Release Notes
OmniSwitch 6600/7000/8800
Release 5.1.6.R02

These release notes accompany release 5.1.6.R02 software for the OmniSwitch 6600 family 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 family 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

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 Family Getting Started Guide*

  Describes the hardware and software procedures for getting an OmniSwitch 6600 Family switch up and running.

- *OmniSwitch 6600 Family Hardware User Guide*

  Complete technical specifications and procedures for all OmniSwitch 6600 Family switches, power supplies, fans, and Network Interface (NI) modules.

- *OmniSwitch 6600 Family 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 6600 Family 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 6600 Family* 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 5.1.6.R02*

  Provides instructions for upgrading the switch software.

System Requirements

Memory Requirements

- OmniSwitch 6624 Release 5.1.6.R02 requires 128 MB of SDRAM and 32MB of flash memory. This is the standard configuration shipped.
- OmniSwitch 6648 Release 5.1.6.R02 requires 128 MB of SDRAM and 32MB of flash memory. This is the standard configuration shipped.
- OmniSwitch 6600-U24 Release 5.1.6.R02 requires 128 MB of SDRAM and 32MB of flash memory. This is the standard configuration shipped.
- OmniSwitch 6600-P24 Release 5.1.6.R02 requires 128 MB of SDRAM and 32MB of flash memory. This is the standard configuration shipped.
- OmniSwitch 6602-24 Release 5.1.6.R02 requires 128 MB of SDRAM and 32MB of flash memory. This is the standard configuration shipped.
- OmniSwitch 6602-48 Release 5.1.6.R02 requires 128 MB of SDRAM and 32MB of flash memory. This is the standard configuration shipped.
- OmniSwitch 7700 Release 5.1.6.R02 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 5.1.6.R02 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 5.1.6.R02 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 6600

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 5.1.6.R02. 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 OS7700 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 5.1.6.R02

Instructions for upgrading to 5.1.6.R02 (image files, Miniboot, Bootrom, FPGA) are available on the Customer Support website along with the 5.1.6.R02 software (http://eservice.ind.alcatel.com).

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

Note. Once you have upgraded to 5.1.6.R02, downgrading the system must be done on each CMM separately.

Note. Due to changes in such features as STP and the new **ip interface** command, **Release 5.1.6.R02 configuration files are *not* backwards compatible to Release 5.1.5.x and earlier. Therefore, Alcatel recommends that you back up your configuration files before performing an upgrade.**

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 that 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 Family Getting Started Guide*.

5 Connect the two stacks together into one stack. Refer to *OmniSwitch 6600 Family 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

No new hardware has been introduced in release 5.1.6.R02.

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
802.1s Multiple Spanning Tree	all	base
802.1x Multiclient Support	all	base
802.1x Guest VLAN Support	all	base
ARP Filtering	all	base
Copper Gigabit SFP Support	OS6600	base
Configurable Flood Queue Bandwidth for High Availability VLANs	OS7000/OS8800	base
DoS Phase 1 (Pinpoint which device is doing a DoS with OmniVista)	all	base
EtherType Prioritization	OS7700/OS7800/OS8800	base
Fixed Management IP Address for Traps	all	base
Generic UDP Relay	OS6600	base
Improved Spanning Tree Support for High Availability VLANs	OS7000/OS8800	base
IPv6	all	base
IP Loopback0 Interface	all	base
LPS Release Command	all	base
Multinetting	OS7700/OS7800/OS8800	base
Port Monitoring	OS6600	base
SLB Probes	OS7700/OS7800/OS8800	base
VRRP Traceroute	all	base

Feature Descriptions

802.1s Multiple Spanning Tree

The Alcatel Spanning Tree implementation provides support for the IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), 802.1W Rapid Spanning Tree Algorithm and Protocol (RSTP), and the 802.1D Spanning Tree Algorithm and Protocol (STP). All three supported protocols ensure that there is always only one data path between any two switches for a given Spanning Tree instance to prevent network loops.

802.1s MSTP is based on 2003 802.1Q standard. MSTP allows the configuration of Multiple Spanning Tree Instances (MSTIs) in addition to the CST instance. Each MSTI is mapped to a set of VLANs. As a result, flat mode can now support the forwarding of VLAN traffic over separate data paths.

In addition to 802.1s MSTP support, the 802.1D STP and 802.1W RSTP are also available in either the flat or 1x1 mode. The flat mode applies a single spanning tree instance across all VLAN port connections on a switch. However, if using 802.1D or 802.1W in the flat mode, the single spanning tree instance per switch algorithm applies.

A new path cost mode command is available to control whether the switch uses a 16-bit port path cost (PPC) or a 32-bit PPC. When a 32-bit PPC switch connects to a 16-bit PPC switch, the 32-bit switch will have a higher PPC value that will advertise an inferior path cost to the 16-bit switch. In this case, it may be desirable to set the 32-bit switch to use STP or RSTP with a 16-bit PPC value.

By default, the path cost mode is set to automatically use a 16-bit PPC value, which is used for all ports that are associated with an STP (802.1D) instance or an RSTP (802.1w) instance, and a 32-bit value for all ports associated with an MSTP (802.1s) value. It is also possible to configure the path cost mode to always use a 32-bit PPC regardless of which protocol is active.

802.1x Multiple Client Support

Physical devices attached to a LAN port on a switch through a point-to-point LAN connection may be authenticated through the switch via port-based network access control. This control is available through the IEEE 802.1X standard, which uses the Extensible Authentication Protocol (EAP) and includes three components: a supplicant device, an authenticator (the switch), and an authentication server. On the OmniSwitch, only RADIUS servers are currently supported for 802.1X authentication.

This implementation of 802.1X supports the authentication of multiple clients (supplicants) per physical 802.1X port. After successful authentication, clients are eligible for assignment to one or more VLANs.

In addition, interoperability between Alcatel 802.1x and Sygate Management Server (SMS) and Sygate Enforcer is also supported. The login identity field in Alcatel 802.1x authentication can be up to 63 bytes (e.g., Sygate).

Note. On the OmniSwitch 6600 switches, only one VLAN can be assigned to a single physical port. Multiple clients are supported on OmniSwitch 6600s, but all clients need to be assigned to the same VLAN.

802.1X Guest VLAN Support

An optional guest VLAN feature is now available for 802.1X ports. Clients that are connected to an 802.1x port that do not send EAP- Request/Identity frames within a configurable number of polling attempts, are identified as non-802.1x clients. If a guest VLAN is configured for an 802.1X port, the MAC address of the non-802.1x client is learned in the guest VLAN. If a guest VLAN is not configured for the 802.1X port, the client is blocked.

Note that on an OmniSwitch 6600 switch, guest VLAN access is only available when there is no other 802.1x client on the port. If a device is learned in the guest VLAN and an 802.1x client successfully authenticates on the same port, the guest VLAN client is dropped. In addition, an 802.1x port may only have an association with one VLAN at a time. Multiple VLAN membership is currently not supported on this platform.

The number of times the switch polls a device for EAP frames is a user- defined value. The polling interval time is set to 0.5 seconds between each retry. This interval is not configurable.

ARP Filtering

The extended proxy ARP process allows you to block specific IP addresses in order to block the switch from providing ARP replies for the specified IP address(es). This is primarily to get answers on ARP requests from local clients.

Copper Gigabit SFP Support on OmniSwitch 6600 Family

In release 5.1.6.R01 and later, copper Gigabit SFPs are now supported on OmniSwitch 6600 Family switches. These SFPs can be used with the built-in Gigabit uplink slots on the OS6602-24 and OS6602-48 switches and on the OS6600-GNI-U2 uplink submodule.

