhancements	all	base
OS6600 Anti-spoofing ACLs	OS6600	base
OS6600 Reboot Strategy	OS6600	base
OS7700/7800/8800 Anti Spoofing ACLs	OS7700/7800/8800	base
OSPF Enhancements	all	base advanced routing
PIM-SSM (Source-Specific Multicast)	OS7700/7800/8800	base advanced routing
Port Mirroring Enhancements	OS7700/7800/8800	base
Port Mirroring to Mirror IPMS	all	base

Feature	Platform	Software Package
Power over Ethernet	OS6600/OS7700/7800	base
QoS Enhancements	all	base
Reduce Processor Resources Used by ACL/QoS	OS7700/OS7800/OS8800	base
Router Discovery Protocol (RDP)	all	base
Second-Generation NI Dynamic Link Aggregation	OS7700/OS7800/OS8800	base
VRRP Tracking	all	base

Feature Descriptions

10 Gigabit Enhancements

The following features are now supported on OmniSwitch 8800 OS8-10GNI-UR1 modules:

- CMM takeover
- Redundant 10 Gigabit port cutover enhancements.

4 to 1 Port Mirroring

A single destination port can now be shared by 4 sessions.

802.1x Sygate Phase 1

Interoperability between Alcatel 802.1x and Sygate Management Server (SMS) and Sygate Enforcer is now supported.

Ability to log in when the identity field is greater than or equal to 32 bytes

The identity field in Alcatel 802.1x authentication now works with all applications that send more than 32 bytes (e.g., Sygate).

ACL for Traffic Management

Management access can now be restricted to a specific physical port and management access can now be restricted to originate from a specific management subnet.

AVLAN Enhancements

Authenticated VLAN enhancements in this release include:

- Specifying an authentication IP address other than the default
- Enabling the default VLAN for authentication
- Supporting certain port binding rules on authenticated VLANs
- Creating a web browser client language file

AVLAN Users Increased from 1024 to 2048

The number of possible AVLAN users has been increased from 1024 to 2048.

CLI Command to Disable PoE Capacitor Detector

The following new command has been added to enable/disable capacitor detection for Power over Ethernet (PoE) devices:

- **lanpower capacitor-detection**

In addition, the following new command has been added to display the current PoE capacitor detection method:

- **show lanpower capacitor-detection**

Destination TCP Port ACL Enhancements

A special service group named DropServices has been added to OS software for all platforms that improves performance with ACLs intended to drop traffic with specific destination TCP/UDP ports. See documentation for configuration examples and details on this new enhancement.

A new trap has been added whereby a switch will send a trap when a single link in the aggregate group is down or cannot join the aggregate group.

DOS Attacks and Port Security

Enhanced port security and additional features to prevent DOS attacks. These include:

- Detect and prevent IP source address spoofing
- BPDU control Packets on defined sets of ports
- Designate a set of switch ports as user ports
- Dropping packets based on TCP/UDP destination port
- Prevent VRRP flapping under virus/worm attack
- Filter ICMP Echo PING packets on user ports

Dynamic Link Aggregation across OS6600 Stacks

Dynamic link aggregation groups can now be configured across multiple switches in an OS6600 stack.

Ethernet Enhancements

Half duplex mode on the OmniSwitch 7700/7800 OS7-ENI-FM-12 is now supported.

Generic UDP Relay

In addition to BOOTP/DHCP relay, generic UDP relay is now available on OmniSwitch 7700/7800/8800 switches. Using generic UDP relay, traffic destined for well-known service ports (e.g., NBNS/NBDD, DNS, TFTP, TACACS) or destined for a user-defined service port can be forwarded to a maximum of 256 VLANs on the switch.

High Availability VLANs

High availability VLANs are now supported on OS7000 and OS8800 switches. High availability VLANs, unlike standard Alcatel VLANs, allow you to send unicast and multicast traffic intended for a single destination MAC address to multiple switch ports within the same VLAN.

Note. This feature requires second generation (i.e., ENI-2, GNI-2) NI modules.

Increased IPX Routing Table Size

The size of the IPX routing table now supports up to 5000 entries. This is an increase from the previous maximum of 2000 entries.

IPMS Enhancements

- IPMS is now supported with link aggregation.
- IGMP version 3 (IGMPv3), which handles forwarding by source IP address and IP multicast destination address, is now supported on OS7000 and OS8800 only. (IGMPv2 handles forwarding by IP multicast destination address only.)

IP Routing Enhancements

The number of routing instances is changed from 64 to 128.

LACP Port Down Trap

A new trap has been added whereby a switch will send a trap when a single link in the aggregate group is down or cannot join the aggregate group.

NTP Client Enhancements

The NTP client may now be configured to operate in broadcast mode. Broadcast mode specifies a client switch listens on all interfaces for server broadcast timestamp information; it uses these messages to update its time.

OS6600 Anti-spoofing ACLs

A new ACL enhancement has been added that will disable a port on 6600 series OmniSwitches when IP spoofing is detected on the ports. By creating a new policy action called DisablePorts, ports will automatically be administratively disabled when spoofed traffic is detected. The user may reset this state by disconnecting and reconnecting their ethernet cable. See documentation for details and configuration examples for this enhancement.

OS6600 Reboot Strategy

It is no longer necessary to reboot an entire OS6600 stack for synchronization of the configuration. Due to this change the **restore redundancy** and **show restore redundancy status** commands have been deleted.

OS7700/7800/8800 Anti Spoofing ACLs

It is now possible to prevent IP source address spoofing using a new port group named UserPorts. Ports placed in this special port group will block traffic whose source IP does not match the IP subnet configured for that port. See documentation for details and configuration examples.

OSPF Enhancements

The following new features are now supported:

- Graceful (Hitless) Support During Failover, which is the time period between the restart and the reestablishment of adjacencies after a planned (e.g., the users performs the takeover) or unplanned (e.g., the primary CMM unexpectedly fails) failover.
- OSPF adjacencies over non broadcast links.

PIM-SSM (Source-Specific Multicast) Support

By default, PIM-SM software now supports Source-Specific Multicast. No additional user configuration is required. PIM-SSM is automatically enabled and operational as long as PIM-SM is loaded and IGMPv3 source-specific joins are received within the SSM address range.

Port Mirroring Enhancements

Up to four unidirectional or up to two bidirectional port mirroring sessions are now supported on OmniSwitch 7700/7800 and 8800 switches. In earlier releases only one session was supported.

Port Mirroring to Mirror IPMS

IPMS has been enhanced to support port mirroring on OmniSwitch 6600/7700/7800/8800

Power over Ethernet (PoE)

The Power over Ethernet software in the switch is used to configure the OS7-ENI-P24 module on OS7000 switches and on the OS6600-P24.

QoS Enhancements

- **QoS on High Density Gigabit Modules (OmniSwitch 7700/7800/8800 only)** On high-density gigabit modules, packets coming into the switch are classified on the module first before any QoS settings take effect. The QoS software may be used to set the default classification, determine the internal protocol priority and control the buffering, queuing, servicing, and discarding of packets.
- **ToS Stamping and Source/Destination ACLs**
The OmniSwitch 6600 series now supports ToS stamping and source/destination access control lists.

Reduce Processor Resources Used by ACL/QoS

ACL/QoS functions are now highly optimized for speed in order to prevent a Denial of Service (DoS) condition on a particular NI or switch in a stack.

Router Discovery Protocol (RDP)

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

Second-Generation NI Dynamic Link Aggregation

Hardware multicast routing is now supported on OmniSwitch 7000/8800 second-generation NI modules.

VRRP Tracking

VRRP Tracking is now supported. A virtual router's priority may be conditionally modified to prevent another router from taking over as master. Tracking policies are used to conditionally modify the priority setting whenever a VLAN, slot/port, and/or IP address associated with a virtual router goes down.

Unsupported Software Features

CLI commands and web management options are available in the switch software for the following features; however, these features are not supported in the current release:

Feature	Platform	Software Package
Interswitch Protocols (GMAP)	all	base
IP Multicast Routing	OS6600	base
OSPF Database Overflow (RFC 1765)	all	base advanced routing

Unsupported CLI Commands

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

Software Feature	Unsupported CLI Commands
Chassis Mac Server	mac-range local mac-range duplicate-EEPROM mac-range allocate-local-only show mac-range status
Hot Swap	reload ni [slot] #
Interswitch Protocols (GMAP)	All Interswitch Protocols (GMAP) CLI Commands on all platforms are unsupported
IP Multicast Routing IPX	All IP Multicast Routing CLI Commands on OS6600 are unsupported ipx watchdog-spoof [vlan] [enable disable] no ipx watchdog-spoof [vlan] show ipx watchdog-spoof ipx serialization [vlan] [enable disable] no ipx serialization [vlan] show ipx serialization ipx spx-spoof [vlan] [enable disable] no ipx spx-spoof [vlan] show ipx spx-spoof
NTP	no ntp server all
Quality of Service	qos port <slot/port> [no] maximum bandwidth qos port <slot/port> [no] maximum default depth qos port <slot/port> [no] maximum default buffers qos port <slot/port> [no] maximum bandwidth qos port <slot/port> [no] maximum signal bandwidth qos port <slot/port> [no] maximum reserve bandwidth qos [no] classify fragments

Unsupported MIBs by Platform

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

Feature	MIB
Interswitch Protocols (GMAP)	All MIBs are unsupported.
IP Multicast Routing	All MIBs for OS6600 are unsupported.
Quality of Service (QoS)	IETF_P_BRIDGE

Unsupported MIB Variables – All Platforms

MIB Name	Unsupported MIB variables on All Platforms
AlcatelIND1AAA	aaauProfile
AlcatelIND1LAG	alclnkaggAggEniActivate
AlcatelIND1WebMgt	alaIND1WebMgtRFSCfgTable alaIND1WebMgtHttpPort alaIND1WebMgtHttpsPort
IEEE_802_1X	dot1xAuthDiagTable dot1xAuthSessionStatsTable dot1xSuppConfigTable dot1xSuppStatsTable
IETF_BGP4	bgpRcvdPathAttrTable
IETF_BRIDGE	dot1dTpPortTable dot1dStaticTable
IETF_ENTITY	entLogicalTable entLPMMappingTable entAliasMappingTable
IETF_ETHERLIKE	dot3CollTable dot3StatsSQETestErrors dot3StatsInternalMacTransmitErrors dot3StatsCarrierSenseErrors dot3StatsInternalMacReceiveErrors dot3StatsEtherChipSet dot3StatsSymbolErrors dot3ControlInUnknownOpcodes
IETF_IF	ifRcvAddressTable ifTestTable
IETF_IP_FORWARD_MIB	ipForwardTable
IETF_IPMROUTE_STD	ipMrouteScopeNameTable
IETF_MAU (RFC 2668)	rpMauTable rpJackTable broadMauBasicTable ifMauFalseCarriers ifMauTypeList ifMauAutoNegCapability ifMauAutoNegCapAdvertised ifMauAutoNegCapReceived
IETF_OSPF (RFC 1850)	ospfAreaRangeTable

MIB Name	Unsupported MIB variables on All Platforms
IETF_OSPF_TRAP	ospfTrapControl
IETF-PIM	pimRPTable
IETF_P_BRIDGE	dot1dExtBase dot1dPortCapabilitiesTable dot1dPortPriorityTable dot1dUserPriorityRegenTable dot1dTrafficClassTable dot1dPortOutboundAccessPriorityTable dot1dPortGarpTable dot1dPortGmrpTable dot1dTpHCPortTable dot1dTpPortOverflowTable
IETF_Q_BRIDGE (RFC 2674)	dot1qTpGroupTable dot1qForwardAllTable dot1qForwardUnregisteredTable dot1qStaticMulticastTable dot1qPortVlanStatisticsTable dot1qPortVlanHCStatisticsTable dot1qLearningConstraintsTable
IETF_RIPv2	rip2IfConfDomain
IETF_RMON	hostControlTable hostTable hostTimeTable hostTopNControlTable hostTopNTable matrixControlTable matrixSDTable matrixDSTable filterTable channelTable bufferControlTable captureBufferTable
IETF_RS_232 (RFC 1659)	all synchronous and sdhc objects and tables rs232SyncPortTable
IETF_SNMPv2	sysORTable snmpTrap sysORLastChange
IETF_SNMP_COMMUNITY (RFC 2576)	snmpTargetAddrExtTable
IETF_SNMP_NOTIFICATION (RFC 2576)	snmpNotifyTable snmpNotifyFilterProfileTable snmpNotifyFilterTable
IETF_SNMP_PROXY (RFC 2573)	snmpProxyTable
IETF_SNMP_TARGET (RFC 2573)	snmpTargetAddrTable snmpTargetParamsTable snmpTargetSpinLock
IETF_SNMP_USER_BASED_SM (RFC 2574)	usmUser
IETF_SNMP_VIEW_BASED_ACM (RFC 2575)	vasmMIBViews

MIB Name	Unsupported MIB variables on All Platforms
NOVELL_IPX	ipxCircCompressState ipxCircCompressSlots ipxCircStaticStatus ipxCircCompressedSent ipxCircCompressedInitSent ipxCircCompressedRejectsSent ipxCircUncompressedSent ipxCircCompressedReceived ipxCircCompressedInitReceived ipxCircCompressedRejectsReceived ipxCircUncompressedReceived ipxCircNeighRouterName ipxCircNeighInternalNetNum

Unsupported MIB Variables—OmniSwitch 7000 series

MIB Name	Unsupported MIB Variables—OmniSwitch 7000 Series
AlcatelIND1Chassis	chasGlobalControl
AlcatelIND1Port	Alcether10GigTable
AlcatelIND1VlanManager	vlanTagMobilePortStatus
AlcatelIND1StackManager	alaStackMgrChassisTable alaStackMgrStatsTable alcatelIND1StackMgrMIBObjects

Unsupported MIB Variables—OmniSwitch 8800

MIB Name	Unsupported MIB Variables—OmniSwitch 8800
AlcatelIND1Chassis	chasGlobalControl
AlcatelIND1VlanManager	vlanTagMobilePortStatus
AlcatelIND1StackManager	alaStackMgrChassisTable alaStackMgrStatsTable alcatelIND1StackMgrMIBObjects

Unsupported MIB Variables—OmniSwitch 6600 Series

MIB Name	Unsupported MIB Variables—OmniSwitch 6600 Series
AlcatelIND1Bgp	alaBgpGlobal alaBgpPeerTable alaBgpAggrTable alaBgpNetworkTable alaBgpRedistRouteTable alaBgpRouteTable alaBgpPathTable alaBgpDampTable alaBgpRouteMapTable alaBgpAspathMatchListTable alaBgpAspathPriMatchListTable alaBgpPrefixMatchListTable alaBgpCommunityMatchListTable alaBgpCommunityPriMatchListTable alaBgpDebugTable
AlcatelIND1Dot1Q	qPortVlanForceTagInternal
AlcatelIND1Dvmp	alaDvmpGlobalConfig alaDvmpDebugConfig
AlcatelIND1Health	healthDeviceTemperatureCmmCpuLatest healthDeviceTemperatureCmmCpu1MinAvg healthDeviceTemperatureCmmCpu1HrAvg healthDeviceTemperatureCmmCpu1HrMax

MIB Name	Unsupported MIB Variables—OmniSwitch 6600 Series
AlcatelIND1Ipmm	alaIpmmDebugConfig
AlcatelIND1Ipms	alaIpmsForwardSrcIpAddr alaIpmsForwardSrcIfIndex
AlcatelIND1LAG	alcInkaggSlotTable
AlcatelIND1Port	esmPortCfgMaxFrameSize alcether10GigTable esmPortCfgLongEnable esmPortCfgRuntEnable esmPortCfgRuntSize
AlcatelIND1Pcam	alcatelIND1PCAMMIBObjects alaCoroL3HrePerModeTable alaCoroL3HrePerCoronadoStatsTable alaCoroL3HreChangeTable
AlcatelIND1Pism	alaPismGlobalConfig alaPismDebugConfig
AlcatelIND1QoS	alaQoSRuleReflexive alaQoSAppliedRuleReflexive alaQoSActionShared alaQoSActionSourceRewriteIpAddr alaQoSActionSourceRewriteIpAddrStatus alaQoSActionSourceRewriteIpMask alaQoSActionSourceRewriteNetworkGroup alaQoSActionSourceRewriteNetworkGroupStatus alaQoSActionDestinationRewriteIpAddr alaQoSActionDestinationRewriteIpAddrStatus alaQoSActionDestinationRewriteIpMask alaQoSActionDestinationRewriteNetworkGroup alaQoSActionDestinationRewriteNetworkGroupStatus alaQoSActionLoadBalanceGroup alaQoSActionLoadBalanceGroupStatus alaQoSAppliedActionShared alaQoSAppliedActionSourceRewriteIpAddr alaQoSAppliedActionSourceRewriteIpAddrStatus alaQoSAppliedActionSourceRewriteIpMask alaQoSAppliedActionSourceRewriteNetworkGroup alaQoSAppliedActionSourceRewriteNetworkGroupStatus alaQoSAppliedActionDestinationRewriteIpAddr alaQoSAppliedActionDestinationRewriteIpAddrStatus alaQoSAppliedActionDestinationRewriteIpMask alaQoSAppliedActionDestinationRewriteNetworkGroup alaQoSAppliedActionDestinationRewriteNetworkGroupStatus alaQoSAppliedActionLoadBalanceGroup alaQoSAppliedActionLoadBalanceGroupStatus alaQoSAppliedActionPermanentGatewayIpAddr alaQoSAppliedActionPermanentGatewayIpAddrStatus alaQoSAppliedActionAlternateGatewayIpAddr alaQoSAppliedActionAlternateGatewayIpAddrStatus alaQoSPortDefaultQueues alaQoSPortAppliedDefaultQueues alaQoSPortDefaultDSCP alaQoSPortPdiTable alaQoSslotPcamTable alaQoSPortProtocolTable alaQoSslotProtocolTable alaQoSslotDscpTable alaQoSConfigReflexiveTimeout alaQoSConfig alaQoSConfigNatTimeout

MIB Name	Unsupported MIB Variables—OmniSwitch 6600 Series	
AlcatelIND1Slb	slbFeature slbClusterTable slbServerTableg	
AlcatelIND1StackManager	alaStackMgrStatsTable	
AlcatelIND1VlanManager	vlanIpxNet vlanIpxEncap vlanIpxRipSapMode vlanIpxDelayTicks	vlanIpxStatus vlanSetIpxRouterCount vlanSetMultiRtrMacStatus
IETF_BGP4	bgp bgpPeerTable bgp4PathAttrTabl	
IETF_DVMRP_STD_DRAFT	dvmpScalar dvmpInterfaceTable dvmpNeighborTable	dvmpRouteTable dvmpRouteNextHopTable dvmpPruneTable
IETF_PIM	pim pimInterfaceTable pimNeighborTable pimIpMRRouteTable	pimIpMRRouteNextHopTable pimRPSetTable pimCandidateRPTTable pimComponentTable
IETF_TUNNEL (RFC 2667)	tunnelIfTable tunnelIfConfigTable	
IETF_IPMROUTE_STD	ipMRRoute ipMRRouteTable ipMRRouteNextHopTable	ipMRRouteInterfaceTable ipMRRouteBoundaryTable
NOVELL_IPX	ipxBasicSysTable ipxAdvSysTable ipxCircTable ipxDestTable ipxServTable	
NOVELL_RIPSAP	ripSysTable sapSysTable ripCircTable sapCircTable	

AVLAN Web Authentication

The Mac OS X 10.2.x is supported for AVLAN web authentication using JVM-v1.4.2

Fixed Problem Reports

The fixed problems listed here were reported by customers and fixed in this release.