Note. Copper Gigabit SFPs on OmniSwitch 6600 Family switches support 1000 Mbps and full duplex. They do not support 10 or 100 Mbps speeds or half duplex mode.

Configurable Flood Queue Bandwidth for High Availability VLANs

The ingress flood queue bandwidth size for high availability VLANs is now a configurable value. By default, the bandwidth size is 15 Mbps and can be set to a maximum of 1000 Mbps with a minimum of 1 Mbps. This queue is created when the first high availability VLAN becomes active and is removed when the last high availability VLAN is deleted.

DoS Phase 1

The Alcatel DoS trap has been enhanced so that it now provides the source address of the device performing the DoS attack. This is particularly useful for OmniVista.

A trap will be generated if configured on the switch to indicate an offensive device.

EtherType Prioritization

A new QoS policy condition is now available to classify and prioritize traffic based on EtherType. When a rule is created and applied using this new condition, traffic containing the specified EtherType is identified and then queued to a higher priority queue.

Note. This feature is not supported on traffic received with an 802.1Q tag.

Fixed Management IP Address for Traps

One single IP address of a switch with multiple routed VLANs is now used as the source IP address sent on every SNMP request or trap. When a trap is sent from the switch, the source IP address is the same as the IP address configured by the **ip router router-id** command. If no address is configured by the **ip router router-id** command, then the default value for **router-id** will be the primary IP address of the VLAN with the lowest VLAN identifier.

Note. You cannot remove the ip router router-id from CLI. You need to delete the line from the boot.cfg and reboot the switch.

Generic UDP Relay

In addition to BOOTP/DHCP relay, generic UDP relay is now available on OmniSwitch 6600 switches. Using generic UDP relay, traffic destined for well-known service ports (e.g., NBNS/NBDD, DNS, TFTP, and TACACS) or destined for a user-defined service port can be forwarded to a maximum of 256 VLANs on the switch.

Improved Spanning Tree Support for High Availability VLANs

High Availability (HA) VLANs now run on inter switch links in conjunction with spanning tree. All spanning tree modes and protocols are supported (flat, 1x1, 802.1d, 802.1w, and 802.1s).

IPv6

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

- Address size increased from 32 bits (IPv4) to 128 bits (IPv6)
- Dual Stack IPv4/IPv6
- ICMPv6
- Neighbor Discovery
- Stateless Autoconfiguration
- RIPng
- Static Routes
- Tunneling: Configured and 6-to-4 dynamic tunneling
- Ping, traceroute
- FTP and Telnet servers
- DNS client using AAAA records

IP LoopBack0 Interface

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

LPS Release Command

After a security violation occurs, the LPS port is either administratively disabled or filters traffic from one or more source MAC address. The new **port-security release** CLI command is used to return the port to normal operation without having to manually reset the port and/or module.

Multinetting

This feature allows IP traffic from multiple subnets to coexist on the same VLAN. A network is said to be multinetted when multiple IP subnets are brought together within a single broadcast domain (VLAN). It is possible to assign up to eight different IP interfaces per VLAN.

Port Monitoring

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

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

SLB Probes

Server Load Balancing (SLB) probes allow you to check the health of logical SLB cluster and physical SLB servers. Supported features include:

- Support for Server Health Monitoring using Ethernet link state detection
- Support for Server Health Monitoring using IPv4 ICMP Ping
- Support for Server Health Monitoring using a Content Verification Probe.

VRRP Traceroute

The ability to do a traceroute to a virtual VRRP interface on OmniSwitch 6600, 7700, 7800, and 8800 switches is now supported. This is enabled by default.

Supported Traps

The following traps are supported in 5.1.6.R02:

No.	Trap Name	Description
0	coldStart	The SNMP agent in the switch is reinitiating and its configuration may have been altered.
1	warmStart	The SNMP agent in the switch is reinitiating itself and its configuration is unaltered.
2	linkDown	The SNMP agent in the switch recognizes a failure in one of the communications links configured for the switch.
3	linkUp	The SNMP agent in the switch recognizes that one of the communications links configured for the switch has come up.
4	authenticationFailure	The SNMP agent in the switch has received a protocol message that is not properly authenticated.
5	entConfigChange	An entConfigChange notification is generated when a conceptual row is created, modified, or deleted in one of the entity tables.
6	aipAMAPStatusTrap	The status of the Alcatel Mapping Adjacency Protocol (AMAP) port changed.
7	aipGMAPConflictTrap *This feature in not supported	Indicates a Group Mobility Advertisement Protocol (GMAP) port update conflict.
8	policyEventNotification	The switch notifies the NMS when a significant event happens that involves the policy manager.
9	chassisTrapsStr	A software trouble report (STR) was sent by an application encountering a problem during its execution.
10	chassisTrapsAlert	A notification that some change has occurred in the chassis.
11	chassisTrapsStateChange	An NI status change was detected.
12	chassisTrapsMacOverlap	A MAC range overlap was found in the backplane eeprom.
13	vrrpTrapNewMaster	The SNMP agent has transferred from the backup state to the master state.
14	vrrpTrapAuthFailure	A packet was received from the network whose authentication key conflicts with the switch's authentication key or type.
15	healthMonDeviceTrap	Indicates a device-level threshold was crossed.
16	healthMonModuleTrap	Indicates a module-level threshold was crossed.
17	healthMonPortTrap	Indicates a port-level threshold was crossed.
18	bgpEstablished	The BGP routing protocol has entered the established state.

No.	Trap Name	Description
19	bgpBackwardTransition	This trap is generated when the BGP router port has moved from a more active to a less active state.
20	esmDrvTrapDropsLink	This trap is sent when the Ethernet code drops the link because of excessive errors.
21	pimNeighborLoss	Signifies the loss of adjacency with a neighbor device. This trap is generated when the neighbor time expires and the switch has no other neighbors on the same interface with a lower IP address than itself.
22	dvmrpNeighborLoss	A 2-way adjacency relationship with a neighbor has been lost. This trap is generated when the neighbor state changes from “active” to “one-way,” “ignoring” or “down.” The trap is sent only when the switch has no other neighbors on the same interface with a lower IP address than itself.
23	dvmrpNeighborNotPruning	A non-pruning neighbor has been detected in an implementation-dependent manner. This trap is generated at most once per generation ID of the neighbor. For example, it should be generated at the time a neighbor is first heard from if the prune bit is not set. It should also be generated if the local system has the ability to tell that a neighbor which sets the prune bit is not pruning any branches over an extended period of time. The trap should be generated if the router has no other neighbors on the same interface with a lower IP address than itself.
24	risingAlarm	An Ethernet statistical variable has exceeded its rising threshold. The variable’s rising threshold and whether it will issue an SNMP trap for this condition are configured by an NMS station running RMON.
25	fallingAlarm	An Ethernet statistical variable has dipped below its falling threshold. The variable’s falling threshold and whether it will issue an SNMP trap for this condition are configured by an NMS station running RMON.
26	stpNewRoot	Sent by a bridge that became the new root of the spanning tree.
27	stpRootPortChange	A root port has changed for a spanning tree bridge. The root port is the port that offers the lowest cost path from this bridge to the root bridge.
28	mirrorConfigError	The mirroring configuration failed on an NI. This trap is sent when any NI fails to configure mirroring. Due to this error, port mirroring session will be terminated.