Switch Management

Layer 2

PR 81286

After running a long capacity test, flows may not age out on an OS7000.

PR 84499

On an OS7000, configuring a static neighbor or a static member on a non-primary port of a link-aggregation might lead to unexpected flow duplications and membership registrations.

Layer 3

Basic IP Routing

Fixed Problem Reports

PR 83712

On the OS6600, the DHCP Offer from the DHCP server, may not be delivered to the UDP Relay application by Q-dispatcher.

PR 60070

The boot.cfg file can easily become large when configuring many QoS rules, actions, and conditions on the OS7000/8800. Currently, QoS can handle up to 4096 criterias to classify traffic and apply the QoS actions. However, the switch can not reboot properly when the boot.cfg has such a large QoS configuration.

Advanced Routing

OmniSwitch 7000 NIs

PR 62382

Under heavy traffic, if a remote switch is either reloaded or the backbone NI is reset, the WebView and telnet connection to this switch might hang and no access will be available until the sessions timeout.

OmniSwitch 8800 Feature Exceptions

Redundancy / Hot Swap

Fixed Problem Reports

PR 83682

When a Xenpak module is "hot-inserted" with the power applied to the board, the link sometimes does not come up.

PR 84365

After takeover, the status of NI remains DOWN if it got a message, "Time out waiting for ESM_ENI_RCVD_SLOTINFO", on the console on an OS6600.

PR 86033

Fpga or miniboot/bootrom upgrades are not supported on a dual CMM switch on the OS7000/8800.

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 Technical Support organization as soon as possible. Please contact customer support for updates on problem reports (PRs) where no known workaround was available at time of release.

Switch Management

Command Line Interface (CLI)

Problem Reports

PR 51249

The error message does not display the position of the errored keyword using "^" after one successful command on the OS7000.

Workaround: Exit and re-enter the telnet session, the first error message will show up with the position of the errored keyword.

PR 54887

Serial port information can be viewed from the WebView "Console Port Table" page, but not with CLI on the OS7000.

Workaround: Use WebView to reference console port information.

PR 55576

When doing a **config apply** command, applications may not appear to be loaded on the OS7000.

Workaround: Applications must be manually loaded before doing a **config apply**. Loading them automatically introduces many of problems that are not easily overcome.

PR 56593

Only one parameter can be modified when making changes to link aggregation on the OS7000.

Workaround: Execute the CLI command again for any further modifications.

PR 57355

With large image files, the zmodem (**rz**) CLI command will cause excessive "Bad CRC" errors and hang up after a few percentage of data transferring on the OS7000. It also will not allow the user to select a particular directory, such as /working or /certified, to download files to. It always downloads files to /flash only.

Workaround: There is no known workaround at this time.

PR 58437

A number or other variable value i.e. <num><string> will be erased if it is tabbed over on the OS7000.

Workaround: Do not "Tab" over entered variables.

PR 60688

The **debug bridge hash-bitmask** command displays incorrect help description such as "<slot/port>" instead of "<slot/slice>" on the OS7000.

Workaround: There is no known workaround at this time.

PR 69058

The **admin down** CLI command on an OS7-GNI-U2 or OS6-GNI-U2 port does not bring the link down on the remote end.

Workaround: Unplug the port.

PR 71993

The **show fabric** command will not work on Secondary CMM and will return an error message.

Workaround: There is no known workaround at this time.

PR 77445

The **write terminal** and **show configuration snapshot** output may be lost when using Windows 2000 telnet to connect to the switch.

Workaround: Use Unix, Windows NT, or Windows XP to connect to switch.

PR 80061

On the OS8800, error message "+++ [CLISHELL 22] Error on setting tty options at password (851971)" is displayed on the console during DoS attacks. The functionality of the switch is not affected.

Workaround: There is no known workaround at this time.

PR 83127

A DoS attack on port 23(Telnet) results in the message "[CLISHELL 32] Error on setting tty options at password(851971)" on an OS7000.

Workaround: Issue is cosmetic and doesn't effect performance of the switch.

PR 87022

Entering "debug command-info enable", enter the command info mode. Trying to exit that mode is impossible because the command "debug command-info disable" is not taking effect in command info mode.

Workaround: Exit from the session and then log on again.

RMON

Problem Reports

PR 55770

Duration and System Resources for RMON are not accessible via SNMP or WebView on the OS7000. The RMON subsystem only shows the values for these objects using CLI.

Workaround: There is no known workaround at this time.

PR 87876

If rows are rapidly added/deleted on the RMON history table, the switch may reload.

Workaround: There is no known workaround at this time.

SNMP

Problem Reports

PR 43837

Each time an SNMP v3 Manager "discovers" a new switch, the switch SNMP agent reports a "time stamp error" when answering the first v3 request on the OS7000.

Workaround: There is no known workaround at this time.

PR 50089/53442

When a GetNext request is sent on any object of the trapConfigTable, sessionConfigTable or trapFilterTable and if the index value equal to 4294967295, then the agent does not respond as expected; i.e. the object returned is not lexicographically larger on the OS7000.

Workaround: There is no known workaround at this time.

PR 50404

Our system treats user name "admin" differently from other user names. It is defined for our system with no SNMP access. This cannot be modified.

Workaround: There is no known workaround at this time.

PR 53289

Flood multicast changes on the OS7000 are applicable for all the ports in that slot.

Workaround: In order to change the flood multicast value, chose any ifIndex for that slot and change the value. The change will be applicable for all the ports in that slot.

PR 53817

Session Inactivity settings do not affect active sessions on the OS7000. Only new sessions will use the changed settings.

Workaround: Disconnect all active sessions and reconnect to the switch.

PR 79611

On the OS7000, the SNMP Agent does not respond to discover requests when the packet has an unknown user id.

Workaround: There is no known workaround at this time

PR 80197

On the OS7000, the SNMP Agent fails to increment snmpInASNParseErrs for PDUs with invalid ASN.1 BER encoding.

Workaround: There is no known workaround at this time.

PR 81409

On OS6600 series switches, the SNMP Agent fails to properly handle invalid msgID value.

Workaround: There is no known workaround at this time.

PR 81410

On OS6600 series switches, the SNMP Agent fails to properly handle out of range msgSecurityModel values.

Workaround: There is no known workaround at this time.

Web-Based Management (WebView)

Feature Exceptions

- WebView uses signed applets for the automatic IP reconfiguration. Those applets are signed using VeriSign Certificates that expire every year. The certificate used for Internet Explorer and Netscape expires every August. WebView users have to validate a warning indicating that the certificate used by the applet has expired.

Problem Reports

PR 53599

WebView session logout does not close a TCP port on the OS7000. The port stays in established state until the web browser is closed and restarted. A session timeout, a WebView logout, or a closure of the browser session does not cause the remote ports to close.

Workaround: Close the web browser and restart it.

PR 55346

Java Virtual Machine needs to be installed in order to use WebView for use of Java Applets in pages such as Health Home on the OS7000.

Workaround: If the Java Virtual Machine was not installed along with the browser, please install.

PR 56179

After a switch software update, sometimes WebView starts throwing javascript errors on the OS7000.

Workaround: Always clear the browser's cache, before trying the newer version of WebView.

PR 57944

A warning box appears on the Netscape browser when trying to telnet using HP-UX 11.0 or Sun Solaris' on the OS7000. This is due to missing or invalid telnet settings on the applications used by the browser.

Workaround: Update your telnet settings per the instructions below:

- 1 Click on the "Edit Menu" on the Netscape Browser and select "Preferences".
- 2 Select "Navigator" on the "Category" list located to the left of the "Preferences" dialog box.
- 3 If the "Navigator" category doesn't show subcategories (arrowhead to the left of the "Navigator" label is pointing to the right), then click on the arrowhead to extend the category (now the arrowhead will point downwards).
- 4 Select the "Applications" sub-category.
- 5 Look for the 'telnet' entry (under the Description column).
- 6 If there is none, click on the "New..." button below the select box, or select the 'telnet' entry and click on the "Edit..." button.

7 On the "Application" dialog box window, fill out the following [leave the rest empty and unselected]:

8 Description: telnet

9 Handled By: (select) Application: xterm -e telnet %h %p

10 Click OK to close each window.

11 Exit Netscape and Restart.

PR 58989

Sometimes, when a user tries to login via WebView, with the HTTP server on the switch accessed through an HTTP proxy server, the login page may be served back without an error message on the OS7000. This situation might happen because of different settings and behaviors on the proxy server.

Workaround: If possible, setup your browser to bypass the proxy server. If you cannot bypass the proxy server, then clear the browser cache and relogin again.

PR 59678

In Netscape, some home pages may display tables misaligned on the OS7000. This is due to Netscape browser having problems aligning tables even though they're coded to have the same alignment—this is true for all platforms.⁸

Workaround: Scroll down to view all tables.

PR 60192

Some WebView screens will not display if Internet Explorer 5.5 was installed without Java Virtual Machine (JVM) on the OS7000. Current screens affected are Physical-Health-Home, and System-FilesystemMgt-Install.

Workaround: Internet Explorer browser must be installed with Java Virtual Machine (JVM). After the installation of service pack 2 for Internet Explorer 5.5, WebView has successfully displayed the java applet, which is the file transfer applet in the System-FilesystemMgt-Instal page.

PR 60877

When the contents of the directory (WORKING or CERTIFIED) where the system boots up from are updated, the **WebView-System-FileSys-Images-Loaded** WebView command displays the new contents of the directory, not the version of the running system on the OS7000.

Workaround: The **show microcode loaded** CLI command displays the true status of the loaded software.

PR 61457

WebView brings the first paging table after the following event (refresh, delete, add and modify) on an OS7000.

Workaround: Use the next and the previous icon to go to another paging html page.

PR 61476

Certain long strings in the policy manager event table cannot be completely displayed using WebView on an OS6624/6648/7700/7800.

Workaround: View the display through CLI.

PR 63329

Some of the Modify pages in WebView lose their content when an error occurs and an error message is displayed below the title of the page on the OS7000.

Workaround: Close the modify window and re-modify again.

PR 63713

Sliding the mouse pointer over the menus located above the main viewing window in Webview will cause a garbling of the menu items.

Workaround: Refresh the view window and navigation bar together by clicking on the left hand menu icons. This will cause the navigation frame-set to reload and reset the menu items from the bad state. This bad state is reached by overload and subsequent dropping of DOM events in the browser.

PR 64271

Some WebView pages have "gray" buttons instead of "white" — so the button color is not consistent all throughout on an OS6624/6648. This is due to the limited support of CSS in UNIX Netscape 4.7*. There are also some differences (shading, border) among the buttons and this is due to the focus function of the buttons.

Workaround: This is a display issue only. Ignore the difference in color of the buttons. Gray buttons have no special meaning as opposed to white ones.

PR 65263

A JavaScript error may appear when a session is terminated by a method other than WebView on an OS6624/6648.

Workaround: This is a display issue only. Disregard any warnings / dialog boxes.

PR 66619

On the OS6600/OS8800, in WebView, Policy > Network Services > LDAP Servers page: after deleting an LDAP server, the entry might still be displayed after the table page has been refreshed although the server has actually been deleted.

Workaround: Please refresh manually the LDAP Servers page by clicking on the "Refresh" button located at the bottom of the page after the table before the "Help" button or by clicking again on the menu "LDAP Servers."

PR 68687

It is possible to see the ARP table empty in WebView, even though there are static routes.

Workaround: Click on the "Next" arrow found under the table. If this arrow appears under the table, this is an indication that there are static routes, but they might be on the next page.

PR 71023

For Security -> ASA -> End-User configuration, one may add ports that are not there.

Workaround: The maximum number of ports per slot are: 24 for OS7000/8800, and 52 for OS6624/6648.

PR 71434

When viewing files in System-SystemMgt-Install-ViewWorkingDir before acknowledging the security certificate, a Java error will occur on an OS6600.

Workaround: In this WebView path, wait for and acknowledge the security certificate before opening any popup windows.

PR 71484

On the OS7000, the Webview configuration dialog windows appear too low on the screen at resolutions less than 800x600.

Workaround: None. The least resolution that the Webview Configuration Manager supports comfortably is 800x600. While most browsers enforce bounds for new window pop-up browser windows so that they remain visible, graphics cards set at lower than recommended resolutions will result in poor browsing performance.

PR 71891

When adding an accept action on the OS7000 using the Actions > ACL page, if no SLB cluster is provided, the just added action will not show up on the Actions > ACL table. (However, it will be displayed in the Actions > All table.)

Workaround: Go to the Actions > All table.

PR 75312

If an external authentication server has a user name that's spelled exactly like another user that's local on the switch, the option link will still appear even though the switch authenticated through the external server.

Workaround: Use different user names.

PR 76783

When one clicks on the column header of a table with the SHIFT key held down, an empty browser window is opened up. This is because column headers are functionally HTML links, and the programmed browser behavior is to open up a link in a new browser window when the SHIFT key is held down.

Workaround: Don't hold down the SHIFT key when clicking on the column header.

PR 76949

With WebView, if you try to create an action for minimum bandwidth no error is generated.

Workaround: There is a warning message when action with min. bandwidth created from "Add QoS Action" screen, but not from "Add Action" screen on OS7000/8800.

PR 77106

User is randomly unable to relogin to Webview on Netscape 4.7x.

Workaround: Close browser and open a new window.

PR 77279

On the OS6000 in WebView Physical - Health - LED Status, information is incorrect in the table. There should not be two columns for the same module. The Physical Name contains unuseful data. The Primary CMM should say "Green On", the Temperature and the Fan should say "Green(OK)"

Workaround: Ignore the extra column and the Physical Name row. Use CLI for correct status of Primary/Secondary CMM, Temperature, and Fan.

PR 77528

On the OS6600/7000, LDAP Server entries on WebView show up with Authentication type 'None' instead of 'Simple Password' when configured from CLI with a user ID and password.

Workaround: Change the authentication to 'simple password' type on WebView when using a userID with Password.

PR 77638

On the OS7000, when running 'copy flash synchro' from WebView while the working and certified directories are not synchronized, Webview will report a successful operation even though it will show that it failed on the console.

Workaround: Make sure the working directory and certified directory is synchronized before running flash synchro.

PR 78032

On the OS7000, an error displays when clicking on a menu that doesn't have submenus before the home page is completely loaded.

Workaround: Wait until the home page is fully loaded, and then click on the menu for the selected table / page to view. [Currently, there is no way to detect from a browser (except IE—even then the function is not fully reliable) when a specific page is fully loaded in order to force a wait.] If an error displays, refresh by clicking on the left-hand side feature icon.

PR 78915

On the OS7700, the WebView session help does not explain that you must create the banner text file in the root /flash directory that holds the banner text.

Workaround: There is no known workaround at this time.

PR 79507

In the Health help pages for OS6600 switches, the hypertext link for OK1 is broken.

Workaround: There is no known workaround at this time.

PR 80209

WebView health port clear statistics will not clear slot 16 on an OS7000 full chassis.

Workaround: Please ignore old information.

PR 80236

The Remote System File Management page on OS6600 switches: Applying List Files doesn't display the directory contents in time due to the timing issue.

Workaround: It is required for a user to click the refresh button in order to see directory contents on the screen.

PR 80237

On the OS6600, in WebView Remote System File Management when deleting, the file won't automatically refresh the directory with the current content; it requires you to click the list button in order to see the updated directory contents. Also, there is a timing issue for "List File" which requires clicking the "Refresh" button more than once.

Workaround: There is no known workaround at this time.

PR 80249

On the OS7000, in Webview, some deeply nested navigation menus may be misplaced in the event that one scrolls down a scrollable feature homepage.

Workaround: Refresh the home page by clicking on the appropriate icon on the left navigation menu.

PR 80593

The drop-down menu in the Switch Log File page will not let a user select an option from the combo box for Session, Severity Level, Application ID in Netscape 7.0 on Solaris 2.8 on an OS8800.

Workaround: Use arrow key to scroll down the combo box and select an option.

PR 80851

On OS6600 series switches, WebView Remote System File Management doesn't check if the files exist.

Workaround: There is no known workaround at this time.

PR 80979

WebView Local Installation File Transfer from a floppy on Solaris 2.8 fails to read the diskette.

Workaround: There is no known workaround at this time.

PR 81067

WebView's Physical Modules Summary information does not sort the slot column data properly. WebView is using a numerical sort which is not ideal for data in this column. All slot data is displayed however.

Workaround: There is no known workaround at this time.

PR 81316

The Chassis Hardware Information page does not show the Firmware Revision on OS6600 chassis.

Workaround: There is no known workaround at this time.

PR 81424

In WebView, Physical > Health > LED Status page show LED off for fabric modules.

Workaround: There is no known workaround at this time.

PR 81464

Due to the Netscape browser's behavior, WebView Add IPX RIP/SAP Filter Help button is misaligned under the Restore button when the window isn't big enough to display all buttons in one line.

Workaround: There is no known workaround at this time.

PR 81817

The WebView Health help page for OS6600 switches does not have description for the Danger Limit and Hardware Board fields.

Workaround: There is no known workaround at this time.

PR 81893

On OS6600 series switches, in WebView, Policy > Policy > Conditions > Slot/Port Add and Modify pages: Port Group listbox displays items that don't exist on a switch.

Workaround: Ignore the items listed on the listbox that are not displayed In WebView, Policy > Policy > Groups > Port page.

PR 81940

Using the OS6600 stack WebView System File Management: Update: Bootrom when the current bootrom is of a different version and you quickly go to the primary switch console and enter the **show hardware info** command.

You'll get an endless loop of garbage characters. Now if you had waited say, a minute, and then did the above command on the primary switch console, you won't get this problem. Somehow, when using the CLI command **update bootrom bootrom.bin** and you quickly do **show hardware info**, the update process finishes first and then it will display the hardware information.

Workaround: On the secondary switch console, do a CLI command "takeover". Once the former primary switch is in idle mode, do a "reload all" from the secondary switch console. Now the OS6600 stack is functioning correctly.

PR 82009

On the OS7000, sometimes in the WebView physical adjacencies section, the right click on switch in map will not show connected IP addresses when Netscape 4.79 is used on Solaris.

Workaround: We recommend IE 6.0 or later, or Netscape7.0 on solaris.

PR 82075

WebView physical console port is showing 9 pin connector instead of Rj45 for the fiber version of the OS6600 switches.

Workaround: Please ignore. This is a cosmetic flaw. The console is RJ45.

PR 82309

On the OS7000, the virtual ospf interface status is not displayed in WebView.

Workaround: Use the CLI show ip ospf virtual-link command.

PR 82540

On the OS7000, in the WebView help page for VRRP Tracking there is no hypertext link for Admin Status and the Entity Type and Oper Status hypertext links and information sections need to be deleted.

Workaround: There is no known workaround at this time.

PR 82634

On an OS8800 chassis, WebView's Power Supply information page shows incorrect slot information.

Workaround: There is no known workaround at this time.

PR 82864

WebView > Physical > Ethernet > Interface Configuration > General modify page might not show the "Set Successful" message in Netscape 7.1.

Workaround: Ignore; whenever there is an error message, the modify page stays open automatically.

PR 82912

The WebView help main page does not necessarily display the correct chassis.

Workaround: There is no known workaround at this time.

PR 83005

WebView adjacencies shows multiple connections when a your link is a aggregate.

Workaround: There is no known workaround at this time.

PR 83131

During the phase of the Mutilate DoS script attack, the **show http** CLI command will cause the CLI console to hang. The CLI console will resume working once the attack is finished.

Workaround: There is no known workaround at this time.

PR 83402

On the OS7000, the title for the VRRP Delay help page says VRRP Global Parameters instead of VRRP Delay.

Workaround: There is no known workaround at this time.

PR 83794

Menu corruption may occur when selecting VLAN Management Binding Rules under Netscape. The menu may appear in the middle of the tabular display.

Workaround: Use Internet Explorer 6.

PR 83810

Resizing the Netscape 4.79 browser window with WebView displayed on an OS7000 may not force a reload of the Webview page under Solaris 2.9.

Workaround: Try Mozilla 1.4 or Netscape 7.1 on Solaris or use a Windows based system at this time.

PR 83829

Whenever you access a WebView page through the browser history list after logging into an OS7000, the page accessed will display without the usual control frames.

Workaround: Refrain from using the history list. ("Site Map" page is available from each home page containing direct links to table and configuration pages)

PR 84031

WebView's "Reload On" function for the OS6600 does not function according to specification.

Workaround: There is no known workaround at this time.

PR 84035

Webview allows more than 8 hex characters to be entered and may scramble the network number when applied for IPX VLANs.

Workaround: Only enter 8 hex characters at this time.

PR 84048

The WebView physical expansion modules help on OS6600 switches does not describe inline (i.e., PoE) parameters.

Workaround: There is no known workaround at this time.

PR 84051

In WebView's Network Interfaces display, there is no warning popup message when reloading an NI on the OS6600.

Workaround: Be aware that reloading an NI may disconnect network services until the NI has reloaded.

PR 84052

WebView allows the user to try and reload network interfaces on OS7000/8800 chassis.

Workaround: There is no workaround at this time. The switch will report an error when attempting to reload the network interface so there is no harm done. The option to reload network interfaces on the OS8800 and OS7000 Series chassis' will be removed in future builds.

PR 84091

WebView > Layer 2 > Vlan Mgmt > Vlan Configuration > Port-MAC Multicast MAC Addresses menu option is not supported on the OS6600.

Workaround: Ignore.

PR 84151

With WebView on an OS6600 chassis, the Expanded View at the bottom of the VLAN Configuration/VLAN table may refresh back to the Summary View instead of intended Expanded View when using Netscape 4.79 on Solaris 2.9.

Workaround: Try Mozilla 1.4 or Netscape 7.1 on Solaris or use a Windows based system at this time.

PR 84250

In WebView, on the Physical > Health > Device page, the CMM Temperature might read 0 degrees Celsius. This feature might not be supported.

Workaround: Please ignore the zero.

PR 84255

When doing multiple modifications on an OS7000, such as Layer 2 > Vlan Mgmt > VLAN Configuration > Ports > Port Association > Move Ports, Only the first 64 ports of the entire selection will be associated. A WebView dialog box comes up indicating that only the first 64 will be applied with the choice of proceeding or cancelling.

Workaround: There is a design limitation, which allows only 64 entries to be modified at a time.

PR 84268

There are multiple bad hypertext links in the WebView help pages for Ethernet Accounting Input Statistics and Ethernet Accounting Output Statistics whereby links will incorrectly take you from one help page to the other.

Workaround: Do not use the hyperlinks. Please use the scroll bar.

PR 84269

There are multiple bad hypertext links in the WebView help pages for Ethernet Accounting Output Statistics and Ethernet Accounting Input Statistics, whereby links will incorrectly take you from one help page to the other.

Workaround: None.

PR 84270

Webview's UDP Relay Association page only allows a maximum of 3 entries on an OS7000.

Workaround: All services are displayed via CLI.

PR 84281

WebView's sort button may disappear on longer pages.

Workaround: There is no known workaround at this time.

PR 84338

Out-of-range value for "Session ID" such as 9999999999, a new entry is successfully created with the upper boundary number (2147483647) instead of retaining the out-of-range entered value and displaying an out-of-range error.

Workaround: Please enter a value within the correct range to avoid this problem.

PR 84416

On the OS7000, the "Addressless IP" section in the WebView OSPF Area Interfaces help page needs to be removed since there is no such field.

Workaround: Ignore the field.

PR 84423

In WebView, on the Physical > Ethernet > Interface Configuration > General Modify Slot window, the Runt Size boundary is 0 - 6 bytes instead of 0 - 64 bytes.

Workaround: Use the Modify Multiple, select entire slot (use <Ctrl> or <Shift> key), and change Runt Size.

PR 84438

The main WebView help page does not list the Adjacencies feature in the Physical Group, the Port Security feature in the Layer 2 Group, or the Port-Based NAC feature in the Security Group.

Workaround: There is no known workaround at this time.

PR 84528

The WebView help pages for the Console Port incorrectly say that the Input/Output states are None, Enabled, and Disabled when in reality the states are None, ON, and OFF.

Workaround: There is no known workaround at this time.

PR 84616

When changing spanning tree bridge modes using CLI while WebView Spanning Tree menu has already loaded, the menu might not correspond to the correct mode even though when refreshing the home page the correct mode is displayed.

Workaround: Click on the Spanning Tree icon at the Outlook-like-bar located the left of the screen to refresh the menu to the current mode.

PR 84618

On Policy > Policy > Ports Modify window, whenever trying to make a change it returns the error message, "Port enable/disable is not supported."

Workaround: Manually set "Enabled" field to a blank during modification and continue with the rest of the changes.

PR 84626

WebView's Adjacencies icon has non-consistent background color.

Workaround: This is a Display Issue only.

PR 84634

The WebView System File and Local Installation Management help pages for OS6600 switches document an Update feature.

Workaround: Please ignore. The update is only available for OS7000/8800.

PR 84635

WebView may sort some numerical columns incorrectly. For example, the HRE tables and sorting by the firmware revision.

Workaround: There is no known workaround at this time.

PR 84663

On the OS6600, the WebView IP EMP Routes page has no help page.

Workaround: There is no known workaround at this time.

PR 84721

Garbage characters "NaN" shows up above the File Operations section in System File Management on OS8800.

Workaround: Ignore the garbage character, they are cosmetic.

PR 84780

On the OS8800, in WebView, Physical > Ethernet > Interface Configuration > General "Modify" window might display a "Set operation finished successfully!" message and the changes not made to the table.

Workaround: Use the "Multiple Modify" window and select the desired slot/port to perform the changes.

PR 87494

On the OS6800, by default the BPDU Switching is disabled and the WebView page "Spanning Tree One to One Bridge Parameters" displays an empty field. Only if a user modifies the bridge parameters and sets the BPDU Switching to Enable or Disable the values will be displayed in the table.

Workaround: If the BPDU Switching field is empty, please treat it as disabled.

Layer 2

802.1Q

Problem Reports

PR 37415

The OS7000 frame parser does not recognize Token Ring or FDDI SNAP frames with 802.1Q encapsulation. If the parser encounters these frames, they are misclassified as flood frames.

Workaround: There is no known workaround at this time.

PR 72541

The OmniCore does not support hybrid VLANs where tagged and untagged frames are present. A port must be tagged to add it to multiple VLANs. From that point forward, it will drop all untagged frames. This is only a problem when connected to the OS7000 that has the default VLAN on the switch in use and that port is connected to a tagged port on an OmniCore. The OS7000 will not be able to talk to the OmniCore on the default VLAN on that port.

Workaround: Make the default VLAN on a port connected to an OmniCore an unused VLAN. This will cause all the frames coming out of the OS7000 be tagged, and it will also accept all the tagged frames coming from the OmniCore.

PR 78486

CLI `debug 802.1q <slot/port>` command on an OS8800 10G port does not display hw port info for all the internal aggregate ports.

Workaround: There is no known workaround at this time.

Bridging

Problem Reports

PR 84343

Under certain large IP configurations, occasionally a few ports can remain inactive upon bootup on an OS8800.

Workaround: Admin down/up the port.

PR 84353

Ethernet tab -> Interface Configuration -> General -> Modify (select an interface first).

Title: Modify Ethernet Network Interface

1. It accepts an invalid value such as -2 without an ERROR message.
2. The input rate is adjusted to the best value for the switch.

Workaround: 1. Do not put invalid values. 2. It is not a critical issue. (The System finds the best values for the switch.)

PR 86084

The configuration file from 5.1.4 or older releases is not be compatible for autonegotiation if either speed or duplex is set to non-auto.

On such releases, autonegotiation was automatically disabled and saved in the boot.cfg configuration file.

Workaround: Enable autonegotiation and save the config

PR 87050

On the OS6000, after a takeover, the "show health" command may not always display correct information for all slots.

Workaround: There is no known workaround at this time.

PR 88037

On the OS6600, after multiple takeovers, part of the traffic might be flooded in the associated vlan.

Workaround: Flush the mac address table (no mac-address-table learned).

Flow Control**Problem Reports**

PR 38896

Clause 31 of the IEEE 802.3 Specifications specifies a MAC Control Frame format consisting of Destination Address, Source Address, Type, MAC Control Opcode and Reserved (PAD) field. The MAC Control Frames are transmitted correctly as specified by the standard. However, during receive, operation checks for the validity of all the fields as specified in the standard, except the 'reserve' field which is specified as all 'zeroes' on the OS7000.

Workaround: There is no known workaround at this time.

PR 54096

The ESM driver does not return a pause frame when traffic exceeds 100% into the port on the OS7000.

Workaround: There is no known workaround at this time.

PR 56817

The Rx Pause Frame counter does not increment when there is an incoming PAUSE frame on an OS7000/8800.

Workaround: There is no known workaround at this time.

Interswitch Protocols (AMAP/GMAP)

Problem Reports

PR 80256

AOS switches are not forwarding AMAP hello packets when AMAP is disabled.

Workaround: There is no known workaround at this time.

IP Multicast Switching (IPMS)

Problem Reports

PR 57746

IP Multicast does not support hardware routing with 802.1Q service on the OS7000.

Workaround: There is no known workaround at this time.

PR 59814

If a multicast routing interface is "Oper-Status" enabled, not just "Admin-Status" enabled, then IPMS will not be enabled silently on the OS7000. When the first multicast routing interface moves to the "enabled" state, IPMS will be enabled silently.

Workaround: There is no known workaround at this time.

PR 59907

If IP multicast switching is configured along with group mobility, and multiple clients are configured in different IP VLANs on the same physical port, multiple copies of the same packet can be routed to that port causing duplicate delivery of IP multicast traffic on the OS7000. Note: IP multicast routing must also be enabled, and multiple clients in different subnets must request the IP multicast traffic from the same physical port.

Workaround: The CLI command **ip multicast hardware-routing** may be used to remedy this problem. This will ensure that only one copy of the packet will be forwarded out any switch port. Please see restrictions in using ip multicast hardware routing in the user manual. Note: The route selected for transmitting the multicast to the port will be selected randomly which may cause problems with TTL threshold and multicast scoping.

PR 61590

If one (1) Gb/s multicast traffic, composed of one or several streams, is sent on only one port per EGRESS NI on the OS7000, wire rate is not achieved. The speed is limited to around 600Mb/s whatever the packet size.

Workaround: There is no known workaround at this time.

PR 69039

Cannot achieve wire rate multicast performance between stack elements on an OS6624/6648. Standalone performance is wire rate.

Workaround: There is no known workaround at this time.

PR 72334

IPMS may not learn all flows if flooded with many new flows in a short period of time. Flows will flood during learning process.

Workaround: Retry joining multicast group again.

PR 75172

On the OS7000, IGMP memberships may be lost if the hosts reside on the NI having high CPU utilization.

Workaround: There is no known workaround at this time.

PR 77650

On the OS7000, IPMS doesn't allow for the configuration of static entities for link aggregation trunks by trunk number.

Workaround: Link aggregation trunks can be configured instead by specifying the primary port of the link aggregate group.

PR 80143

Windows IGMPv1 clients do not respond to IPMS queries on an OS7000.

Workaround: There is no known workaround at this time.

PR 81111

On the OS8800, IPMS routes packets through the 10Gig NI in software only, even to untagged ports. Hardware forwarding is only available for bridged traffic over the 10Gig NI. As a result multicast routing performance is greatly reduced.

Workaround: There is no known workaround at this time.

PR 83680

When a mirroring port is configured on an OS6600, IP multicast traffic may temporarily be disabled until the various information is relearned on the mirroring and mirrored ports.

Workaround: There is no known workaround at this time.

PR 83721

When a 'proxy version' is configured to V3 on an OS7000, 'default' itself is changed to 'V3'. Hence CLI is saying 'V3' when it says 'default' after 'proxy version' is configured to 'V3'. This can be verified by invoking **show ip multicast switching** through CLI.

Workaround: There is no known workaround at this time.

PR 83765

IPMS does not perform IGMPv3 Include/Exclude filtering on a per VLAN basis on an OS7000.

Workaround: There is no known workaround at this time.

PR 83965

CLI and WebView do not allow configuration of "Last Member Query Interval" on an OS800.

Workaround: It can be configured through SNMP object `igmpInterfaceLastMembQueryIntvl`.

PR 83992

The `igmpInterfaceStatus` value can not be set through CLI or WebView on an OS7000.

Workaround: IGMP enable/disable is not supported per VLAN interface, though it is supported per router. Though setting `igmpInterfaceStatus` through SNMP succeeds, the router's interface configuration does not change.

PR 83996

Query Max Response Time can not be set through CLI or WebView on an OS7000.

Workaround: This can be set through SNMP variable `igmpInterfaceQueryMaxResponseTime`.

PR 84009

It is not possible to configure an interface as IGMPv1 through the CLI or WebView on an OS7000.

Workaround: Configure an interface as IGMPv1 through SNMP.

PR 84642

On the OS8800, static neighbors/queriers/members may have problems being applied to 10 Gig ports. The static neighbor/querier/member command applies to the actual underlying port and does not map to the underlying link aggregation instance.

Workaround: Apply the static neighbor/querier/member command to the underlying primary port of the link aggregate instance.

Learned Port Security

Problem Reports

PR 71412

When Learned Port Security is configured on an OS6624/6648, traffic gets flooded until MAC addresses are learned.

Workaround: Directly create the objects in an active state. Thereby, bypassing this problem by previously configuring together both sides of the static aggregates, with aggregation set "disable". Thus, the "admin state" must be set to "disable" just after the creation. When the whole configuration is ready, set the admin state to "enable" such it is by default. There is also the possibility of setting down/up ports. Thus interfaces could be also set admin "down/up" before everything is ready.

PR 73953

With an LPS (Learned Port Security) configuration set to only allow a specific MAC on a port and when the port receives non-authorized traffic (ARP requests), the MAC info shows that the unauthorized host is in a "filtering" state hence all traffic should be filtered. However the ARP table learns the ARP entry for the filtered host. ARPs should not be learned for "filtered" hosts.

Workaround: There is no known workaround at this time.

PR 80776

On OS6600 series switches, after the port is in violated mode, changing the violation option to shutdown does not take effect operationally.

Workaround: Please do not change the violation option once the port is already in violated state. Instead change the port's LPS state to disabled and then apply the new violation option and again enable the LPS on the port.