No.	Trap Name	Description
29	mirrorUnlikeNi	The mirroring configuration is deleted due to the swapping of different NI board type. The Port Mirroring session which was active on a slot cannot continue with the insertion of different NI type in the same slot.
30	slPesudoCAMStatusTrap	The trap status of the Layer 2 pesudoCAM for this NI.
31	unused	
32	unused	
33	slbTrapOperStatus	A change occurred in the operational status of the server load balancing entity.
34	ifMauJabber	This trap is sent whenever a managed interface MAU enters the jabber state.
35	sessionAuthenticationTrap	An authentication failure trap is sent each time a user authentication is refused.
36	trapAbsorptionTrap	The absorption trap is sent when a trap has been absorbed at least once.
37	alaStackMgrDuplicateSlotTrap	Two or more slots claim to have the same slot number.
38	alaStackMgrNeighborChangeTrap	Indicates whether or not the stack is in loop.
39	alaStackMgrRoleChangeTrap	Indicates that a new primary or secondary stack is elected.
40	lpsViolationTrap	A Learned Port Security (LPS) violation has occurred.
41	alaDoSTrap (*See note at the end of the table)	Indicates that the sending agent has received a Denial of Service (DoS) attack.
42	gmBindRuleViolation	Occurs whenever a binding rule which has been configured gets violated.
43	unused	
44	unused	
45	unused	
46	unused	
47	pethPsePortOnOffNotification	Indicates if power inline port is or is not delivering power to the a power inline device.
48	pethPsePortPowerMaintenanceStatusNotification	Indicates the status of the power maintenance signature for inline power.
49	pethMainPowerUsageOnNotification	Indicates that the power inline usage is above the threshold.
50	pethMainPowerUsageOffNotification	Indicates that the power inline usage is below the threshold.
51	ospfNbrStateChange	Indicates a state change of the neighbor relationship.

No.	Trap Name	Description
52	ospfVirtNbrStateChange	Indicates a state change of the virtual neighbor relationship.
53	httpServerDoSAttackTrap	This trap is sent to management station(s) when the HTTP server is under Denial of Service attack. The HTTP and HTTPS connections are sampled at a 15 second interval. This trap is sent every 1 minute while the HTTP server detects it is under attack.
54	alaStackMgrDuplicateRoleTrap	The element identified by alaStackMgrSlotNI-Number detected the presence of two elements with the same primary or secondary role as specified by alaStackMgrChasRole on the stack.
55	alaStackMgrClearedSlotTrap	The element identified by alaStackMgrSlotNI-Number will enter the pass through mode because its operational slot was cleared with immediate effect.
56	alaStackMgrOutOfSlotsTrap	One element of the stack will enter the pass through mode because there are no slot numbers available to be assigned to this element.
57	alaStackMgrOutOfTokensTrap	The element identified by alaStackMgrSlotNI-Number will enter the pass through mode because there are no tokens available to be assigned to this element.
58	alaStackMgrOutOfPassThroughSlotsTrap	There are no pass through slots available to be assigned to an element that is supposed to enter the pass through mode.
59	gmHwVlanRuleTableOverloadAlert	An overload trap occurs whenever a new entry to the hardware VLAN rule table gets dropped due to the overload of the table.
60	lnkaggAggUp	Indicates the link aggregate is active. This trap is sent when any one port of the link aggregate group goes into the attached state.
61	lnkaggAggDown	Indicates the link aggregate is not active. This trap is sent when all ports of the link aggregate group are no longer in the attached state.
62	lnkaggPortJoin	This trap is sent when any given port of the link aggregate group goes to the attached state.
63	lnkaggPortLeave	This trap is sent when any given port detaches from the link aggregate group.
64	lnkaggPortRemove	This trap is sent when any given port of the link aggregate group is removed due to an invalid configuration.
65	pktDrop	The pktDrop trap indicates that the sending agent has dropped certain packets (to blocked IP ports, from spoofed addresses, etc.).

No.	Trap Name	Description
66	monitorFileWritten (* See note below)	A File Written Trap is sent when the amount of data requested by the user has been written by the port monitoring instance.

Note. *These are new or enhanced traps.

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	**All IP Multicast Routing CLI Commands on OS6600 are unsupported**
IPX	**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
AlcatelIND1Dot1X.mib	alaDot1xPortLookupTable
AlcatelIND1LAG	alclnkaggAggEniActivate
AlcatelIND1VlanManager.mib	vpaPortMacType vlanIpAddress vlanIpMask vlanIpEncap vlanIpForward vlanMtu
AlcatelIND1WebMgt	alaIND1WebMgtRFSConfigTable alaIND1WebMgtHttpPort alaIND1WebMgtHttpsPort
IEEE_802_1X	dot1xAuthDiagTable dot1xAuthSessionStatsTable dot1xSuppConfigTable dot1xSuppStatsTable
IETF_BGP4	bgpRcvdPathAttrTable
IETF_BRIDGE	dot1dTpPortTable dot1dStaticTable
IETF_ENTITY	entLogicalTable entLPMappingTable entAliasMappingTable
IETF_ETHERLIKE	dot3CollTable dot3StatsSQETestErrors dot3StatsInternalMacTransmitErrors dot3StatsCarrierSenseErrors dot3StatsInternalMacReceiveErrors dot3StatsEtherChipSet dot3StatsSymbolErrors dot3ControlInUnknownOpcodes
IETF_IF	ifRcvAddressTable ifTestTable
IETF_IP_FORWARD_MIB	ipForwardTable
IETF_IPMROUTE_STD	ipMrouteScopeNameTable

MIB Name	Unsupported MIB variables on All Platforms
IETF_MAU (RFC 2668)	rpMauTable rpJackTable broadMauBasicTable ifMauFalseCarriers ifMauTypeList ifMauAutoNegCapability ifMauAutoNegCapAdvertised ifMauAutoNegCapReceived
IETF_OSPF (RFC 1850)	ospfAreaRangeTable
IETF_OSPF_TRAP	ospfTrapControl
IETF-PIM	pimRPTable
IETF_P_BRIDGE	dot1dExtBase dot1dPortCapabilitiesTable dot1dPortPriorityTable dot1dUserPriorityRegenTable dot1dTrafficClassTable dot1dPortOutboundAccessPriorityTable dot1dPortGarpTable dot1dPortGmrpTable dot1dTpHCPortTable dot1dTpPortOverflowTable
IETF_Q_BRIDGE (RFC 2674)	dot1qTpGroupTable dot1qForwardAllTable dot1qForwardUnregisteredTable dot1qStaticMulticastTable dot1qPortVlanStatisticsTable dot1qPortVlanHCStatisticsTable dot1qLearningConstraintsTable
IETF_RIPv2	rip2IfConfDomain
IETF_RMON	hostControlTable hostTable hostTimeTable hostTopNControlTable hostTopNTable matrixControlTable matrixSDTable matrixDSTable filterTable channelTable bufferControlTable captureBufferTable
IETF_RS_232 (RFC 1659)	all synchronous and sdlc objects and tables rs232SyncPortTable
IETF_SNMPv2	sysORTable snmpTrap sysORLastChange
IETF_SNMP_ COMMUNITY (RFC 2576)	snmpTargetAddrExtTable
IETF_SNMP_ NOTIFICATION (RFC 2576)	snmpNotifyTable snmpNotifyFilterProfileTable snmpNotifyFilterTable
IETF_SNMP_PROXY (RFC 2573)	snmpProxyTable

MIB Name	Unsupported MIB variables on All Platforms
IETF_SNMP_TARGET (RFC 2573)	snmpTargetAddrTable snmpTargetParamsTable snmpTargetSpinLock
IETF_SNMP_USER_BASED_SM (RFC 2574)	usmUser
IETF_SNMP_VIEW_BASED_ACM (RFC 2575)	vasmMIBViews
NOVELL_IPX	ipxStaticRouteTable ipxDestServTable ipxStaticServTable ipxBasicSysConfigSockets ipxBasicSysOpenSocketFails ipxAdvSysInCompressDiscards ipxAdvSysOutCompressDiscards ipxCircDialName 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
AlcatelIND1Port	Alcether10GigTable
AlcatelIND1VlanManager	vlanTagMobilePortStatus
AlcatelIND1StackManager	alaStackMgrChassisTable alaStackMgrStatsTable alcatelIND1StackMgrMIBObjects

Unsupported MIB Variables—OmniSwitch 8800

MIB Name	Unsupported MIB Variables—OmniSwitch 8800
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
AlcatelIND1Health	healthDeviceTemperatureCmmCpuLatest healthDeviceTemperatureCmmCpu1MinAvg healthDeviceTemperatureCmmCpu1HrAvg healthDeviceTemperatureCmmCpu1HrMax
AlcatelIND1Ipmrm	alaIPmrmDebugConfig
AlcatelIND1Ipms	alaIpmsForwardSrcIpAddr alaIpmsForwardSrcIfIndex
AlcatelIND1LAG	alclnkaggSlotTable
AlcatelIND1Port	esmPortCfgMaxFrameSize alcether10GigTable esmPortCfgLongEnable esmPortCfgRuntEnable esmPortCfgRuntSize

MIB Name	Unsupported MIB Variables—OmniSwitch 6600 Series
AlcatelIND1Pcam	alcatelIND1PCAMMIBObjects alaCoroL3HrePerModeTable alaCoroL3HrePerCoronadoStatsTable alaCoroL3HreChangeTable
AlcatelIND1Pimsm	alaPimsmGlobalConfig alaPimsmDebugConfig
AlcatelIND1QoS	alaQoSRuleReflexive alaQoSAppliedRuleReflexive alaQoSActionAlternateGatewayIpAddr alaQoSActionAlternateGatewayIpAddrStatus alaQoSActionPermanentGatewayIpAddr alaQoSActionPermanentGatewayIpAddrStatus alaQoSActionShared alaQoSActionSourceRewriteIpAddr alaQoSActionSourceRewriteIpAddrStatus alaQoSActionSourceRewriteIpMask alaQoSActionSourceRewriteNetworkGroup alaQoSActionSourceRewriteNetworkGroupStatus alaQoSActionDestinationRewriteIpAddr alaQoSActionDestinationRewriteIpAddrStatus alaQoSActionDestinationRewriteIpMask alaQoSActionDestinationRewriteNetworkGroup alaQoSActionDestinationRewriteNetworkGroupStatus alaQoSActionLoadBalanceGroup alaQoSActionLoadBalanceGroupStatus alaQoSAppliedActionPermanentGatewayIpAddr alaQoSAppliedActionPermanent GatewayIpAddrStatus 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
AlcatelIND1Slb	slbFeature slbClusterTable slbServerTableg
AlcatelIND1StackManager	alaStackMgrStatsTable

MIB Name	Unsupported MIB Variables—OmniSwitch 6600 Series	
AlcatelIND1VlanManager	vlanIpxNet vlanIpxEncap vlanIpxRipSapMode vlanIpxDelayTicks	vlanIpxStatus vlanSetIpxRouterCount vlanSetMultiRtrMacStatus
IETF_BGP4	bgp bgpPeerTable bgp4PathAttrTabl	
IETF_PIM	pim pimInterfaceTable pimNeighborTable pimIpMRouteTable	pimIpMRouteNextHopTable pimRPSetTable pimCandidateRPTable pimComponentTable
IETF_IPMROUTE_STD	ipMRoute ipMRouteTable ipMRouteNextHopTable	ipMRouteInterfaceTable ipMRouteBoundaryTable
NOVELL_IPX	ipxBasicSysTable ipxAdvSysTable ipxCircTable ipxDestTable ipxServTable	
NOVELL_RIPSAP	ripSysTable sapSysTable ripCircTable sapCircTable	

Fixed Problem Reports

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

Switch Management

Command Line Interface (CLI)

Problem Reports

PR 91398

On an OS7000 series switch, the bandwidth parameter for High Availability VLANs is not available in CLI.

Layer 2

Bridging

Problem Reports

PR 88192

Decnet frames make the mobility port not to work.

Layer 3

Basic IP Routing

Problem Reports

PR 88634

The Layer 3 forwarding (kernel) table is not in sync with the BGP protocol table when access to the next hop toggles.

IPv6

Problem Reports

PR 91124

If routes from two different peers have the same network address, but different mask lengths, only one route is created / updated.

Quality of Service (includes ACLs and NAT)

Problem Reports

PR 68906

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

PR 81620

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

PR 89112

The wildcard mask for L2 ACLs does not work after reboot; creates boot.cfg.err file.

PR 89888

If Layer 3 Classify Bridged traffic QoS rules are configured on an OS7000/OS8800 series switch, then Policy Based Routing rules can only be configured for routed traffic.

Advanced Routing

DVMRP

Problem Reports

PR 91577

When multiple multicast flows are sent to a switch on the same port instantaneously, ipc buffers may not be released by tDrcIpmrm on an OS7000/OS8800 series switch.

Security

Authenticated VLANs

Problem Reports

PR 86129

Authenticated users are lost after a QoS apply.

PR 87149

MAC-ADDRESS gets learned on the default VLAN even if AVLAN default traffic is disabled.

Policy Server Management

Problem Reports

PR 68906

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

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 the time of release.

Switch Management

Command Line Interface (CLI)

Problem Reports

PR 54887

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

Workaround: Use WebView to reference the console port information.

PR 55576

When executing a **config apply** command, applications may not appear to be loaded on an OS7000 series switch.

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

PR 57355

With large image files, the zmodem (**rz**) CLI command causes excessive "Bad CRC" errors and hang up after a small percentage of data is transferred on an OS7000 series switch. It also does not allow the user to select a particular directory, such as /working or /certified to download files. 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> is erased if it is tabbed over on an OS7000 series switch.

Workaround: Do not "Tab" over entered variables.

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 77445

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

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

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 series switch.

Workaround: The issue is cosmetic and does not effect performance of the switch.

PR 87642

The CLI command to specifically disable 802.1x or AVLAN authentication on a port disables either of the authentication options configured on the port of an OS6600/OS7000 series switch.

Workaround: There is no known workaround at this time.

PR 88606

Quotes must be used for special characters in a password and exclamation marks are not allowed.

Workaround: There is no known workaround at this time.

PR 90479

On an OS7000 series switch, WebView uses the encapsulation 'ETHERNET2' only; to avoid confusion, the redundant encapsulation 'E2' has been removed from the CLI command. The 'ETHERNET2' encapsulation remains.

Workaround: There is no known workaround at this time.

PR 91912

While configuring an OSPF interface with the **?ip ospf interface?** command, spaces cannot be used in the interface name. For example, entering the **?ip ospf interface vlan-101?** command is valid, but entering the **?ip ospf interface vlan 101?** command is not.

Workaround: Do not use spaces in the OSPF interface name.