Link Aggregation (including OmniChannel)

Feature Exceptions

- OS7000: Please refer to the Link Aggregation chapters of the *OmniSwitch 7700/7800/8800 Network Configuration Guide*, which include instructions for optimizing first-generation Network Interface modules for link aggregation.
 - OS6600—Static link aggregation: Single aggregate group can have 16 ports in a stack as long as no more than 8 ports are added on a single switch. The ports must be assigned sequentially and the first port configured must begin with port number 1, 9, 17, or 25 on a 6624 or 1, 9, 17, 25, 33, 41, 49 or 51 on a 6648. The ports on different switches (NIs) can be in the same aggregate group. The ports should be with the same speed. The flow of traffic will be such that it goes out from the closest linkagg port.
 - For more information, please send an email to support@ind.alcatel.com.
-

Problem Reports

PR 61641

The OS7000 switch with static link aggregation configured and connected to several simple ports could lock up if the flooding traffic is immediately opened before configuring the necessary opposite aggregate on the remote side.

Workaround: Directly create the objects in an active state. Thereby, bypassing this problem by previously configuring together both sides of the static aggregates, with aggregation set "disable". Thus, the "admin state" must be set to "disable" just after the creation. When the whole configuration is ready, set the admin state to "enable" such it is by default. There is also the possibility of setting down/up ports. Thus interfaces could be also set admin "down/up" before everything is ready.

PR 65519

Modifying the LACP Actor Admin Key for consecutive ports is allowed by CLI and SNMP on an OS6624/6648.

Workaround: Modification can be done by taking one port at a time.

PR 67598

Link aggregate on GIG uplinks occasionally fails to load balance traffic on an OS6624/6648.

Workaround: There is no known workaround at this time.

PR 70779

Dynamic link aggregation over 802.1q on the OmniSwitch 8800 does not work with Cisco Cat 6509.

Workaround: There is no known workaround at this time.

PR 70920

There will be a warning message displayed when you create multiple system priorities in the same range for Link Aggregation on an OS6624/6648.

Workaround: The system priorities should be the same.

PR 72619

On the OS8800, sending continuous wire rate traffic over dynamic link aggregation over extended periods of time, results in traffic loss over link aggregation.

Workaround: Increase the mac-aging time out with such a stress configuration. Using static link aggregation will also prevent this problem.

PR 74071

On the OS6600, Dynamic link aggregated ports may go down after a takeover.

Workaround: There is no known workaround at this time.

PR 74223

Link aggregation is not supported on 2 Gigabit ports located on two separated gigabit uplinks on an OS6624/6648. The unit is considered as "1 slot" but the two gigabit uplinks are linked to two separated ASICS. "The ports of the linkagg can not be in two different asics in the same slot".

Workaround: There is no known workaround at this time.

PR 75520

With multiple dynamic link aggregates on the OmniSwitch 8800, each aggregate should have an admin key which matches the port's admin key.

Workaround: Specify the admin key for the link aggregate and the port.

PR 75538

On the OS6600 series switches, not able to change dynamic Linkagg Parameters on run time.

Workaround: Delete the linkagg lacp port and add with new modified parameters.

PR 77684

On the OS7000, replacing second generation NIs with first generation NIs causes ports not to come up.

Workaround: If second generation boards are hotswapped with first generation boards, some linkagg ports may not come up. Replace second generation interfaces with second generation interfaces only.

PR 77693

On the OS7000, Not able to pass traffic through a linkagg if the traffic is originated from the same slice as linkagg.

Workaround: Do not use same NI port to pass the bridged traffic through the same slice ports configured as linkagg.

PR 78281

If second generation NI ports come up first, cannot add first generation NI ports to the same aggregate.

Workaround: When configuring mixed NI version ports in the same agg, make sure first generation ports added first before adding second generation ports.

PR 78374

After hotswapping a second generation NI with a first generation NI, spanning tree detects a misconfiguration.

Workaround: Do not hot swap a second generation board with first generation board, if linkagg is configured across multiple boards.

PR 78752

On the OS6600 series switches, deleting actor system id on lacp port makes the display set to all Zero.

Workaround: LACP port needs to set with a non Zero system id else, the default system id will be used. Delete the port and add again to use the default system id.

PR 78804

On OS6600 series switches, changing LACP parameters on runtime affects the LACP mechanism.

Workaround: Don't change LACP port parameters on run time. If modification needed, delete and add the port again

PR 78909

On OS8800 switches, once second-generation NI port added to a linkagg, cannot add first-generation NI port.

Workaround: Add first generation NI port first then add subsequent second generation ports, else add them in boot.cfg and reboot.

PR 78945

Cannot add more than 14 linkagg with size 8.

Workaround: The limitation documentation is modified with correct numbers for OS7000/8800. Refer to the limitation document for the exact numbers.

PR 79116

On the OmniSwitch 6624/6648, LACP port priority is not supported. The port priorities do not control the order of the ports joining the aggregate.

Workaround: Do not configure port priorities.

PR 79204

On the OS7000, the LACP system priority and port priority doesn't have any effect on ports joining the aggregate

Workaround: Do not use port priority and system priority values in LACP as a selection criteria, these are needed for compatibility issues.

PR 79829

On the OS7000, LACP parameters cannot be modified on run time.

Workaround: Delete the port and add when and if LACP parameters have to be changed.

PR 80033

On the OS7000, if second generation NI port comes up, then first generation NI port doesn't join.

Workaround: When configuring mixed version NI ports, make sure first generation ports are configured first then second generation ports are configured.

PR 80908

On the OS7000, the **linkagg eni dedicated enable/disable** command gives an error.

Workaround: This command is not supported any more. No need to use this command.

PR 80995

On the OS8800, on takeover some NI (with linkagg configured) may not get reset.

Workaround: Do not hotswap second generation boards with first generation boards.

PR 81061

If second generation ports are added first to an linkagg then first generation ports added, error message gets displayed.

Workaround: Add first generation ports first then add second generation ports when using CLI.

PR 81288

On the OS7000, enabling backpressure command stop LACP packets being exchanged.

Workaround: Do not run this command with LACP configured.

PR 81416

On the OS7000, changing LACP values on run time makes the ports not join the linkagg.

Workaround: Do not change LACP values on the run time. If needed delete the port and add again to make a modification.

PR 81531

On OS6600 series switches, sometimes multicast flow stops when linkagg ports are added and deleted multiple times.

Workaround: There is no known workaround at this time.

PR 81650

When LACP ports with misconfiguration connected to an LACP ports which sends LACP pdus, the LACP pdus parameters can make port join a wrong a linkagg.

Workaround: When configuring LACP values, make sure that each end of the linkagg is configured properly.

PR 81722

If more ports are configured than the actual linkagg size, some or all ports may not join the dynamic link aggregate.

Workaround: Do not configure more ports than the actual linkagg size.

PR 81736

On OS8800 switches, when more linkagg ports with same configuration than the size of the linkagg, when any of active port goes down the non-joining ports do not join the aggregate.

Workaround: Do not configure more ports than the actual linkagg size.

PR 81937

With optimization enabled command, its impossible to delete a port from linkagg.

Workaround: Disable optimization command to delete the ports from linkagg. and re-enable the optimization command.

PR 81985

On the OS8800, LACP ports do not join the aggregate if some of the ports are administratively down.

Workaround: If the ports needs to administratively down and if they are part of LACP linkagg, remove the ports from LACP and add them again when they admin up.

PR 84225

On an OS7000, multiple linkagg on the same VLAN should be on the same flooding mode if optimization is enabled, to pass bridging traffic between them.

Workaround: Do not create mixed mode linkagg ports in the same Slice.

PR 84437

On OS8800 first-generation NI modules, there could be mac movement across the link aggregation ports and the user ports.

Workaround: Enable the optimization mode on link aggregation modules.

Port Mirroring**Feature Exceptions**

- On OS6600 switches, Port Mirroring is not supported across a stack, i.e. mirrored port on slot 1 and mirroring port on slot 4.
 - On an OS6648, port mirroring is not supported between lower ports (Fast Ethernet port 1-24 or Gigabit Ethernet port 51-52) and upper port (Fast Ethernet port 25-48 or Gigabit Ethernet port 49-50).
 - On an OS6602-48, port mirroring is not supported between lower ports (Fast Ethernet port 1-24 or Gigabit Ethernet port 51-52) and upper port (Fast Ethernet port 25-48).
 - When port mirroring is enabled on OS7000/8800 Gigabit modules, Egress mirror performance is 1330974 p/s.
 - When port mirroring is enabled on an OS8-GNI-C24, Egress mirror performance is 1430792 p/s.
-

Problem Reports

PR 35206

The reQid packet delivery is unreliable if Qid has problems on the OS7000. It affects port mirroring. The port mirroring feature may display frames that were received by the switch but never set out because the queue was already full.

Workaround: There is no known workaround at this time.

PR 66806/66847

Packets are mirrored only if the hardware is programmed on an OS6624/6648. During the learning process, the hardware is not yet programmed. Under heavy traffic not all packets will be mirrored.

Workaround: There is no known workaround at this time.

PR 66845

The mirroring (destination) port on the OS8800 gets one frame extra with 'Unknown SA and Known DA' Egress traffic on Mirrored port

Workaround: Use second generation modules.

PR 66862

Port mirroring is not supported across the stack. Please note that you cannot do port mirroring between upper and lower 24 ports on an OS6648.

Workaround: There is no known workaround at this time.

PR 68515

Performance of port mirroring is around 3000 packets/second after a hot swap on the OmniSwitch 8800.

Workaround: There is no known workaround at this time.

PR 69612

On the OS7000, the mirrorConfigError' trap parameters have incorrect data type COUNTER32 instead of INTEGER.

Workaround: There is no known workaround at this time.

PR 69613

The mirrorUnlikeNi' trap parameters have incorrect data type COUNTER32 instead of INTEGER.

Workaround: There is no known workaround at this time.

PR 71793

Port mirroring is not at wire rate. The mirrored port will drop traffic when port mirroring is enabled on the OS7000.

Workaround: There is no known workaround at this time.

PR 72891

On the OS7000, egress port mirroring rate is less than 1Gbps for GNI_C12 modules when the link speed is 1G.

Workaround: There is no known workaround at this time.

PR 77036

There is high performance degradation for port mirroring in OS8-GNI-C8.

Workaround: There is no known workaround at this time.

PR 78852

There is some performance degradation from 1488095pkts/s to 975134pkts/sec in OS8-GNI-U24.

Workaround: There is no known workaround at this time.

PR 79329

There is some performance degradation (from 1,488,095 p/s to 1,333,624 p/s) on Egress (outport) Port Mirroring. OS8-GNI-U24.

Workaround: There is no known workaround at this time.

PR 80242

Unable to modify the in/out port mirroring session using the default port mirroring command on the OS7000. Direction of mirroring takes previous value when modify command is entered.

Workaround: Specify the direction explicitly in the modify command.

PR 81038

Ingress flood traffic is seen on Mirroring port in case of Outport Mirroring on an OS7000 port.

Workaround: There is no known workaround at this time.

PR 81133

On the OS7000, when there are multiple mirror sessions on same second generation NI, with the mirrored ports belonging to different default Vlans and Mirroring port is on first generation NI, Double tagged frame can result when ports are tagged and traffic is also tagged.

Workaround: If multiple mirrored (source) ports on the same second generation NI belong to the same default VLAN this problem won't happen.

PR 83302

Configuring four mirroring sessions on an OS7000 first-generation module causes performance degradation even when one inport traffic was passing.

Workaround: There is no known workaround at this time.

PR 84093

In case of Many-To-One mirroring on an OS7000, the traffic coming in on other mirrored ports, tagging rules on mirroring port might make the packet go out tagged even if it came in untagged.

Workaround: There is no known workaround at this time.

PR 84285

On an OS8800, the mirroring port still shows the state "mirror" and remains blocking even after deleting the Many-To-One port mirroring sessions with different default VLAN.

Workaround: There is no known workaround at this time.

Source Learning

Feature Exceptions

- The number of MAC addresses supported on an OS6600 is 8K.
-

Problem Reports

PR 53663

MAC load balancing does not spread out the MACs among 4 ports on the OS7000.

Workaround: There is no known workaround at this time.

PR 54930

The CLI command **show mac-address-table count** does not have an equivalent in SNMP or WebView on the OS7000.

Workaround: There is no known workaround at this time.

PR 57013

Boot.cfg only changes the age-time value for VLAN1 on the OS7000 although its been configured for all the VLANs.

Workaround: The user should specify the VLAN information while configuring aging time for MAC address table in the boot.cfg, like: mac-address-table aging-time 1000000 VLAN 2.

PR 57976

All MACs age out when a cable is pulled and re-inserted after traffic is stopped during Source Learning on the OS7000. Spanning Tree recalculates and flashes all MACs belonging to the same VLAN as the cable is re-inserted.

Workaround: Make the port being unplugged an "edge port". Spanning tree will ignore the re-insertion event and not flash out all MACs learned.

PR 59745

Due to the time required for the aging check, the aging-time is not very accurate for small measures of time i.e. under 1 minute on the OS7000.

Workaround: There is no known workaround at this time.

PR 64506

When the amount of Macs on an OS6624/6648 switch reaches 85% of 16K, the fast aging mechanism will start to age out all of the Macs faster.

Workaround: There is no known workaround at this time.

PR 68045

ARP replies are sent best effort on an OS6624/6648. This might possibly result in a loss of ARP resolution on adjacent switches while routing over links experiencing sustained congestion.

Workaround: On the adjacent device, add a static ARP entry for the MAC address / IP address of the routing instance.

PR 68052

Link aggregation and Learned Port Security should not be configured on the same port on the OS7000. Presently the switch lets the user configure both on the same port.

Workaround: There is no known workaround at this time.

PR 68780

MAC addresses are learned at a very slow pace after a takeover on an OS6624/6648 during heavy load conditions. Full traffic recovery takes about 15 minutes.

Workaround: There is no known workaround at this time.

PR 69257

Unable to view statically assigned source MAC address in table.

Workaround: The command line interface displays these values just fine and all entries created with Webview can be verified via a telnet session.

PR 72646

On the OS7000/8800, the MAC is learned on the port wherever the MAC is seen on a Link Aggregate port because the NI does not have Link Aggregation concept at ingress side. So the MAC is already learned on the port which this MAC is seen on.

Workaround: There is no known workaround at this time.

PR 74790

There is a limit to the number of protocols that can be processed efficiently on a single mobile port.

Workaround: Limit protocol-based mobility rules, protocol rule, port-protocol rule, or MAC-port-protocol rule, to 5 different protocols per port.

PR 76491

The aging process in the case of disabled vlans is not the same on OS6600 as it is on OS7000 and OS8000 switches. This is due to the architectural difference between the software running in those switches.

Workaround: There is no known workaround at this time.

PR 80435

On the OS8800, if you change the protocol to 1W in the Root switch first, chances are the root switch would still receive 1D BPDUs from other switches, causing the root switch to revert back to 1D. There's nothing we can do here.

Workaround: Please change the protocol on the non-root switches first and then do the root switch last.

PR 84694

On an OS6600, some of the mac-addresses (learned across the link aggregate ports) are not flushed completely, even after passing the aging-timeout value (set for that VLAN).

Workaround: There is no known workaround at this time.

PR 84695

On an OS6600, even after configuring a permanent MAC address for a linkagg port, the address is learned as a dynamic MAC address.

Workaround: There is no known workaround at this time.

Spanning Tree

Problem Reports

PR 61259

The 802.1Q Spanning Tree (also called Multiple Spanning Tree) is a proprietary protocol based on tagging BPDU. As a consequence, the OS7000 Spanning Tree is not compatible with other vendors' Spanning Tree.

Workaround: In order to inter-operate with Spanning Tree from other vendors (802.1d,802.1w and 802.1s), the Spanning Tree of the OS7000 must be configured in Flat mode.

PR 62244

During a takeover, some over processing on the NI side may prevent the switch (root bridge) to forward its BPDU on the OS7000/8800. In such a case, the max age timer may trigger on the switch closest to the root bridge, generating a Topology change. After the over processing burst, everything returns to the initial state.

Workaround: There is no known workaround at this time.

PR 64668

Spanning Tree may bounce because there are too many Spanning Tree instances attached to the port on the OS7000.

Workaround: If more than 256 VLANs require a Spanning Tree, the switch must be configured in flat mode (Spanning tree per VLAN is inactivated).

PR 65465

Changing any Spanning Tree parameter on a port for VLAN 1, when VLAN 1 is tagged for that port, is not applied during the execution of the initial configuration file (boot.cfg) on the OS7000/8800.

Workaround: Do not use VLAN 1 as a 'tagged' VLAN.

PR 66521

If a local OS7000 port is configured to use 802.1W and a remote OS7000 port is configured to use 802.1D, then migrate times on the local port prevents the use of 802.1D bpdus and a loop is created for 2 seconds.

Workaround: There is no known workaround at this time.

PR 67917

Sometimes, a Listening/Learning state can be observed during a spanning tree topology change (change of the Root port) on the OS7000/8800.

Workaround: There is no known workaround at this time.

PR 68476

The mirroring port is blocked by the spanning tree after the module hot swapping procedure on an OS6624/6648.

Workaround: There is no known workaround at this time.

PR 74365

If a port on an OS7000 or OS6600 is connected to another port that is Blocked/Alternate, then this port might not receive any BPDU from the Blocked port in order to figure out the 'Next Best Root' port. So the **show spantree x** command for this switch will not show the 'Next Best Root' port. (Note that this information is provided to be compatible with the XOS products and is not needed to compute spanning tree topology)

Workaround: Try disconnecting/reconnecting the link so BPDUs may be exchanged through these ports.

PR 76688

Path cost of 0 is mistakenly allowed to configure a port on the OS7000.

Workaround: Do not use path cost 0.

PR 76951

'Show Spantree' command still displays some values in the 'Path Cost', 'Op Cnx', and 'Designated Bridge ID' columns for a port when it is down.

Workaround: If the port's 'Operating Status' Column shows DIS (for disabled), just ignore the values for the rest of other columns. These values are being displayed to show the past connection history of the path cost, connection type and Bridge ID etc.

PR 77228

When running scripts using automation tools to configure an OS7000 from 1d protocol to 1w, the STP seems to be stuck in blocking state for a certain VLAN in 1w protocol.

Workaround: Executing commands manually or from the **boot.cfg** file to switch protocols works OK. In case this problem occurs, try switching STP modes: **bridge mode flat** and then **bridge mode 1x1** to see if this problem goes away.