PR 92286

Command prompt may disappear after attempting the "show" command not allowed for users.

Workaround: Type exit and then login again.The prompt will come back.

RMON

Problem Reports

PR 55770

Duration and System Resources for RMON are not accessible via SNMP or WebView on an OS7000 series switch.

Workaround: The RMON subsystem only shows the values for these objects using CLI.

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 an OS7000 series switch.

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 trapFilter-Table, and if the index value is equal to 4294967295, then the agent does not respond as expected; i.e. the object returned is not lexicographically larger on an OS7000 series switch.

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 without SNMP access. This cannot be modified.

Workaround: There is no known workaround at this time.

PR 53289

Flood multicast changes on an OS7000 series switch 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 an OS7000 series switch. Only new sessions use the changed settings.

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

PR 79611

On an OS7000 series switch, 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 an OS7000 series switch, 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.

PR 82635

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

PR 90857

On an OS7000 series switch, after a new SNMP trap station is added to the configuration, the traps are not seen by the station.

Workaround: After adding a new SNMP trap station to the switch configuration, the administrator should save the configuration and reboot the switch.

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 an OS7000 series switch. 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 on an OS7000 series switch, in order to use Java Applets in WebView pages, such as Health Home.

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 an OS7000 series switch.

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 an OS7000 series switch. This is due to missing or invalid telnet settings on the applications used by the browser.

Workaround: Update your telnet settings as 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.

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 an OS7000 series switch. 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 re-login again.

PR 59678

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

Workaround: Scroll down to view all tables.

PR 60192

Some WebView screens do not display if Internet Explorer 5.5 is installed without Java Virtual Machine (JVM) on an OS7000 series switch. Current screens affected are Physical-Health-Home, and System-File-systemMgt-Install.

Workaround: The 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-Install page.

PR 60877

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

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

PR 61457

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

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

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 an OS7000 series switch.

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 causes 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 series switch. 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 series switch.

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

PR 66619

On an OS6600/OS8800 series switch, 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 the LDAP server page manually 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 entries.

Workaround: Please click on the "Next" arrow found under the table. If this arrow appears under the table, this is an indication that there are static ARPs, 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 an OS7000/8800 series switch, and (52) for an OS6624/6648 series switch.

PR 71434

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

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

PR 71484

On an OS7000 series switch, the WebView configuration dialog windows appear too low on the screen at resolutions less than 800x600.

Workaround: There is no known workaround at this time. 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 an OS7000 series switch 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 a local user on a switch, the option link still appears, even though the switch is 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 opens. 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 the SHIFT key down when clicking on the column header.

PR 77106

The user is randomly unable to re-login to WebView on Netscape 4.7x.

Workaround: Close the browser and open a new window.

PR 77279

On an OS6000 series switch 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 the correct status of the Primary/Secondary CMM, Temperature, and Fan.

PR 78032

On an OS7000 series switch, 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 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: The user must click the Refresh button in order to see the directory contents on the screen.

PR 80237

On an OS6600 series switch, 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 an OS7000 series switch, 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 switch.

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

PR 80851

On OS6600 series switches, WebView Remote System File Management does not 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. However, all slot data is displayed.

Workaround: There is no known workaround at this time.

PR 81316

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

Workaround: There is no known workaround at this time.

PR 81755

On an OS8800 switch, in WebView, Networking > IP > BGP4 > Neighbor Settings page, the columns "In Reconfigure" and "Out Reconfigure" always say "Reconfigure".

Workaround: Please ignore; these columns are extra.

PR 82009

On an OS7000 series switch, 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: It is recommended to use Internet Explorer 6.0 or later, or Netscape 7.0 on Solaris.

PR 82075

The WebView physical console port shows a 9 pin connector instead of an RJ45 for the fiber version of the OS6600 switches.

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

PR 83005

WebView adjacencies show multiple connections when a link is an aggregate.

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 83829

Whenever you access a WebView page through the browser history list after logging in an OS7000 series switch, 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 an OS6600 series switch does not function according to specification.

Workaround: There is no known workaround at this time.

PR 84243

The firmware revision cannot be viewed in Webview under Chassis Management.

Workaround: There is no known workaround at this time.

PR 84255

When doing multiple modifications on an OS7000 series switch, such as Layer 2 > Vlan Mgmt > VLAN Configuration > Ports > Port Association > Move Ports, only the first 64 ports of the entire selection is associated. A WebView dialog box comes up indicating that only the first 64 is 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 84270

WebView’s UDP Relay Association page only allows a maximum of (3) entries on an OS7000 series switch.

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 84616

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

Workaround: Click on the Spanning Tree icon located on the Outlook-like bar to the left of the screen.

PR 84618

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

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

PR 84635

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

Workaround: There is no known workaround at this time.

PR 84677

On an OS6600 series switch, the ACE server should not be listed on available accounting/authentication servers since it is not supported.

Workaround: There is no known workaround at this time. It is only cosmetic.

PR 85654

CLI allows one to configure read-write for Spanning Tree under EUPM. Functionally, one can only configure read-only. WebView reflects this properly.

Workaround: The read-write and read-only options behave in a similar manner.

PR 87960

Sometimes WebView doesn't refresh the Source Learning table properly causing submission failed when trying to delete a MAC.

Workaround: Press the refresh button before performing MAC address deletion.

PR 88765

On an OS7000 series switch, WebView's system management switch logging tech-support page does not have provisions for dumping RIPng configuration information.

Workaround: Technical support logs created using CLI gives the user an option to dump RIPng.

PR 88942

On an OS8800 switch, an IPv6 default route to the configuration cannot be added using WebView.

Workaround: Add the IPv6 default route to the configuration using CLI.

PR 89093

On an OS6600 series switch, in WebView, Networking > IP Multicast users with only read-write permissions on IPMS, IPMR, and Web Management cannot add a static neighbor/groups/querier due to the VLAN and slot/port drop-downs being empty (insufficient permissions).

Workaround: Add read-only permissions to include VLANs and ports, or use corresponding CLI commands (VLAN, slot/port will have to be known as well).

PR 89576

In WebView, Networking > IP > OSPF > Interfaces > Area page shows the wrong value for "Priority" on the table.This applies to all platforms.

Workaround: Look at value from the "Modify" page.

PR 89965

When an OS6600 series switch is under attack, sometimes it temporarily runs out of system resources. The HTTP server in this case fails to send out the trap.

Workaround: There is no known workaround at this time.

PR 90643

On an OS8800 switch, in WebView, Networking > IP > ARP > Create ARP > Proxy Add page Name appends extra text to the end.

Workaround: Leave Name blank on the Add page and use the Modify page to change to the desired Name.

PR 90754

On an OS7000 series switch, WebView does not provide the necessary web page for adding and removing IPv6 prefixes.

Workaround: Use the CLI to add IPv6 prefixes.

PR 91961

In WebView, Networking > IP > BGP4 > Neighbors > Configuration modify page, Local Interface Name cannot be changed back to None.

Workaround: Delete the neighbor and add the same again without specifying a Local Interface name.

PR 91962

In WebView, Networking > IP > BGP4 > Neighbors > Administration modify page, the field "Remove Private AS" has the wrong drop-down options.

Workaround: There is no known workaround at this time.

PR 92311

In WebView, Networking > IPv6 > Addresses page is missing the ability to add an EUI-64 address to an IPv6 interface.

Workaround: There is no known workaround at this time.

PR 90790

On an OS8800 switch, adding an IPv6 protocol rule to a VLAN fails with "protocol limit reached".

Workaround: An IPv6 protocol Ethertype 0x86dd rule can be added to a VLAN using the CLI.

PR 92314

In WebView, Layer 2 > Link Aggregation > Static > Port add page, when there is an error, and the error message layer appears, the select boxes block the error message.

Workaround: Expand the Add window until none of the select boxes block the error message.

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

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 an OS7000 series switch that has the default VLAN on the switch in use, and that port is connected to a tagged port on an OmniCore. The OS7000 series switch is 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 series switch to be tagged, and it will also accept all the tagged frames coming from the OmniCore.

PR 91014

On an OS8800 switch, the force tag internal disable is not working. The original VLAN id in an 802.1q packet ingressing an untagged port is replaced with the default VLAN of the ingress port when this VLAN id is tagged on the egress port.

Workaround: There is no known workaround at this time.

Bridging

Problem Reports

PR 75329

On an OS7000 series switch, the user guide has a bug which requires the custom rule mask values to be in nibble patterns (f). The custom rule mask values can be any combination of bit patterns and do not have to be defined as fs for nibbles.

Workaround: There is no known workaround at this time.

PR 84780

In WebView, Physical > Ethernet > Interface Configuration > General "Modify" window might display a "Set operation finished successfully!" message. However, the changes are not made to the table.

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

PR 86084

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

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

Workaround: Enable autonegotiation and save the configuration.

PR 88974

On an OS7000 series switch, in case of a MAC-IP-PORT binding rule violation, if the MAC-address is the cause of a rule violation, then the violating flow is filtered on the default VLAN of the port; if the IP address is the cause of the rule violation, then the violating flow is filtered on the mobile VLAN configured in the rule.

Workaround: There is no known workaround at this time.

PR 89596

On an OS6600 series switch, group mobility only recognizes Ethertype 0x6003 for DECNET protocol classification. All other DECNET Ethertypes are treated as unknown or default protocol types.

Workaround: There is no known workaround at this time.

PR 89608

On an OS6600 series switch, as per the design of the group mobility rule structure, creation of a DSAP-SSAP rule is expected only for the non standard or custom defined DSAP SSAP values. For well known DSAP SSAP values like IPX-SNAP, an IPX-SNAP rule should be configured.

Workaround: There is no known workaround at this time.

PR 89827

Network rule conflicts are not resolved or prevented at the CLI level. Conflicts are resolved only at run-time on an OS6600 series switch.

Workaround: There is no known workaround at this time.

PR 90044

On an OS6600 series switch, it is possible to see a brief interruption in traffic flows once you add rules. This is because all MACs are flushed in the anticipation that rule precedence change may potentially affect the classification status of the learned MACs.

Workaround: There is no known workaround at this time.

PR 90081

On an OS6600 series switch, a runtime change in the IP address for a given MAC may result in the flow being put in filtering for non-matching IP addresses. The MAC is learned on the right VLAN once the filtering entry gets aged out.

Workaround: There is no known workaround at this time.

PR 90995

On an OS8800 switch, sometimes an error message "admin conf in NI for slot/port failed” may be displayed after issuing the admin up or down command.

Workaround: Re-enter the admin up or down command.

PR 91437

Certain user defined rules end up classifying non-matching traffic patterns on the user defined VLAN instead of the default VLAN on an OS6600 series switch.

Workaround: There is no known workaround at this time.

PR 92718

Upon VLAN deletion, there is a sufficient delay for the Group Mobility message to move from the CMM to NI for the deletion of rules associated with this NI. If the switch has live traffic, it continues to apply these rules and classify the frames. If the classification is for discard on a binding rule violation, the existence of the VLAN is not checked.

Workaround: 1) After VLAN deletion, the traffic needs to be stopped, which ages out the MACs from the source learning table based on source learning aging time. 2) Users can issue the **no mac-address-table learned** command, which flushes the MACs with filtering status, and if the traffic is still running, the MACs are relearned with bridging status.

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 an OS7000 series switch.

Workaround: There is no known workaround at this time.

PR 54096

The ESM driver does not return a pause frame when traffic exceeds 100% in the port on an OS7000 series switch.

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 series switch.

Workaround: There is no known workaround at this time.

Interswitch Protocols (AMAP)

Feature Exceptions

- The AMAP protocol uses the default VLAN on all interconnected ports to communicate with neighbors. The default VLAN on the port(s) must be enabled. AMAP cannot communicate via 802.1Q connections.

Problem Reports

PR 70128

AMAP currently works on the default VLAN for tagged ports only. So, if VLAN 1 (default VLAN) is disabled, AMAP does not work.

Workaround: When using AMAP, make sure that VLAN 1 (default VLAN) is not disabled.

IP Multicast Switching (IPMS)

Problem Reports

PR 57746

IP Multicast does not support hardware routing with 802.1Q service on an OS7000 series switch.

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 is not be enabled silently on an OS7000 series switch. When the first multicast routing interface moves to the "enabled" state, IPMS is 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 an OS7000 series switch. **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 is forwarded out of 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 the 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 an OS7000 series switch, wire rate is not achieved. The speed is limited to around 600Mb/s regardless of the packet size.

Workaround: There is no known workaround at this time.

PR 69039

The user cannot achieve wire rate multicast performance between stack elements on an OS6624/6648 series switch. Standalone performance is wire rate.

Workaround: There is no known workaround at this time.

PR 75172

On an OS7000 series switch, 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 81111

On an OS8800 switch, IPMS routes packets through the 10 gigabit NI in software only, even to untagged ports. Hardware forwarding is only available for bridged traffic over the 10 gigabit NI. Therefore, multicast routing performance is greatly reduced.

Workaround: There is no known workaround at this time.

PR 83721

When a 'proxy version' is configured to V3 on an OS7000 series switch, 'default' itself is changed to 'V3'. Hence, the 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 series switch.

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 OS8000 switch.

Workaround: It can be configured through SNMP object igmpInterfaceLastMembQueryIntvl.

PR 83992

The igmpInterfaceStatus value cannot be set through CLI or WebView on an OS7000 series switch.

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 cannot 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 series switch.

Workaround: Configure an interface as IGMPv1 through SNMP.

PR 89462

Ingress IGMP packets are not mirrored to the destination port.

Workaround: There is no known workaround at this time.

PR 90069

Received IGMP reports are not proxied as V3 reports when IGMP proxy version is configured as V3 on an OS7000 series switch.

Workaround: There is no known workaround at this time.

PR 90688

A static member configured on port 'p' and VLAN 'v' for multicast-stream 's' will receive 's' even if 'p' is not a member of 'v'. The received traffic is untagged.

Workaround: To stop receiving traffic, remove the configuration. To receive the traffic tagged, configure 'v' tagged on 'p'.

Learned Port Security

Problem Reports

PR 71412

When Learned Port Security is configured on an OS6624/6648 series switch, traffic is 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". Therefore, 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 as it is by default. There is also the possibility of setting down/up ports. Thus, interfaces could also be set admin "down/up" before everything is ready.

PR 73953

With an LPS (Learned Port Security) configuration is set only to allow a specific MAC on a port, and when the port receives non-authorized traffic (ARP requests), the MAC information shows that the unauthorized host is in a "filtering" state; therefore 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.

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: A 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 an OS6624 or 1, 9, 17, 25, 33, 41, 49 or 51 on an OS6648. 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 link-aggregate port.
- For more information, please contact Customer Support via email at support@ind.alcatel.com.