PR 77262

When running scripts using automation tools to configure STP on a stand-alone OS6600 stack, it's observed that the CPU Utilization could go up to 100% after changing the bridge protocol from 1d to 1w. The STP task seems to be stuck in a loop forever, causing the CPU utilization to go up.

Workaround: Manually typing in the commands to switch protocols and configure STP works OK. In addition, executing the same commands in **boot.cfg** file also work OK.

PR 81949

On the OS8800, in flat mode, the default path cost value for a link agg port is being used instead of the new path cost value in the configuration file after the switch as booted up. (It seems like any new path cost value in the thousand range is more likely to experience this problem).

Workaround: Manually re-configure the path cost again for the link agg port after the switch has booted up.

PR 84258

When Spanning Tree bridge parameters are changed for a group of VLANs at the same time repeatedly, it might lead to Spanning Tree loop for some VLANs on an OS8800.

Workaround: There is no known workaround at this time.

VLANs

Feature Exceptions

- The number of VLANs on an OS6600 with spanning tree is 128 and without spanning tree is 256.
 - The number of VLANs on the OS7000/8800 with Spanning Tree is 256 and without Spanning Tree is 1024.
 - User-Defined (Custom) VLAN Rule on OS7000/OS8800—Contact Customer Support for supported configurations
-

Problem Reports

PR 54327

If the Vlan ID of the AV-Client dialog box is entered incorrectly twice, on the OS7000 one receives the following error: "Failure during DoSendData () call" and the AV-Client dies. Similar behavior is observed with unsuccessful authentication, for example, unknown user on the remote authentication server.

Workaround: Reboot of the PC is required.

PR 55491

On a mobile port with mac-port-ip (and other ip) rules, on the OS7000, changing a station's IP address without the layer 2 address being aged out or flushed by link down results in the station remaining in the same VLAN despite the change.

Workaround: There is no known workaround other than aging or pulling the link. The layer 3 address is only examined when the MAC address is not source learned which is the cost of wire-speed group mobility.

PR 59422

The **show interfaces slot/port traffic** command will display the values irrespective of the port state (up or down) on the OS7000 unlike the other interface statistics commands which display the statistics only if the port is up.

Workaround: There is no known workaround at this time.

PR 59883

Flash-synchro does not synchronize the IP address of EMP port on the OS7000.

Workaround: There is no known workaround at this time.

PR 60125

The Tag Value cannot be changed from the VLAN Number on the OS7000. This is a hardware limitation.

Workaround: There is no known workaround at this time.

PR 60680

If a single MAC address of a single device is attached to a single port on the switch and is generating multiple SNAP types with non-zero vendor identification, on the OS7000, one will be unable to create VLAN protocol rules to isolate each generated SNAP type into its own VLAN.

Workaround: There is no known workaround at this time.

PR 60983

Changing the IP address on workstations connected to a hub will not force the workstation MAC address to drop from a VLAN that it has already qualified for by a network address rule to join a new network address-ruled VLAN on the OS7000.

Workaround: Follow the instructions below:

1. Remove hub connection from switch and re-attach.
 2. Connect workstations directly to the switch and reboot workstation when IP address changes made.
 3. Let the MAC address for the station age out of switch CAM.
-

PR 61740

On OOS7000 mobile ports, stations using the IP address range after a station has “autoconfigured itself” will not be learned.

Workaround: The user must perform a release and renew to recover the DHCP-provided IP address. The use of autoconfiguration (aka Automatic Private IP Addressing) is not recommended within an enterprise network environment.

PR 61994

When traffic violates a port-protocol binding rule, source learning does not indicate by VLAN which rule was violated on the OmniSwitch 8800.

Workaround: There is no known workaround at this time.

PR 62119

The ip-port and mac-ip-port binding rules filter the IP address on the port configured if it does not match on the OS7000. Once the MAC address is made part of the VLAN targeted by such rules, the IP address can change to another address in the subnet or subnets carried on that VLAN.

For instance, if an ip-port binding rule is created for VLAN 21 with an IP address of 21.0.0.22 and a port of 2/3, and the device has an IP address configured as 22.0.0.22. When the device is connected to 2/3 and traffic is generated, such as a ping to another subnet 22 address, the port will be listed by the MAC address table in VLAN 21. If the device, such as Windows NT or 2000, changes its address to 21.0.0.41, the switch will continue to carry the new traffic and not blocked as expected with this type of binding rule.

Workaround: Reboot the device or disconnect the link to restore normal binding rule behavior.

PR 63001

MAC-port rules does not block other MACs from using the same port on the OS7000.

Workaround: There is no known workaround at this time.

PR 68371

VPA on a mobile port does not flush out the VPAs when rules are deleted on the OS7000.

Workaround: System relies on the VPA aging out process rather than deleting it proactively on rule deletion. However VPAs are deleted when the VLAN as a whole is deleted or if mobility is removed from port.

PR 68495

During the learning process of two flows matching two different rules on a mobile port, the second flow is seen as learned on the VLAN of the first flows on an OS6624/6648. This is temporary as the address is going to age out.

Workaround: There is no known workaround at this time.

PR 68762

Traffic gets discarded or classified only in default VLAN on an OS6624/6648.

Workaround: Change the mobile port which is having the problem to a fixed port and then back to mobile again. If this does not the problem, apply a link down and up on the port.

PR 68968

Switching to a single mode MAC router will not deallocate already allocated macs which have been saved in the configuration file on the OS7000/8800.

Workaround: If you are switching to single mode, delete all MAC alloc commands from boot.cfg.

PR 69656

Unicast frames will be flooded on the OmniSwitch 8800 until all the MAC addresses are learned in both the source and destination CAMs.

Workaround: There is no known workaround at this time.

PR 70502

The multicast packet with a destination of 01:20:2a:02:01:01 needs a path where the default VLAN for the connecting ports is enabled on the OS7000. The inter-VLAN routers are a brick wall to the GMAP packets.

Workaround: Provide a maintenance network where any two or more switches are bridged together with ports sharing a default VLAN.

PR 70811

A default VLAN might come up in operational state when it is disabled to accommodate group mobility.

Workaround: There is no known workaround at this time.

PR 70954

The first IPX encapsulation learned on a fresh OS6624/6648 switch becomes the only encapsulation that can be learned until the switch is rebooted regardless of the encapsulation selected in the IPX (ipx-e2, ipx-llc, or ipx-novell) protocol rule.

Workaround: There is no known workaround at this time.

PR 71665

Setting the egress flood limit to zero will still allow a small number of flood packets to egress the port.

Workaround: There is no known workaround at this time.

PR 72223

ENI 10/100C-24 Autoneg disabled if speed/duplex changed to non-auto.

Workaround: There is no known workaround at this time.

PR 73334

When the configuration for a range is applied on the OmniSwitch 8800, and if there is an error in the middle of the group configuration (all slot, groups of ports), the rest of configuration will not apply from the point of error.

Workaround: Apply the configuration from the next valid starting point (e.g. next valid port).

PR 73367

Mobile and default VLAN traffic flow is not effective if the ingress frames to the OS6600 series switches contain IEEE 802.1Q VLAN tagging and mobile-tagging is disabled for the destination VLAN; transparent tagging is not supported.

Workaround: There is no known workaround at this time.

PR 75199

When using group mobility custom rule, traffic will go on the default VLAN even though the content (at the offset) of a new stream of traffic (from the same MAC device) is matching the MAC address already learned in the default VLAN.

Workaround: Flush the MAC address learned on the default VLAN, then resending traffic.

PR 76336

When IP traffic is classified on a mobile port on an OS6624/6648, the IP source address must be learned by the system in order for traffic to be correctly processed from each source host.

Workaround: Resolve ARP for all IP hosts classified on mobile ports.

PR 76348

Using port mobility, when the OS7000 host (PC) fails to match a mobile binding rule such as **mac-ip-port** if for example the IP-JSA fails to match the IP address in the rule, the host will be learned in “filtering” mode. If the PC host is then updated with the correct IP, even though the IP address from the host now matches the IP in the rule, the host will continue to be in “filtering” mode.

Workaround: When attempting to reclassify any host that has a pre-existing “filtering” entry. The MAC entry needs to be removed. Either by disconnecting and then reconnecting the physical link or via the system management software using “no-mac-address-table learned.”

PR 83373

On an OS6600, MAC doesn't get flushed out from the VLAN when the MAC rule that matches the MAC address is deleted from the VLAN. The port goes into filtering mode and stays there.

Workaround: Unplug/replug the port.

PR 84262

On an OS6600, VLAN Manager continues to show port forwarding in multiple VLANs for about ~30 secs. after a mobile port movement has occurred and the MAC is flushed and relearned correctly in the new VLAN. This eventually goes away.

Workaround: Wait for a little while.

PR 84314

When a MAC address is learned as filtered on OS6600, traffic received by the switch with the filtered MAC address as a source MAC address is blocked.

Workaround: Works as designed.

PR 88175

On the OS7000, you cannot add ports to high-availability VLANs. Unable to configure Feature. "vlan x port-mac ingress-port x/y" will generate "INTERNAL ERROR".

Workaround: Upgrade to Service Release 5.1.5.63.R04 or Greater.

Layer 3

Basic IP Routing

Problem Reports

PR 57299

The unloading and reloading of RIP/BGP/OSPF is not supported on all OmniSwitch platforms.

Workaround: Reboot switch for reloading of operation protocol.

PR 58974

Changing ethernet encapsulation from eth2 to snap while running traffic does not take effect until manual route cache clear is performed on the OS7000.

Workaround: There is no known workaround at this time.

PR 59599

The number of TCP Reset does not match the number of SYN Request packets after doing a **Show tcp statistics** command on the OS7000.

Workaround: There is no known workaround at this time.

PR 62481

ARP entries do not get updated until they timeout first (300 seconds) even though layer 3 traffic has changed its path after a spanning tree reconfiguration due to a change in the state of a port. For these 300 seconds, the MAC is seen on the new port but the ARP entry is still learned on the old port because of which all layer 3 traffic is dropped for 300 seconds.

Workaround: There are two workarounds:

1. Wait for 300 seconds so that the entry times out and is learned again on the new port. (recommended).
 2. Clear the ARP cache using CLI command **clear arp-cache**.
-

PR 63599

debug ip packet ip-pair does not filter out all traffic based on the 'ip-pair' on the OS7000.

Workaround: 'ip-pair' only applies to IP packets. If you do not want to see ARP packets, you might want to enter **debug ip packet ether-type ip**.

PR 65650

With a large number of RIP routes on the OS7000, (i.e. 200), setting the Debug Level to a high value (i.e. 100) ties up RIP with printing debug messages, which causes RIP not to accept other inputs ex: CLI or SNMP.

Workaround: Reduce the debug-level to a lower value (i.e. 70).

PR 65678

On the OS8800 debug IP packet can only display bogus characters.

Workaround: There is no known workaround at this time.

PR 67799

Performance may drop slightly below wire-rate while routing small-sized packets on an OS6624/6648.

Workaround: There is no known workaround at this time.

PR 71573

OS6624/6648 does not support multiple router MAC address mode.

Workaround: If connecting an OS6624/6648 to an XOS box, make sure that only one port per IP VLAN is physically connected between the two boxes. Otherwise, routing will not work.

PR 72943

The protocol processing on the OS6600 family of switches includes IP-SNAP protocol in the IP Ethernet protocol set. That means, if an protocol rule for ip-e2 exists with an ip-snap protocol rule on the same switch, the ip-snap rule will be disregarded.

The OS7000 switches do process ip-e2 and ip-snap protocols separately.

Workaround: Use an IP network address rule instead of an IP protocol rule in conjunction with an ip-snap protocol rule, if possible.

PR 73015

The IP ETHERNET 2 protocol and the IPX ETHERNET 2 protocols cannot be associated with the same MAC address in two separate mac-port-protocol rules (using the same port is assumed). Either one or the other protocol's traffic will flow, but not both on the OS7000.

Workaround: Use only a mac-port-protocol rule with either IP or IPX, or go to a less restricted rule like port-protocol or protocol rule.

PR 74184

Router-ID does not respond to ping. This feature is frequently referred to as a loopback interface and is not available in the current release. The "router-id" and "primary-address" configuration commands are strictly used by the routing protocols for unique router identification.

Workaround: There is no known workaround at this time.

PR 75002

There is no provision to configure per Vlan IP MTU on an OS6624/6648. As a result, once the flow is setup on the OS6624/6648 (meaning both the Src/Dest addresses are learned), if a packet violating the IP MTU is received, it will still be forwarded by the hardware. IP MTU checking is done in software, so it will work for the first packet (that comes to software), i.e. for the first packet, the switch will send back an appropriate ICMP response.

Workaround: There is no known workaround at this time.

PR 75244

When OS6624/6648 is configured for layer 3 routing, the servers with "teamed" or load balanced ports is currently only supported with the 802.3ad service configured on the switch.

Workaround: There is no known workaround at this time.

PR 79799

On OS6600 series switches, an OSPF route cannot be redistributed into Rip when there exists a Static route in the IP Routing Table for the same destination, same metric and same next-hop as the Ospf route.

Workaround: There is no workaround for this issue. Only one of the two routes - Ospf route and Static route - may be used in the IP Routing Table. Hence, the configuration of the network should be such that routes of only one protocol - static or dynamic - exist at exist at any time in the IP Routing Table for the same destination and with the same next-hop.

PR 79931

On OS6600 series switches, when a Static and an OSPF route exist for the same destination and with the same next-hop and metric and if both the Static and OSPF routes are redistributed into Rip with the order being Static config specified first and then OSPF (as specified in the config file), then Static routes are redistributed into Rip.

Workaround: There is no workaround for this issue. The limitation is that at a time, there should be only one kind of route existing for a destination in the OS6600 series IP Routing Table.

PR 80049

When a RIP v1 interface on one OS6600 series Router connects to a Rip v2 interface on another OS6600 Router, then Rip v1-based host-routes will be created by the Rip v1 router for each of the existing Rip v2 routes and added to the IP Routing Table. These will then be aged out after reaching metric 16 and then removed. This is done periodically once in every 4 or 5 minutes. This happens since host-route support is not disabled by default on the Rip v1 or Rip v2 routers.

Workaround: The host-route support should be disabled on each of the Rip v1 or v2 routers. The host-routes will no longer be generated.

PR 80494

On the OmniSwitch 6624/6648, packets routed between IP-SNAP & Ethernet 2 are not translated correctly. The Intel IXE2424 ASIC used in the 6600 platform does not support translations from SNAP to Ethernet II packets.

Workaround: There is no known workaround at this time.

PR 84444

Route 127.1.0.0/16 shows in the IP forwarding table on a OS7000. The route is used for internal communication between CMMs and stacking NIs. There is no side effect on normal switch operation.

Workaround: There is no known workaround at this time.

IPX

Problem Reports

PR 54290

The switch will only change an IPX network field of zero to the appropriate source network when the first zero packet arrives on the OS7000. After that point the IPX packets are passing through the HRE, and cannot be changed.

Workaround: There is no known workaround at this time.

PR 61257

The **show ipx interface <vlan>** command displays "WAN processing not enabled on this interface." on the OS7000. Since WAN connections are not allowed in this release, the WAN state of the interface will always be "not enabled."

Workaround: There is no known workaround at this time.

PR 68826

When using the Ixia ScriptMate on the OmniSwitch 8800, Ixia tries to reacquire the link. It detects a time-out and is unable to pass traffic.

Workaround: Configure Ixia side as non-auto, then there will be no more link changes.

PR 73198

The MAC-IP binding rule will allow IPX traffic to flow along with the classified IP traffic in the VLAN classified to. Other products will filter IPX traffic in a disabled default VLAN instead of moving the traffic in the IP VLAN.

Workaround: If a lower precedence rule is available, the IPX traffic will be classified and flow in the VLAN covered by the rule.

PR 80153

The ipxServName in the ipxServTable MIB is a 48 octet identifier of the server. The IPX specification says that it contains up to 48 octets and is NULL terminated. The Object is used (all 48 bytes) as part of an index into the ipxServTable.

Normally these octets are printable characters. However, with the introduction of NDS by Novell, there can be non-printable octets in ipxSerName. These characters are Netware identifiers in the NDS tree. These octets are an integral part of the name, and index, and are used for the SNMP OID. Since the octets are non-printable characters, they can cause confusion to the user and result in their interpretation as invalid octets.

Workaround: Verification of the name can be done on the Netware server

NTP Client**Feature Exceptions**

- NTP is not supported in Server mode.
-

Problem Reports

PR 72478

A preferred (NTP) server does not synchronize the client before an non-preferred server.

Workaround: There is no known workaround at this time.

PR 72889

It may take about 12 minutes for the NTP client to readjust its internal clock when the offset is small.

The time update is triggered by the NTP algorithm itself. In general, if offset is larger than 128 milliseconds continuously for 900 seconds (15 minutes), a time update will be done. This design prevents excessive time updates by using a threshold to debounce timestamp data received.

Workaround: There is no known workaround at this time.

Server Load Balancing (SLB)

Problem Reports

PR 60561

If an SLB cluster is configured with "failover" as the distribution algorithm and when a new server in the cluster comes UP, then the connections already established with a less priority server are not re-established through the new one (no automatic switchback) on the OS7000.

Workaround: There is no known workaround at this time.

UDP Relay

Problem Reports

PR 67723

false packets sent by udp relay.

Workaround: There is no known workaround at this time.

PR 67896

SNMP agent return values from "iphelperVlan" with an invalid SNMP data type on the OS7000.

Workaround: There is no known workaround at this time.

PR 77401

On the OS7000, if the lease time expires for a particular IP address used by one switch, and the server is out of new IP addresses, and another switch requests for a IP address, then the server gives out the IP address whose lease has expired to this new switch. Thus resulting in duplicate IP addresses on the two switches.

Workaround: Increase the lease time on the server or configure larger pool of addresses on the server.

PR 80755

In some cases, DHCP required packets with source IP address of 127.0.0.1 being received from the previous UDP relay hop.

Workaround: Configuring the correct IP interface would eliminate this problem.

PR 83528

Well known UDP ports are only configurable with a service name on an OS7000.

Workaround: No known workaround at this time.

PR 83643

If a total of three non-BOOTP/DHCP Generic UDP relay services are configured on an OS7000/OS8800, the last one configured will be replaced with a BOOTP/DHCP service the next time the switch reboots.

Workaround: Delete the BOOTP/DHCP service and enable the Generic service again.

PR 83947

On OS7000, **show ip udp relay service** has zero value for statistic.

Workaround: There is no known workaround at this time.

PR 83949

On an OS7000, you can configure any UDP port # even if it is out of its range. (range 0-65535)

Workaround: There is no known workaround at this time.

PR 84359

If a VLAN's router IP address is changed on an OS7000, UDP relay agent still has the previous IP.

Workaround: Disable the relay service on the VLAN using the **no ip udp relay service vlan**, then enable the relay service on the VLAN again using the **ip udp relay service vlan** command.

PR 84471

On an OS7000, the yipped field gets changed.

Workaround: There is no known workaround at this time.

PR 84500

On an OS7000, once UDP framed is relayed, its TTL value is always set to 32 secs (hex 20)

Workaround: There is no known workaround at this time.

PR 84592

In certain cases, frames get duplicated with UDP Relay on an OS7000.

Workaround:

1. With VRRP, enabling only on one VRRP router (either master or backup) is desirable for any UDP relay service to avoid UDP frames being duplicated.
 2. If there are ECMP routes, enabling on one backbone VLAN is desirable for any UDP relay service.
 3. If 802.1Q is configured on multiple switches, UDP relay service only needs to be enabled on one switch.
-

VRRP

Problem Reports

PR 61934

OS7000 does not support VRID 0. OmniCore does

Workaround: Do not use VRID 0 on the OmniCore other devices when running VRRP with the OS7000.

PR 62272

Exceeding the multicast software routing processing limits can introduce instability to VRRP master to backup communications resulting in VRRP switching between master and backup states frequently on the OS7000.

Workaround: Reduce the amount of IP multicast traffic running through the affected NI.

PR 68342

VRRP neighbors may switch between master and backup when more than 20 virtual routers are on the OS7000.

Workaround: One must have OS7-GNI-U2's with a 1.3 Catalina or greater. The version of the Catalina for a Gigabit module is determined by running the command "show ni <slot>". In the line "ASIC-Physical", the last two values represent the version of the Catalina i.e.

ASIC - Physical: 0x1901 0x0201 0x0201

The version number should be greater than 0x0301

PR 70384

VRRP will occasionally send out the hardware MAC instead of the virtual MAC

Workaround: Make sure clients on the network honor gratuitous ARP's. If this is not possible, use an IP address that is not actually assigned to an interface as the VRRP IP address. This will ensure that no hardware MAC address is ever associated with the virtual IP address.

PR 84166

On the OS7000, this debug message may be seen when VRRP is enabled. Please ignore as it does not affect functionality.

Workaround: There is no known workaround at this time.

Quality of Service (includes ACLs and NAT)

Feature Exceptions

- Only 512 policy rules, conditions and actions are supported OS7000/8800.
- Only 128 policy rules on OS6600.

Problem Reports

PR 56327

Using Layer 2 traffic, with Dest Mac condition and Stamping TOS action, when the ingress port is untrusted, the outgoing stamped TOS value is always zero regardless of the stamped value on the OS7000. If the ingress port is changed to trusted, then the outgoing stamped TOS value is correct.

Workaround: There is no known workaround at this time.

PR 56387

Using Layer 2 traffic on the OS7000 with untrusted ingress ports, where Dest Mac condition with 802.1p is stamping or marking action, the 802.1p value is always set to zero. If the same ingress port is changed to trusted, the 802.1p value is stamped correctly.

Workaround: There is no known workaround at this time.

PR 57581

When the current value of QoS log lines is changed dynamically on the OS7000, it forces the log to be cleared.

Workaround: Change the value of QoS log lines in the boot.cfg file before the next reboot.

PR 57836

Policy service group is broken by using "source ip port" with "destination ip port" on the OS7000.

Workaround: There is no known workaround at this time. Service groups can contain either:

1. All source port conditions.
 2. All destination port conditions.
 3. All source+destination port conditions.
-

PR 57932

ARP packets are not classified by QoS with NAT on the OS7000.

Workaround: There is no known workaround at this time.

PR 58008

When "classify13 bridged" is turned on, on the OS7000, if a specific Layer 2 DA rule is not matched (or gets dropped due to the Layer 2SA lookup), then traffic is treated as if it is routed which includes what you prioritized on. Layer 2 traffic that does not have an IP header is not prioritized on TOS due to there being TOS values to prioritize on. QoS only really deals with IP for the most part.

Workaround: There is no known workaround at this time.

PR 58182

Layer 2 ACL DENY does not work on the OS7000 when the destination MAC for the Layer 2 flow is not learned.

Workaround: There is no known workaround at this time.

PR 58244

Only one "L2 DSCP stamping" action OR one "something to DSCP mapping" action is supported on the OS7000. The first rule that uses such an action will work. If other rules use the same kind of actions, they will be "ignored", and they will execute the action.

Workaround: There is no known workaround at this time.

PR 59341

The **destination port/interface type** cannot be used with action NAT on the OS7000.

Workaround: There is no known workaround at this time.

PR 60928

Active FTP not supported with NAT on the OS7000.

Workaround: There is no known workaround at this time. Use passive FTP if using NAT.

PR 61072

Simple NAT rules, on the OS7000, that have conditions whose IP address/subnet overlaps with switch addresses will match traffic sent from these addresses, even if the traffic is bridged.

Workaround: Along with the generic NAT rule, a higher precedence non-NAT rule must be added to match traffic from the switch addresses that overlap with the generic NAT rule.

For instance, if you wanted to remap the subnet 124.10.10/24 to 60.0.0.2, but also had a switch address of 124.10.10.5, you would have two rules:

```
policy condition nat source ip 124.10.10.0 mask 255.255.255.0
policy action nat destination rewrite ip 60.0.0.2
policy rule nat condition nat action nat precedence 100
```

```
policy condition exception_ip source ip 124.10.10.5
policy action accept disposition accept
policy rule exception condition exception_ip action accept precedence 200.
```

PR 61874

Destination Port and Destination Interface Type policies are not supported across Link Aggregation using QoS Policy on the OS7000.

Workaround: There is no known workaround at this time.

PR 62076

After a **write memory** command and subsequent reboots on the OS7000, QoS will display all the LDAP policies as active, even if these policies were previously deleted from the LDAP Server or if the Policy Validity Period had expired.

Workaround: There are two workarounds:

1. From CLI, issue a **policy server flush** command before a **write memory** command.
 2. If the **write memory** command has been issued before a reboot, edit the boot.cfg file and remove any LDAP policies (conditions, action and rules) that are no longer valid and reboot the switch.
-

PR 63285

TCP/UDP fragment classification is not supported on the OS7000.

Workaround: There is no known workaround at this time.

PR 65449

Reflexive policies, on the OS7000, do not work properly if the drop rule that denies the "reverse" traffic coming from the outside is created first or has a higher precedence. With "qos default routed disposition drop", it works fine.

Example

```
Inside Network 10.0.0.0 -- SWITCH -- Outside Network 192.0.0.0  
policy condition cOut source ip 192.0.0.0  
policy action deny disposition deny  
policy rule rOut condition cOut action deny  
policy condition cIn ip 192.0.0.0  
policy action accept disposition accept  
policy rule rIn reflexive condition cIn action accept  
qos apply
```

This will not work because the "drop" rule is created first (with the same precedence, the first rule is taken first).

Workaround: Make sure the "reflexive" rules ALWAYS have a higher precedence than ANY "drop" rules that can deny "reflexive" traffic.

```
policy rule rIn precedence 1  
qos apply
```

PR 66077

Sometimes, it can take a reflexive flow 3 seconds before being accepted on the OS7000. This is due to the TCP timeout configured on PC/sun IP stack (standard value). The first "open request" will hit the switch but the response of this request could be dropped before the reflexive policy gets really applied. Then the PC will retry 3 seconds after.

Workaround: There is no known workaround at this time.

PR 66914

Drop and deny are synonymous key words for QoS ACL disposition on an OS6624/6648.

Workaround: There is no known workaround at this time.

PR 67871

The **show active policy rule** command does not display rule matches for a given flow once that flow is learned and handled on an OS6624/6648.

Workaround: There is no known workaround at this time.

PR 67882

show qos queue does not display Xmit or Drop Packets for any port queue on an OS6624/6648.

Workaround: There is no known workaround at this time.

PR 68472

OS6624 and OS6648 does not prioritize traffic on saturated half-duplex links, possibly allowing data traffic through the phone to cause drops of voice traffic or signaling to the PCX. This happens only when we have PC connected through phone and have heavy PC traffic going through the IP phone. Link is acting in accordance with CSMA/CD standards.

Workaround: There is no known workaround at this time.

PR 68550

When using Link Aggregation, one cannot use QoS with **destination port slot/port** or **destination interface type** to match the traffic going through the Link Aggregation on the OS7000/8800. QoS only knows the virtual port of the Link Aggregation, but does not know anything about the physical port that is used to forward traffic.

Workaround: There is no known workaround at this time.

PR 68555

Every time one does a **qos apply** when the qos configuration has changed, all traffic on the OS7000/8800 will be disturbed. Basically, all hardware entries are flushed and all traffic goes to source learning again. The switch throughput will drop for a short time. (software speed instead of wire speed) This means that some packets may be lost depending on the amount of traffic when the **qos apply** command is issued.

Workaround: There is no known workaround at this time.

PR 68849

Policy->Groups->Ports does not display all built-in port groups.

Workaround: There is no known workaround at this time

PR 68906

Sometimes, all the policies do not flush. This applies on all platforms.

Workaround: Issue the policy server flush command from the command line to delete all the policies.

PR 69252

Mibwalk fails in QOS mib at alaQoSPortGroups and alaQoSAppliedPortGroups because of lexicographic failure on an OS6624/6648.

Workaround: There is no known workaround at this time.

PR 72325

On the OS6624/6648, if the TOS bit is set to 1, when the traffic comes into an untrusted port, it does not set the bit to 0. Packets coming in on untrusted ports will not be dropped. TOS bits will be set to 0 only on L3 traffic. 802.1p bits will be set to 0 on L2 traffic.

Workaround: There is no known workaround at this time.

PR 73767

On an OS7000/8800, when setting a permanent MAC address to filtering, traffic going to this MAC will always be dropped regardless of the qos rules (even if one permit rule match this mac). When setting a permanent MAC address to bridging, traffic going to this MAC will always be accepted at best effort, regardless of the qos rules. Therefore it becomes impossible to set any priority, stamping/mapping or bandwidth shaping actions for traffic going to this MAC address.

Workaround: There is no known workaround at this time.

PR 74062

On an OS6624/6648 system, it is not possible to create an L3 ACL on a source and another on a destination because currently the it cannot link up source and destination.

Workaround: There is no known workaround at this time.

PR 76509

In some cases a bogus "time change detected" message is displayed in the policy server event log.

Workaround: There is no known workaround at this time.

PR 76901

The OmniSwitch 6624/6648 5.1.4.R01 configuration file is not compatible with 5.1.5.R01 and 5.1.5.R03.

Workaround: Edit the **boot.cfg** file.

PR 80707

QoS rules have no "matches" after 2 takeovers

Workaround: The match count shown from the CLI currently reflects only newly created flows/matches. On a takeover, if the flows aren't flushed and re-learned, the match counts will remain 0 on the secondary until new flows are matched (or the old ones time out and are re-learned).

PR 81351

Layer 2 P-Stamping rules are not supported on OS6600 series Link Aggregation ports.

Workaround: There is no known workaround at this time.

PR 81620

After LDAP server is deleted from a switch, there is no way to remove all related policies from QoS layer.

Workaround: Remove QoS policies before deleting LDAP server.

PR 82571

When entering more than one LDAP policy server, they are retrieved/set incorrectly through SNMP.

Workaround: Enter the policy servers through the CLI.

PR 84257

If there is traffic going out to ipport A via slot/port B on an OS6600 and there are two rules, rule one specifying destination ipport A and rule B specifying destination slot/port B, then rule one is not effected on the traffic.

Workaround: Try defining the rules without specifying the destination slot/port.

PR 84386

In some setups where the same destination is used but the source is different, a Layer 4 rule will not affect traffic if another rule of higher precedence exists on an OS6600.

Workaround: Make the Layer 4 rule the highest precedence rule.

PR 84425

Drop rule still enforced when source MAC or source VLAN is changed in a secure switch access condition on an OS6600.

Workaround: There is no known workaround at this time.

PR 87417

On the OS7000, the user can modify the built-in port groups. But, modifications may not be saved to the config, and the switch will boot-up with the default built-in port groups.

Workaround: Do not modify the built-in port groups.

Advanced Routing

OS7000/8800 Feature Exceptions

- The maximum number of total routes is 65K.
 - The maximum number of RIP routes is 10K.
 - The maximum number of OSPF routes is 40K.
 - The maximum number of BGP routes is 65K.
 - The maximum number of active traffic flows is 16K (based on current default cache allocation).
-

OS6600 Feature Exceptions

- The max number of total routes is 4K.
 - The max number of RIP routes is 2K.
 - The max number of OSPF routes is 4K.
 - The max number of active traffic flows is 1K
-

BGP4

Problem Reports

PR 70681

Cannot use BGP4 route-map policy match-prefix (i.e. 0.0.0.0) to selectively apply (in/out bound) policy to a subset of learned routes on the OS8800.

Workaround: Create another instance of the route-map policy and use a prefix-list of 0.0.0.0 (and mask 0.0.0.0) to allow all routes while the other instance applies the policy on the subset of learned routes.

PR 72024

BGP4 Dampening Suppress value cannot exceed the default Ceiling value of 1600 seconds on the OS8800.

Workaround: Configure a Suppress value less than 1600 seconds.

PR 72300

Cannot use AS number with command: **ip bgp confederation neighbor**.

Workaround: There is no known workaround at this time.

PR 78983

Sometimes on the OS8800, if BGP flap dampening is enabled, BGP task might crash depending on a particular flapping characteristic and setup. This is not a reproducible issue.

Workaround: No workaround exists for this issue. The OS8000 might need to be reloaded to restore normal BGP operation.

DVMRP

Problem Reports

PR 56990

Tunnel destined flows are not displayed in the **show ip multicast forwarding** CLI command on the OS7000. There is simply no room left on the line to display.

Workaround: Use the **show ip mroute-next-hop** CLI command instead to display tunnel endpoint information.

Multicast Routing

Problem Reports

PR 55446

Multicast routing does not handle large multicast bursty traffic on the OS7000.

Workaround: There is no known workaround at this time.

PR 79306

Multicast streams may be momentarily disrupted during NI insertion or removal.

Workaround: This condition is temporary and all flows will resume after a few seconds.

PR 79916

Timeout of group membership may not result in a leave message being sent to an upstream device on the OS7000.

Workaround: None, however this will only result in a small amount of bandwidth over-utilization across the trunk. The actual member will not receive the flow and therefore clients will be unaffected.

PR 80757

Only a single client on a given port for a given multicast group is shown in the group membership displays on the OS6600/7000.

Workaround: This is a result of the way IGMP clients respond to group membership queries. Only a single client will respond in a flooded environment where all clients will see the report. If a client receives a group membership report for the same group on its interface, it will not send its own membership report as a result.

OSPF**Problem Reports**

PR 55287

It is currently not possible to change the key-id for md5 authentication over OSPF virtual links on the OS7000. It will always be 1.

Workaround: Please make sure that the adjacent router on the virtual link has the key-id configured also.

PR 56345

Cannot unload and reload OSPF on the OS7000.

Workaround: There is no known workaround at this time.

PR 58676

OSPF default cost is the same for fast ethernet and giga interface on the OmniSwitch 7700/7800.

Workaround: There is no known workaround at this time.

PR 59813

Loss of unicast traffic across a gigabit module fiber link between 2 OSPF routers results in not achieving FULL adjacency on the OS7000/8800.

Workaround: There is no known workaround at this time.

PR 65617

OSPF stops advertising static routes to the network when the route tag is configured on a redistribution filter on the OS7000.

Workaround: There is no known workaround at this time.

PR 65936

Debug messages are not displayed when connected via Telnet on the OS7000. They only display on the console port.

Workaround: Connect to the console for doing debug commands with display output.

PR 69890

OSPF virtual links will not form an adjacency with gateD switches if MD5 is configured on an OS6600/7000.

Workaround: The MD5 key id for OSPF virtual links is hardcoded to 1. Any switch that uses gateD and MD5 is configured on the virtual link requires that key id is coded accordingly. In this gateD example for an OmniSwitch Router, the ID is set to 1:

```
ospf yes
  backbone { interface 212.1.1.194 { priority 2; };
    virtuallink neighborid 196 transitarea 3
      { auth md5 key "hawkVL" id 1;
        hellointernal 10;
        routerdeadinterval 40; } ;
  } ;
```

PR 69893

OSPF Area Summary ranges no longer have "enabled/disabled" status. The presence or absence of a range itself is equivalent to the "enabled/disabled" state on the OS7000.

Workaround: If a range is to be disabled, it should be deleted with the **no ip osp area summary range** command. On creating a range, it is automatically in the enabled state.

PR 72040

On the OS7000, RIP and OSPF MD5 authentication is not interoperable between AOS and XOS (GateD) & OmniCore.

Workaround: Use Clear Text or SIMPLE authentication.

PR 78386

The OSPF task traps on the OS6600 series switch, either on a standalone or on a stacked switch, sometimes during the following scenario: – the total number of OSPF routes number 250 or more and there is redistribution of 100 or more Rip v2 routes into OSPF; – there is a flap of OSPF routes with routes getting deleted and then added quite frequently like once in half an hour. The trap is found to be due to corruption of the nodes in the Skip List used by OSPF. This is not always reproducible and may happen at any time during runtime of OSPF task.

Workaround: There is no workaround for this issue and the OSPF task will suspend when the Skip List corruption happens. The switch will need to be rebooted.