Problem Reports

PR 61641

An OS7000 series 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 as "disable". Therefore, the "admin state" must be set to "disable" just after the creation. When the whole configuration is ready, set the admin state to "enable", as it is by default. There is also the possibility of setting down/up ports. Therefore interfaces could also be set admin "down/up" before everything is ready.

PR 67598

Link aggregate on gigabit uplinks occasionally fails to load balance traffic on an OS6624/6648 series switch.

Workaround: There is no known workaround at this time.

PR 70779

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

Workaround: There is no known workaround at this time.

PR 70920

There is a warning message displayed when you create multiple system priorities in the same range for link aggregation on an OS6624/6648 series switch.

Workaround: The system priorities should be the same.

PR 72619

On an OS8800 switch, 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 an OS6600 series switch, 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 series switch. The unit is considered as "1 slot", but the two gigabit uplinks are linked to two separated ASICS. "The ports of the link aggregation cannot 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 an OmniSwitch 8800 switch, 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 an OS6600 series switch, the user is not able to change dynamic link aggregate parameters on run time.

Workaround: Delete the link aggregate LACP port and add with new modified parameters.

PR 77684

On an OS7000 series switch, 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 link aggregate ports may not come up. Replace second generation interfaces with second generation interfaces only.

PR 77693

An OS7000 series switch is not able to pass traffic through a link aggregate port if the traffic originates from the same slice as the link aggregate.

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

PR 78281

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

Workaround: When configuring mixed NI version ports in the same aggregate, make sure first generation ports are 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 hotswap a second generation board with a first generation board if link aggregate is configured across multiple boards.

PR 78752

On OS6600 series switches, deleting actor system id on a LACP port makes the display set to all Zeroes.

Workaround: LACP ports need to be set with a non zero system id. Otherwise, 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: Do not change the LACP port parameters on runtime. If a modification is needed, delete and add the port again.

PR 78909

On OS7000 and OS8800 switches, once a second-generation NI port is added to a link aggregate, one cannot add a first-generation NI port.

Workaround: 1) Add a first generation NI port first, and then add subsequent second generation ports. 2) Add ports in boot.cfg and reboot.

PR 78945

More than 14 link aggregates with size “8” cannot be added.

Workaround: There is no known workaround at this time.

PR 79116

On an OmniSwitch 6624/6648 series switch, 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 an OS7000 series switch, the LACP system priority and port priority do not 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 an OS7000 series switch, 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

If Coronado version 2 (Second-Generation NI) port comes up, then Coronado version 1 (First-Generation NI) port does not join.

Workaround: When configuring mixed versions of Coronado ports, make sure Coronado Version 1 ports are configured first, and then Coronado Version 2 ports.

PR 80995

On takeover, some OS8800 NI’s configured with link aggregation may not get reset.

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

PR 81288

On an OS7000 series switch, LACP packets stop being exchanged after enabling the backpressure command.

Workaround: Do not run this command with LACP configured.

PR 81416

On an OS7000 series switch, changing LACP values on run time makes the ports not join the link aggregate.

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 switches, sometimes multicast flow stops when link aggregate ports are added and deleted multiple times.

Workaround: There is no known workaround at this time.

PR 81650

When misconfigured LACP ports are connected to LACP ports which send LACP pdus, the LACP pdus parameters can make the port join a wrong link aggregate.

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

PR 81722

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

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

PR 81736

On OS8800 switches, when link aggregate ports with the same configuration other than the size of the link aggregate has any of the active ports go down, the non-joining ports do not join the aggregate.

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

PR 81937

With the **optimization enabled** command, it is impossible to delete a port from link aggregate.

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

PR 81985

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

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

PR 84225

On an OS7000 series switch, multiple link aggregate 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 link aggregate ports in the same slice.

PR 84437

On OS8800 first generation NI modules, there could be MAC movement across the link aggregate ports and the user ports.

Workaround: Enable the optimization mode on link aggregation modules.

PR 90656

On an OS7000 series switch, if the same actor admin key is assigned for two different dynamic link aggregates, ports could join the wrong aggregates.

Workaround: Assign unique actor parameters for each configured dynamic link aggregate.

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 switch, 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 switch, 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 an OS7000 series switch. 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 switch. During the learning process, the hardware is not yet programmed. Under heavy traffic, not all packets are mirrored.

Workaround: There is no known workaround at this time.

PR 66845

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

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 switch.

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 an OmniSwitch 8800 switch.

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 an OS7000 series switch.

Workaround: There is no known workaround at this time.

PR 72891

On an OS7000 series switch, the egress port mirroring rate is less than 1GBPS for the OS7-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 on an 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 on an OS8-GNI-U24.

Workaround: There is no known workaround at this time.

PR 79329

There is some performance degradation on egress (outport) port mirroring (from 1,488,095 p/s to 1,333,624 p/s) on an 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 an OS7000 series switch. Direction of mirroring takes previous value when the 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 an OS7000 series switch, when there are multiple mirror sessions on the same second generation NI, with the mirrored ports belonging to different default VLANs, and the mirroring port is on a first generation NI, a 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 will not 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 the case of Many-To-One mirroring on an OS7000 series switch, the traffic coming in on other mirrored ports, the tagging rules on the mirroring port might make the packet go out tagged even if it came in untagged.

Workaround: There is no known workaround at this time.

Port Monitoring

Problem Reports

PR 89745

On an OS6600 series switch, no trap information is sent for port monitoring.

Workaround: There is no known workaround at this time.

PR 89980

On an OS6600 series switch, disabling a port monitoring session on a non-existing port causes the port to go to file get (timer) state.

Workaround: Wait for the status to change from timer to disable before deleting the session.

PR 90120

IPMS traffic is not captured during a port monitoring session.

Workaround: There is no known workaround at this time.

Source Learning

Feature Exceptions

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

Problem Reports

PR 53663

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

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 an OS7000 series switch.

Workaround: There is no known workaround at this time.

PR 57013

Boot.cfg only changes the age-time value for VLAN1 on an OS7000 series switch, although it has been configured for all the VLANs.

Workaround: The user should specify the VLAN information while configuring aging time for the 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 an OS7000 series switch. Spanning Tree recalculates and flashes all MACs belonging to the same VLAN as the cable is re-inserted.

Workaround: Make the port that is 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 an OS7000 series switch.

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 switch. 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 69257

Unable to view a statically assigned source MAC address in the 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 an OS7000/8800 switch, the MAC is learned on the port wherever the MAC is seen on a link aggregate port, because the NI does not have a link aggregation concept at the 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 an OS6600 series switch as it is on the 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 an OS8800 switch, 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.

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

PR 84695

On an OS6600 series switch, even after configuring a permanent MAC address for a link aggregate port, the address is learned as a dynamic MAC address.

Workaround: There is no known workaround at this time.

PR 86276

On an OS7000 series switch, the LPS violation trap sent does not include system Date and Time.

Workaround: There is no known workaround at this time.

PR 89161

On an OS8800 switch, some of the ports show 0 MACs learned after an NI is powered down and up. However, the MACs are still being learned correctly at the NI level.

Workaround: Flush the entire MAC table to allow the CMM to have the proper MAC count.

PR 89580

An OS6600 series switch shows the IP-SNAP protocol number as zero.

Workaround: There is no known workaround at this time.

PR 89601

On an OS6600 series switch, AARP is learned as aaaa0000 instead of aaaa80f3.

Workaround: There is no known workaround at this time.

PR 90570

On an OS6600 series switch, the permanent MAC addresses on link aggregates might show as "learned" instead of "permanent".