PR 81763

On OmniSwitch 6600 series switches, when OSPF debugs are enabled from the console, after a while the console will lockup. This is since OSPF tries to use a print from a signal handler. This is a limitation.

Workaround: Use the OSPF debugs only on telnet sessions and never on console sessions.

PR 81782

A non-ABR router generating a Type-7 LSA does not set the P-Bit in the LSA (to enable translation) if an enabled inactive non-NSSA area exists.

Workaround: Delete or disable the inactive area.

PR 81856

On OS6600 series switches, Webview OSPF Routes page does not display the aggregated summary route entry corresponding to the active address range configured for the area.

Workaround: There is no known workaround at this time.

PR 82004

HRE PCAM's max.collision depth of 5 causes Catalina 1.1 boards to stall on some multicast packets.

Workaround: There is no known workaround at this time.

PR 84440

On an OS6600/7000, if a redistributing router is rebooted and if after the reboot the external routes no longer exist, max-aged lsas might remain in the data base of the redistributing router or its neighbors with one or more neighbor retransmission list not being emptied.

Workaround: There is no known workaround at this time.

PIM-SM**Problem Reports**

PR 73783

On an OS7000, a lot of register packets will stress the NI. Everything is going through software and so the NI will be very busy.

Workaround: There is no known workaround at this time.

PR 74581

Some releases of Cisco's PIM implementation default to "full packet" checksums for their register packet checksum algorithm. This causes Cisco routers to reject valid PIM register packets from the OS7000 PIM implementation which defaults to "header only" checksums for PIM register packets.

Workaround: Change "register checksum" to "full" when connecting Cisco PIM-SM router to the OS7000.

PR 74719

If a Cisco router is configured as a C-BSR with the highest priority and it is not directly connected to the OS7000s, the OS7000s will not see the Cisco router as the BSR.

Workaround: Configure the OS7000 to be the BSR instead of the Cisco router if the Cisco router is not directly connected to the OS7000.

PR 74815

On the OS7000, the hashing function, which calculates the hash value used to map a group to an RP, has problems when running with a Cisco router. It appears that the Cisco box is forgetting the last part of the formula ($\text{mod } 2^{31}$) which masks off the upper bit.

Workaround: When running PIM-SM with a Cisco router, do not use multiple RPs with the same priority.

PR 74881

When a Cisco router is acting as the DR (Designated Router) with spt-switchover enabled, the Cisco router may erroneously send (S,G) prunes to the OmniSwitch 7700/7800's causing the multicast streams to be disrupted. This seems to be the case when the route to the RP is the same as the route to the source.

Workaround: Disable spt-switchover on the Cisco.

PR 74979

On the OS7000, the console may scroll the following messages to report that there is something misconfigured or software/hardware is behaving improperly in the lower layers:

```
tPism: Received Hello from my own IP: xx.xx.xx.xx. Invalid configuration
tDvmrp: dvmrpRecvProbe: Configuration/Lower-layer problem V<vlan> Looping back our Probes
tDvmrp: dvmrpRecvReport: Configuration/Lower-layer problem V<vlan> Looping back our own RRs
```

Workaround: If you don't want these messages to scroll on the console, the following commands will stop them: **ip pimsm debug-level 0** or **ip dvmrp debug-level 0**.

PR 75062

When running in a mixed environment consisting of OS7000's and Cisco's, the OS7000 PIMSM router may get into a state in which the flows get disrupted. This is caused by erroneous prunes. Once in this state, the flows will have to be completely timed out.

Workaround: There is no known workaround at this time.

PR 77055

On the OS7000, if there are multiple routes to either the RP or any of the multicast sources, PIM-SM must be enabled on all of the interfaces.

Workaround: Enable PIM-SM on all interfaces that may be considered possible routes to either the RP or any of the multicast sources.

PR 84167

While the CLI command **show ip mroute-boundary** shows the interface index, WebView displays the Vlan Router IP address instead of interface index for the corresponding WebView page (IP Multicast/Routing/Boundaries) on an OS8800.

Workaround: There is no known workaround at this time.

Security

General

Problem Reports

PR 80799

During multiple, sequential SSH connections to an OS8800, the message "++Sorry, traces of my own stack begin at tt ()." might print to the console.

Workaround: There is no known workaround at this time.

802.1X

Problem Reports

PR 70452

On the OS7000, even after the PC is successfully authenticated to a port, the status on the PC will show as not authenticated when using 802.1X with XP SP-1/SP-2.

Workaround: This is a problem in the Microsoft XP driver.

PR 72546

On OS6624/6648, after the supplicant is authenticated and the port is open-global, non-supplicant on that port will be on the supplicant's VLAN. It only supports one VLAN per port. The default should be moved from the original default VLAN to the supplicant's assigned VLAN after the supplicant is authenticated to the port. This behavior is different from the OS7000/8000 platform which can support more than one VLAN per port.

Workaround: There is no known workaround at this time.

Authenticated Switch Access

PR 59686

If a user kills an HTTP session, the table will still display the session when it automatically refreshes.

Workaround: The user must hit the refresh button again, and the table will not display the session. This problem ONLY occurs with HTTP session. Telnet and FTP sessions are removed from the table properly.

PR 63104

During a takeover, switch management sessions (HTTP, FTP, Telnet) are closed on the OS7000. So, the operator must proceed to a new ASA sequence when takeover is completed.

Workaround: There is no known workaround at this time.

PR 66411

On the OS6624/6648, the description of the aaasAceClear in aaaServerTable (AlcatelIND1AAA.mib) nominator indicates that true and false are possible values but only the true value can be used i.e.

- sending a SET request with the value true resets the secret sent by the ACE server
- sending a SET request with the value false has no effect
- the value returned by a GET request is not significant

Workaround: There is no known workaround at this time.

Authenticated VLANs

Feature Exceptions

- AVLAN HTTP uses signed applets for the automatic IP reconfiguration. Those applets are signed using VeriSign Certificates that expire every year. The certificate used for Internet Explorer and Netscape expires every August. AVLAN HTTP users have to validate a warning indicating that the certificate used by the applet has expired. A renewed certificate will be applied to the next release.
-

Problem Reports

PR 55936

Creation of objects in aaaServerTable and aaaUserTable can only be performed using a SNMP browser which support MUTI-VARBIND mode on the OS7000.

Workaround: There is no known workaround at this time.

PR 58192

If an LDAP server is configured in SSL mode on the OS7000 with a TCP port value equal to a non-SSL port configured on the LDAP server side, then LDAP communication is not possible between the switch and the server. Some resources may remain unfreed in the switch.

Workaround: When configuring the SSL port, port numbers are the same on both sides. This is especially true if one is not using the following default port numbers: SSL port = 636 and no SSL port = 389. Using the default value for the port number is best to avoid inconsistency. If used, it is not necessary to set the SSL port number but just necessary to enable or disable SSL through WebView or CLI. When the SSL port number is not mentioned, AAA software initializes with the default values.

PR 63509

Sometimes, on the OS7000, Windows XP does not load the right HTTP authentication applet when the java development kit 1.4 is installed (JDK 1.4) and the SUN java virtual machine (JVM) is used instead of the Microsoft JVM.

Workaround: The solution is to uninstall the JDK 1.4 and to use only the Microsoft's JVM with WindowsXP SP1 when it is available.

PR 66469

Sometimes after takeover, using the HTTP authentication method may cause an AVLAN user to have authentication problems if the Java applet which performs IP reconfiguration fails to be downloaded.

Workaround: Manually reconfigure IP using "ipconfig /release" & "ipconfig /renew" on the Client PC or remove the authenticated MAC address using the CLI command **aaa avlan no mac-address**" and attempting a new authentication.

PR 68240

When an LDAP SSL certificate expiration occurs, the current SSL connection remains established until the TCP connection is broken on the OS7000. But due to the periodic bind between the switch and the server, the TCP connection stays up and the SSL handshake is not done again with the new certificate.

If the switch does not reboot more than once a year, user may observe the certificate expiration a long time after it really occurs.

Workaround: There is no known workaround at this time.

PR 68485

policy server load and **policy server flush** provoke a flush of the CAM MAC SA which leads to disconnecting AVLAN users on the OS7000.

Workaround: After loading or flushing a QoS policy, it is necessary to perform a new authentication from AVLAN users.

PR 76820

When user configures the ip helper on the second hop of an OS6624/48 and thus after authentication, the PC is not able to get the ip address. Therefore AOS appears to not be able to learn the MAC where in fact the PC never gets the IP address and thus no traffic from the PC.

Workaround: Configure ip helper on the first hop.

PR 77107

After HTTP authentication on the OS7000, MAC OS X will reset the link and thus all MAC learned are flushed on that port. This will cause the MAC OS X to be de-authenticated.

Workaround: Use a hub between the MAC OS X and the OmniSwitch switches so that the link does not go down.

PR 77987

With traffic on the default VLAN turned on, sometimes unable to obtain IP address via DHCP for the default VLAN's subnet on an OS7000.

Workaround: There is no known workaround at this time.

Policy Server Management

Problem Reports

PR 61677

When the PolicyView application is started on the OS7000, it automatically creates an entry for the policy server on the switch. This entry is on port 389 without SSL enabled. PolicyView cannot specify the mode (SSL or non-SSL) and the port (389 or 636 or another one) which will be used between the LDAP server and the switch. PolicyView does not provide support for SSL. Every time the PolicyView application is opened, an entry on port 389 of the switch will be made automatically, and each time this work around must be done if the user needs SSL.

Workaround: When PolicyView is activated, a policy server using port 389 is systematically created (by PolicyView) on the switch and policy rules are loaded on that connection.

To use an SSL connection between the LDAP server and the switch to download policies:

- 1) Delete the server (with port 389) on the switch through CLI or WebView.
 - 2) Flush the policy manager cache from CLI or WebView.
 - 3) Close the PolicyView application.
 - 4) Create a server using CLI or WebView on the SSL port and use a server with port 636 (SSL).
 - 5) Policies will now be downloaded automatically to the switch from the SSL connection. Otherwise, two instances of the same server will be created (port 389 & 636) and LDAP server with port 389 will be used as primary server.
-

PR 63005

The LDAP client architecture does not take advantage of the referral service on the LDAP server on the OS7000.

Workaround: There is no known workaround at this time.

PR 68906

Sometimes, all the policies do not flush when flushing from WebView.

Workaround: Issue the "policy server flush" command from the command line to delete all the policies.

PR 74062

On an OS6624/6648 system, it is not possible to create an L3 ACL on a source network and another on a destination network because currently the OS66xx cannot link up source and destination.

Workaround: There is no known workaround at this time.

PR 86995

Default port group, "Slot0X", for an OS6624 contains 52 ports instead of 24, 26 or 28 ports.

Workaround: Define and use a port group consisting of the 24, 26 or 28 ports existing on the OS6624.

System

OmniSwitch 8800 Feature Exceptions

- When a chassis is fully loaded with 5 SFM modules, an Amber Light indicates that the module is in Stand-By mode.
-

General

Problem Reports

PR 51067

Switch based telnet client only supports a single user at a time on the OS7000. If one user already has started using the telnet client, and a second user attempts to use the switch based telnet client at the same time, a message will be generated informing the second user that the client is already in use.

The actual message sent is: "Telnet is already in use."

Workaround: There is no known workaround at this time.

PR 51088

The **more** command is not supported on multiple user sessions on the OS7000. Therefore only one instance may be active on a switch at a time. If a second user attempts to use **more**, when it is already active, they will receive the message: **more** is currently in use, try again later.

Workaround: There is no known workaround at this time.

PR 52676

Blocking sockets need to be released when a remote slot goes down on the OS7000.

Workaround: There is no known workaround at this time.

PR 55967

Only terminal ID vt100 is supported on the OS7000. User must set tty terminal type to vt100 to support some switch software that uses ASCII escape codes. Editor 'vi' is an example.

Workaround: There is no known workaround at this time.

PR 59475/59877

Changing from multiple router MAC to single router MAC mode and vice-versa requires a reboot on the OS7000.

Workaround: There is no known workaround at this time.

PR 59510

The time for 10/100 ports to auto-negotiate is dependent upon the number of such ports configured in the OS7000 system. The more ports configured for auto-negotiation, the longer it will take before they all auto-negotiate. This is observed only at bootup.

Workaround: There is no known workaround at this time.

PR 60599

The watch dog will not reboot the switch when the OS7000 locks up due to a corrupted image file.

Workaround: Power cycle the switch and FTP a new version of the software if possible.

PR 60636

Fully qualified instances in "systemMicrocodeDependencyTable", return a NoSuchInstance error on the OS7000. Only SNMP GetNext requests work on the entire table, but SNMP get for specific instances fail.

Workaround: User must use **snmpget** on table to read items.

PR 60675

The MAC-range command will not update the routing information upon completion on the OS7000.

Workaround: For a MAC-range command to take effect (have the chassis use the new MACs), the chassis will need to be rebooted. In fact, once you change the first MAC-range you MUST reboot, all VLAN and routing functionality after that point will not be supported.

PR 61018

While modifying the boot parameters on the OS7000, an input of "." for an IP address is interpreted as an IP address of 0.0.0.0.

Workaround: There is no known workaround.

PR 61534

The FTP session will have problems connecting to the OS7000 while the certify process is still running.

Workaround: Do not attempt to FTP files to/from switch while certify process is still running.

PR 61572

When the protocol reference is not specified in the ethernet frame, layer2 traffic is not accepted on the OS7000.

Workaround: There is no known workaround at this time.

PR 62067

Port link may toggle if using a Media Converter (100BASE-TX to 100BASE-FX) on the OS7000.

Workaround: There is no known workaround at this time.

PR 62628

The ASIC version number is missing from its field when a **show module long** command is issued.

Workaround: There is no known workaround at this time. It is a display issue only.

PR 63605

Some Fweb* images show up in the "loaded m-code" table before the OS7000 reloads.

Workaround: When a switch comes up, the only file that WebView loads is the web.lnk file from Fweb.img. If there is no web access to the switch, nothing else is loaded. When a user accesses a certain page, the system will dynamically load the necessary file. The WebView image/s that show up in the show microcode loaded output is dependent upon what pages were accessed. Therefore these images can vary from switch to switch and from time to time.

PR 63661

The message "KERNAL reboots!" may display when changing system time on the OS7000.

Workaround: If you want to change the system time, do not execute the debug command **debug chassis auto-reboot disable** prior to doing so or your system will reboot.

PR 65248

When the user configures the EMP IP address to "." or 0.0.0.0 in an attempt to clear the address on the OS7000, it will in fact add it as the default route (0.0.0.0).

Workaround: There is no known workaround at this time.

PR 66781

The Operating System does not support non-contiguous MAC ranges on the OmniSwitch 8800.

Workaround: There is no known workaround at this time.

PR 66815

If the working directory is in upper case "WORKING" (normally will happen if it is created on a PC), then the install command from either CLI or WebView will remove Hrelease.img from the working directory getting removed on an OS6624/6648.

Workaround: Rename the upper case "WORKING" directory to a lower case "working" directory. Do not use **rename WORKING working** (this will not work). Rename WORKING to something else first and then rename it back to lower case "working". For example:

```
rename WORKING ttt
rename ttt working
```

PR 67104

During the system bootup sequence, the memory size may not be display the correct value (i.e., 64 or 128 MB) on an OS6624/6648. This is only a cosmetic problem.

Workaround: Ignore the memory size during bootup.

PR 67889

Ixia Scriptmate automates auto-negotiation test. Hence the timing for enabling port (PHY and MAC) between Ixia and the OS8800 is different. Since the OS8800 does not accumulate statistics before the port is enabled, there is a chance to have statistics mismatch between Ixia and the switch.

Workaround: There is no known workaround at this time.

PR 68266

The **show module** command will not work on the OS8800 if the console of one of the 2 CMMs is configured as the modem port with **modemControlOn**.

Workaround: There is no known workaround at this time.

PR 68275

An unknown destination address, under heavy traffic, may exceed the threshold defined for broadcast traffic on an OS6624/6648.

Workaround: There is no known workaround at this time.

PR 68661

Next error message may appear at startup: sync 93: Accept failed [estatus = CS_CSM_INrrno 5] on an OS6624/6648.

Workaround: There is no known workaround at this time.

PR 68905

ColdStartTrap is sent every time a switch is reset.

Workaround: There is no known workaround at this time.

PR 69073

Stck: Non-Primaries needs to send checksum info to Primary event if CVM action fails (autoCertify).

Workaround: Make those stacks a standalone first, remove any un-needed files, make sure the flash contains at least 4 Meg of free space, and then connect the stack back with the other stacks.

PR 69778

GBIC part number information will not be displayed using CLI commands **show ni** and **show module long** on the OS7000.

Workaround: There is no known workaround at this time.

PR 70760

Highly fragmented file system can slow file system response.

Workaround: Use the **fsck** command on your fragmented file system. If this improves the file system performance.

PR 70885

The System can't detect Smurf attacks to the switch.

Workaround: There is no known workaround at this time.

PR 70886

The System can't detect Pepsi attacks to the switch.

Workaround: There is no known workaround at this time.

PR 70887

BOP can't detect TCP SYN flood attacks to the switch.

Workaround: There is no known workaround at this time.

PR 71482

Under heavy traffic conditions or with hotswap of NI / takeover, you may see the following message on the screen: "Panic: netJobAdd: ring buffer overflow". Functionality on this NI may be lost and switch will rarely reboot itself.

Workaround: There is no known workaround at this time.

PR 72271

When building a new stack using up and running standalone units on an OS6624/OS6648, they system may experience multiple unit reboots and takeovers which might leave the stack in an unstable state.

Workaround: Never connect together or add running standalone units to a stack. Always turn the standalones off, connect them to the stack, and then turn them on.

PR 72648

The 5.1.4 **boot.cfg** file may not be compatible with earlier versions of code.

Workaround: Use the **boot.cfg** file of the earlier version of code.

PR 73037

If a port on the OS7000 is disconnected and reconnected while sending traffic from a traffic generator at a high rate, the port does not become active until the traffic rate decreases.

Workaround: Stop the traffic for a moment before restarting the traffic generator.

PR 74724

The CPU utilization of the system remains high while the system is flushing a big number of IP addresses. The CPU utilization returns to normal once the entire process is completed.

Workaround: There is no known workaround at this time.

PR 75615

On an OS6600, a "continuous Flash synchro" process may occur if the local "working" and "certified" directories are not "Certified".

Workaround: When connecting stacks to other stacks, make sure individual stacks are synchronized between themselves. That is, locally (Working and Certified) and within each module within current stack environment.

PR 76349

On the OS7000, admin down on a port cannot bring down the link on the link partner. As a result, the link partner can detect LINK UP or toggling UP and DOWN.

Workaround: There is no known workaround at this time.

PR 76500

Flash File System May be corrupted after Certify, Restore or Flash Synchro process.

Workaround: There is no known workaround at this time.

PR 76658

MAC Server manager a range of max 256 MACs. If the OS7000 is configured with a MAC range exceeding 256 MACs, MAC server will not be consistent. The MAC range eeprom CLI command rejects the command if the MAC count exceeds 256.

Workaround: Reconfigure the MAC-range eeprom to be 256 MACs or less

PR 77208

If the system watch dog times out on an OS6624/6648, the console may hang after reboot on the primary switch and rebooted again.

Workaround: There is no known workaround. The system will reboot and recover itself.

PR 79104

On the OS6600, when using Webview, if the configuration is changed and a write memory performed, webview is unable to determine that a certify is required (copying the change from working to certified).

Workaround: After performing the write memory action, click refresh on webview page. Then copy working to certified from webview is successful.

PR 79859

Firmware reversion is not shown using SNMP on the OS7000.

Workaround: There is no known workaround at this time.

PR 80937

IPC buffers can be used up by VLAN Manager on an OS8800 when a bootup or CMM takeover occurs.

Workaround: There is no known workaround at this time.

PR 82090

On the OS7000, while ftp'ing in the miniboot, transfer may stop after which no IP traffic of any kind will be returned.

Workaround: Reboot back into the miniboot and finish transferring the files.

PR 82635

On the OS7000, there is no SNMP MIB support to display number and status of fan modules on a switch via SNMP MIB Browsers and WebView. The number and status of fans can be displayed only via the CLI interface's command: **show fan**.

Workaround: There is no known workaround at this time.

PR 82675

If the boot flag is set to 0x40000, then it will cause the tssApp task to crash when attempting to execute some CLI commands on an OS7000 or OS6600.

Workaround: Make sure boot flag is set to 0.

PR 83669

Chassis will not be able to bootup when the boot flag is set to 0xb8000 on an OS7000.

Workaround: Do not set the boot flag to 0xb8000.

PR 84453

On an OS6600, Chassis Supervision does not know if the configuration on the NI side has been modified and then to reload the corresponding NI in case of a takeover with unsaved configs.

Workaround: Reboot the stack.

PR 84469

OS6600 system rebooted with dump file while certifying image.

Workaround: There is no known workaround at this time.

PR 84483

On the OS7000, at the end of the actual fpga driver downloading, there is a short period of wait before the whole update process is declared ended.

Workaround: There is no known workaround at this time.

PR 85230

On the OS7000, when a user does not follow the steps of the automated fpga update procedure and repeatedly issues the fpga update command, the update may be completed correctly.

Workaround: Following the formal fpga update procedure recommended in the user's manual, users will not encounter this problem.

NIs—General

Problem Reports

PR 62573

For following modules, PAUSE frames will be generated per port when the port is oversubscribed: OS7-ENI-C24 and OS7-ENI-FM12, OS7-GNI-U2, OS8-GNI-C8, OS8-GNI-U8 and OS66-GNI-C2.

Workaround: There is no known workaround at this time.

PR 72828

On the OS7000/8800, oversubscribing the egress gigabit module at a rate exceeding 3:1, will result in higher priority traffic sharing the bandwidth equally with lower priority traffic.

Workaround: There is no known workaround at this time.

PR 79427

On the OS7000, there is a compatibility issue with the latest IXIA release, 3.65. Throughput test on ENI-C-24 couldn't get 100 percent.

Workaround: Hash should be manually updated.

PR 86084

The configuration file from 5.1.4 or older releases could not be compatible for autonegotiation if either speed or duplex is set to non-auto.

On such releases, autonegotiation was automatically disabled and saved in the boot.cfg configuration file.

Workaround: Enable autonegotiation and save the config.

System

OmniSwitch 6600

Problem Reports

PR 83540

NTP synchronized time does not include daylight savings time.

Workaround: Do not set system date backward of current date.

PR 87865

Changing switch timezone causes double free of memory environment variable. Problem arises is multiple changes made to timezone.

Workaround: Do not make multiple changes of the system timezone setting.

OmniSwitch 7000 NIs

Problem Reports

PR 34227

Only 32K address seen bits are available to support aging out of the pseudoCAM entries.

Workaround: There is no known workaround at this time.

PR 35050

Jumbo frames cannot be fragmented when bridged.

Workaround: There is no known workaround at this time.

PR 43852

Pause frame with multicast address (01-80-C2-00-00-01) causes switch to flood frames to other ports.

Workaround: There is no known workaround at this time.

PR 58485

Configured egress flood and multicast limits are not exact. There will be a small deviation from the configured limits depending on the packet size.

Workaround: There is no known workaround at this time.

PR 61916

Fast Ethernet ports not able to auto detect speed and duplex setting with some cards. Seen with Dolch sniffer.

Workaround: Manually configure the speed and duplex settings.

PR 65197

The **qos default queues** command may cause the NI to have a different configuration than the CMM.

Workaround: The **qos default queues <num>** command requires a reset of the NI before it takes affect. One can reset the NI by doing a **no power ni <num>** then **power ni <num>** or do a **reload working no roll-back** to have the setting take effect.

PR 69099

Pause frames cannot be generated by the MAC when oversubscribing a single port.

Workaround: There is no known workaround at this time.

PR 71106

Using Xircom CreditCard Ethernet 10/100 + Modem 56, if the speed and duplex of both the OS7-ENI-C24 switch and the NIC are fixed to 100FD, then no link is detected.

If auto-negotiation is enabled on the switch the connection is only detected as 100HD, even though the NIC is configured to 100FD.

Workaround: By using auto-negotiation, a link can be detected, although this will only be 100HD and not 100FD.

PR 71593

Avaya Cajun P333R has connectivity issues when connected to the OS7000.

Workaround: There is no known workaround at this time.

PR 77702

A four-port NetGear Hub gives an uneven number of preamble bytes that will be dropped.

Workaround: Use the 8-port Hub NetGear DS108.

PR 80023

Without a common denominator, a link doesn't come up when either or both sides turns on autonegotiation. For example, when autonegotiation is turned on a port on a switch, the link stays down if the link partner has:

- Autonegotiation turned off and local port is enforced to FULL duplex; or,
- Autonegotiation turned on, but speed mismatches other than auto; or,
- Autonegotiation turned on, but duplex mismatches other than auto.

Workaround: This follows IEEE 802.3 recommendations. Both sides should have a common denominator. Either the switch side or remote side should change the configuration.

PR 80710

OS7-ENI-P24 modules have egress flood rates lower than the regular ENI_C_24 modules.

Workaround: There is no known workaround at this time.

System

OmniSwitch 8800 NIs

Problem Reports

PR 66750

OS8800 ENI encountered packet loss on Coronado.

Workaround: There is no known workaround at this time.

PR 67570

On the OS8-GNI-C8 incoming frames are accumulated by the statistics handler if and only if the port is enabled. If the port is not enabled yet, any incoming frames will be dropped. As a result, statistics between switch and traffic generator might be different.

Workaround: There is no known workaround at this time

PR 68883

When the speed is changed on ENI modules (10M to 100M or vice-versa), the far end is supposed to detect this change if configured as auto. If it does not detect this condition, then the link will be down.

Workaround: Configure the far end or toggle the link status locally to restart the auto negotiation process.

PR 69545

No GBIC information is shown when the **show module long** command is issued on an OS8-GNI-U24. This is harmless and will not affect switch behavior.

Workaround: There is no known workaround at this time.

PR 76652

On OS8800 switches, when broadcast packets inflow to a port, if it is mixed with different sizes, some smaller size packets could be dropped by the system.

Workaround: There is no known workaround at this time.

PR 79957

It is found that under 13 hours of stressed traffic test with PAUSE flow control on 10G, less than 100 PAUSE frames were seen with CRC error, none on data frame. Broadcom has been notified but they have not been able to provide any answer. However, this should not be an issue as the default PAUSE setting is OFF and the rate of corruption is extremely low (<100 out of 23 millions PAUSE frames).

Workaround: Do not turn on PAUSE flow control in 10G.

PR 79958

It is found that after a CLI command issuing an ADMIN DOWN to a 10G link, a few corrupted packets are seen on the remote station. This is believed to be a side effect of Xenpak which chop off the packet abruptly when the Rx and Tx link is disabled. However, this happens only under very heavy traffic.

Workaround: There is no known workaround at this time.

PR 80442

Error message “No Such Object available on this agent” returned for 10G specific tables. This problem only occurs with SNMP walk application.

Workaround: There is no known workaround at this time.

PR 81010

OS8-GNI-C-24 may encounter some packet loss for a small size packets if it is wired traffic (100% traffic inflow).

Workaround: This is an oversubscription condition. Lower the incoming traffic rate.

PR 81489

The BCM 5632 can hang while waiting for EEPROM config download during boot up. The 10G interface will never come up if this situation occurs.

Workaround: Power the NI module off and then on again.

PR 81727

Unable to set primary Xenpak from WebView or OmniVista.

Workaround: Use CLI command.

PR 83062

The 10G interface may not come up upon initial boot up while traffic is running. It may be due to insufficient internal IPC resource.

Workaround: Plug the fiber in after the switch boot up or NI hot swap.

PR 84585

The interface may bounce for no apparent reason, i.e., the link did not go down. However, so far this has happened very infrequently. It may be due to some internal chip access issue but needs to be monitored and verified in next release.

Workaround: There is no known workaround at this time.

Power over Ethernet

Problem Reports

PR 79947

There is no support for driving LED's on ENI-P24 with 5.1.4.R05 release

Workaround: There is no known workaround at this time.

PR 83921

On occasion a message "i2c ReadOnBoardTemp ERROR Status Returned STR" will be displayed when running a stack of 8 OS6600-P24.

Workaround: There is no known workaround at this time.

PR 84290

Hot swap on OS6600-P24 stack can cause the following non-fatal error to occur:

FRI JUL 16 16:02:26 : LANPOWER (108) error message:

+++ lpSocketSend: zcSendto Failed ret -6 size 532!

+++ lpSendPdData: Unable to send data to CMM

Workaround: No action necessary.

PR 84565

Capacitor Detection becomes disabled upon takeover on OS6600-P24. This will be noticeable when non-compliant 802.3af devices are not powered up after takeover.

Workaround: Simply run lanpower <slot> capacitor-detect command on primary.

PR 84710

On the OS6600, the identifiers returned are not in the correct format.

Workaround: None

Redundancy / Hot Swap

CMM Redundancy Feature Exceptions for OmniSwitch 7000/8800

- 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 OS7000/8800 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 configs, 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.
-

Hot Swap Feature Exceptions for OmniSwitch 7000/8800

- Hot swap of NIs needs to be preceded by the removal of all cables connected to the NI.
 - Hot insertion of unlike modules is not supported in this release. Support is planned in next maintenance release.
 - The **Reload NI** command is not supported in this release. 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 6600

- 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.
 - When inserting a new module in the stack, make sure that the new element is synchronized by itself.
-

Hot Swap Time Limitations for OmniSwitch 7000/8800

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

CMM Redundancy / Hot Swap Feature Exceptions

- If you do a write memory, and do not do a certify (**copy working certified**) before doing a **takeover** or **reload primary**, you will lose the boot.cfg contents because the secondary will do an automatic **restore** (copy certified working) when it comes up as the secondary. This allows it to be ready for failovers.

Redundancy / Hot Swap

Problem Reports

PR 54530

An uncontrolled power down could potentially cause the OS7000 CMM to fail.

Workaround: There is no known workaround at this time.

PR 62355

The Feni.img image is not listed as loaded microcode on the secondary CMM, nor will it be on the primary CMM after takeover on OS7000's. This should not affect the functionality of the switch.

Workaround: There is no known workaround at this time.

PR 62403

Voice conversation drops and IP phones directly connected to OS7000 may reboot when a takeover of CMM is issued.

Workaround: Wait until the NI is not busy before hot swapping to avoid this situation.

PR 62534

If a takeover is done after uploading a new **boot.cfg** file, both the OS7000 CMMs could end up trying to be the Primary CMM upon doing reloads.

Workaround: Whenever a new boot.cfg file is loaded into the working directory, the **reload working no rollback-timeout** command has to be issued. This insures that the NIs are properly reloaded and the new configurations are sent to the NIs.

PR 64385

With many layer 3 table entries, takeover from the Secondary is not reliable on the OS7000. Communication between the CMM and NI's fail.

Workaround: There is no known workaround at this time.

PR 66098

The user may see the following message on bootup : "*CSM_PI_4 - csCsmCmmCtx.cmmState = 9*" on the OS7000. This is an informational message indicating that a timeout has occurred during system bootup.

Workaround: There is no known workaround at this time.

PR 67150

If modules are in the middle of a Flash Synchro and a takeover process is issued (both from user or from SM detection), stacks will get into an unstable condition.

Workaround: DO NOT perform (manually) a takeover while Flash Synchro is in progress.

PR 67483

copy flash-synchro will not work between different release versions of code

Workaround: Both CMM's must have the same release version. If not, do the following:

1. Load each CMM separately with the new release in the "working" directory. When doing this, only one CMM should be plugged into the chassis.
 2. Perform **reload working no roll-back** on each CMM.
 3. On each CMM, perform **copy working certified**.
 4. Bring up chassis with both CMMs.
 5. Perform **copy flash-synchro** from the primary CMM.
-

PR 68756

On the OmniSwitch 6624/6648, Temperature Warning threshold is not kept after a takeover.

Workaround: Reset temperature warning threshold again after a takeover.

PR 68913

In case of a takeover, cmmAUnPlugged and cmmBUnplugged alert traps will not be sent on the OS7000.

Workaround: There is no known workaround at this time.

PR 69926

When a CMM takeover occurs on the OmniSwitch 8800, a momentary loss of multicast traffic will be experienced.

Workaround: There is no known workaround at this time.

PR 70127

On the OS6600, when we split the stacks into 2 or more substacks, an STR message of unauthorized CSM socket may be seen on the current Primary Stack.

Workaround: Please ignore this message. If you are missing one of the messages, it will be retransmitted and the system will be fine.

PR 72041

Synchronization of flash will fail if the elements are not running the same version of code.

Workaround: Only inserting the same version of software is supported. If this situation occurs, follow the steps below to synchronize the flash to upgrade the stand alone unit to the same version before inserting:

1. Separate the elements of the stack to form two stacks; each running the same release version.
 2. Upgrade one of the two stacks to the same release version as the other.
 3. Reconnect the two stacks together to reform the initial stack.
-

PR 73460

Rarely, on takeovers, the "ipmem" task may crash. Switch must be rebooted to recover.

Workaround: There is no known workaround at this time.

PR 73895

On takeover, the NI LED momentarily displays amber.

Workaround: This is normal behavior indicating NI acknowledgement of takeover.

PR 75043

Changes made but not saved on a redundant CMM setup will not be reflected in the synchronization state on the OS7000. The user may be unaware based on **show running-directory** that the NIs will all reset on takeover.

Workaround: Changes in configuration should be saved and synchronized for redundant CMMs.

PR 77206

On an OS7000, during a takeover or failover, due to the IP Stack transition, some of the messages may not be able to log to a remote device if one enables the syslog mechanism. This period may be in the boundary of a second.

Workaround: There is no known workaround at this time.

PR 78550

Sometimes logging in and out of a CMM that has newly been made the primary CMM in a redundancy takeover will cause a continuous stream of ioctl messages about lost file descriptors.

Workaround: Perform a "reload all" command to reboot the switch.

PR 79063

Flash Synchro successful, but show running shows CMMs NOT SYNC when new folder is created in / working on the OS7000.

Workaround: Do not create other folders in the Working directory.

PR 79991

On OS6600 series switches, inserting an element with a different release may result in rendering some elements unoperational.

Workaround: Only inserting the same version of software is supported. Upgrade the element(s) running on a different release to the same release level of the stack in which the element(s) will be inserted.

PR 80356

On OS6600 series switches, flash synchronization may fail when we connect a certified stack with a non-certified stack (Primary).

Workaround: Make sure both (working and certified) directories are certified before connecting it to any stacks.

PR 84317

Do not reload the NIs on an OS6600 in case of takeovers with unsaved configs due to some limitations. The unsaved running config is still being applied on the NIs even though the new primary cannot see that portion of the config update. Since the takeover did not reload this NI, the applied GM rules are still in effect.

Workaround: Reboot the stack.

PR 84483

At the end of the actual fpga driver downloading, there is a short period of wait before the whole update process is declared ended. This does not affect the normal operation in any way.

Workaround: There is no known workaround at this time.

PR 84648

Takeovers on updated running configs reset the NIs but they don't come back up on a OS7000. Resetting of the NIs is normal in this case where the running configs have been changed and not committed to the memory and the CMMs have not been synch'd.

Workaround: Another takeover or chassis reboot is required to bring the NIs back up again.

PR 85838

515R04 is NOT backward compatible in term of flash synchro with any of the previous builds.

Workaround: On dual CMM systems (7000 & 8000 series), once users have upgraded existing build to 515R04, if there is any need to downgrade the running build back to the previous running build, they will have to downgrade each CMM individually, then plug them together.

PR 87051

Reload prompt overrides all other session responses on the OS7000.

Workaround: Prior to issuing reload or reboot, ensure all sessions are closed. Use kill command to remove other sessions. Do not issue reload or reboot prompt without fully committed to action.

Technical Support

Alcatel 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	+33-388-55-69-04
Asia Pacific	+65-394-7933
Other International	818-878-4507

Email: support@ind.alcatel.com

Internet: Customers with Alcatel service agreements may open cases 24 hours a day via Alcatel's support web page at: <http://eservice.ind.alcatel.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.