Workaround: There is no known workaround at this time.

PR 90957

After takeover on an OS6600 series switch, sometimes MACs do not get in sync between the CMM and NI. This can cause some unwanted flooding.

Workaround: Applying the command **no mac-address-table learned** should fix the problem.

PR 92317

Traffic with a High Availability VLAN Mac address as a destination address on a port that is NOT configured for HA VLAN is flooded to all ports of the VLAN following the standard flooding path.

Workaround: There is no known workaround at this time.

PR 92627

MAC addresses configured for High Availability VLAN are learned as filtering, if seen as source addresses.

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 series switch must be configured in flat mode.

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 BPDU, and a loop is created for 2 seconds.

Workaround: There is no known workaround at this time.

PR 72119

On an OS7000 series switch, when redundant links are present between two MSTP bridges, the resultant topology will choose a blocking port regardless of the VLAN port mapping on the links. Therefore, if a VLAN is configured on one redundant link, but not the other, the bridge may block the port that the VLAN is configured on.

Workaround: This is a known issue with MSTP and the older flat spanning tree. To send specific VLAN traffic between switches with redundant links, all the redundant links need to be 802.1q tagged members of the VLAN. So, one will always be forwarding. See the Users Guide / CLI Guide for more information.

PR 74365

If a port on an OS7000 or OS6600 series switch is connected to another port that is Blocked/Alternate, then this port might not receive any BPDUs 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**: 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 76951

The **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 the 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 series switch from the 802.1D protocol to 802.1W, the spanning tree seems to be stuck in a blocking state for a certain VLAN in the 802.1W 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 spanning tree on a stand-alone OS6600 stack, it's observed that the CPU Utilization could go up to 100% after changing the bridge protocol from 802.1D to 802.1W. The spanning tree 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 spanning tree works OK. In addition, executing the same commands in the **boot.cfg** file also works OK.

PR 87565

The BPDU switching flag is not applied after reboot.

Workaround: After reboot, typing the command again will solve the problem.

PR 89086

The force version parameter is not supported.

Workaround: Use a protocol identifier, i.e. protocol commands and variables, instead.

PR 89316

With every link-up, a BPDU packet with the Root BridgeID of 0xffff is sent to elicit a BPDU reply from the adjacent switch in the current AutoEdge Detection mechanism.

Workaround: Setting the stpni_useWorstRootBridgeID=0 in NiDbg, and then disabling/re-enabling the Spanning Tree Protocol instance (these steps are not expected to be performed by the customers, but by Alcatel's Automation testers who need to setup ANVL test cases).

PR 90297

On an OS7000 series switch, the slow convergence time is basically due to the circulation of old 'good' spanning tree vectors in the network when a root switch is powered off. The performance parameter, maxAge' for CST and 'hop count' for MSTIs are defined precisely to address this issue by aging out this old information. The set up where this problem was detected has the default values for the above performance parameters and if these parameters are tuned to reflect the size of the network, the convergence time can be reduced substantially.

Due to a discrepancy in the 802.1s 2002 protocol specifications, boundary ports could transition into forwarding much faster than they should and may create loops.

Workaround: 1) Use single MSTP region as much as possible. 2) Tune the performance parameters maxAge and hop count to optimal values for the network.

VLANs

Feature Exceptions

- The number of VLANs on an OS6600 series switch with spanning tree is 128 and without spanning tree is 256.
- The number of VLANs on an OS7000/8800 switch with spanning tree is 256 and without spanning tree is 1024.
- User-Defined (Custom) VLAN Rules 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 an OS7000 series switch, one receives the following error: "Failure during DoSendData () call" and the AV-Client dies. A 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 an OS7000 series switch, 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 58160

Sometimes a mobile VLAN port association remains, showing the blocking mode. This behaves properly on the NI, but the CMM still shows the VLAN port association, as existing. The blocking property indicates that it is no longer forwarding the correct state. The mobile VPA stays as long as there is a continuous stream of DHCP traffic incoming on the NI ports.This is as per design, as DHCP traffic is expected to be in short spurts and not continuous in nature as this test-case suggests.

Workaround: There is no known workaround at this time.

PR 59422

The **show interfaces slot/port traffic** command displays the values irrespective of the port state (up or down) on an OS7000 series switch, 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 the EMP port on an OS7000 series switch.

Workaround: There is no known workaround at this time.

PR 60125

The tag value cannot be changed from the VLAN number on an OS7000 series switch. This is a hardware limitation.

Workaround: There is no known workaround at this time.

PR 60680

On an OS7000 series switch, 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 a non-zero vender identification, one is 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 an OS7000 series switch.

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

PR 61740

On OS7000 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 an OmniSwitch 8800 switch.

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 a port configured if it does not match on an OS7000 series switch. 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 example, 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, 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 be 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 an OS7000 series switch.

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 an OS7000 series switch.

Workaround: The 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 the 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 series switch. This is temporary because the address ages out.

Workaround: There is no known workaround at this time.

PR 68762

Traffic is discarded or classified only in default VLANs on an OS6624/6648 series switch.

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

PR 68968

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

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

PR 69656

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

Workaround: There is no known workaround at this time.

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

Autonegotiation is disabled if either speed or duplex is set to non-autonegotiation on the OS7-ENI-C24, OS7-ENI2-C24 and OS8-ENI-C24.

Workaround: There is no known workaround at this time.

PR 73334

When the configuration for a range is applied on an OmniSwitch 8800 switch, and if there is an error in the middle of the group configuration (all slot, groups of ports), the rest of the 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 the group mobility custom rule, traffic goes 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 resend the traffic.

PR 76336

When IP traffic is classified on a mobile port on an OS6624/6648 switch, 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 an 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 84314

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

Workaround: Works as designed.

PR 90293

On deleting an IP, IPv6, or IPX interface of VLAN 1, the switch tries without success to free base MAC addresses, which are not needed on an OS7000 series switch.

Workaround: There is no known workaround at this time.

PR 92405

If High Availability(HA) vlan is configured in the switch and HA traffic is flowing through it, HA traffic might get dropped for 5-10 seconds during a takeover.

Workaround: There is no known workaround at this time.

PR 92573

The configured High Availability VLAN bandwidth is global on a switch and not per VLAN even though the CLI command is on a per VLAN basis. The latest High Availability VLAN bandwidth configured determines the global bandwidth.

Workaround: There is no known workaround at this time.

PR 92575

The High Availability VLAN Bandwidth is granted on a per ingress slot basis. When ingress ports are on different slots, the transmission rate on egress ports can be higher than the configured bandwidth.

Workaround: There is no known workaround at this time.

PR 92628

Once a port is added to an ingress list or tagged for a High Availability VLAN, all other ports in the same slot behave like ingress ports.

Workaround: There is no known workaround at this time.

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 the switch for reloading of the operation protocol.

PR 58974

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

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 an OS7000 series switch.

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 an OS7000 series switch.

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 switch.

Workaround: There is no known workaround at this time.

PR 71573

An OS6624/6648 switch 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 the IP-SNAP protocol in the IP Ethernet protocol set. That means, if a 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 series 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 an OS7000 series switch.

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

Workaround: There is no known workaround at this time.

PR 79799

On the OS6600 series switches, an OSPF route cannot be redistributed into RIP when a Static route exists 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. Therefore, the configuration of the network should be such that routes of only one protocol - static or dynamic - 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, with the same next-hop and metric; and, if both the Static and OSPF routes are redistributed into RIP with the order being Static configuration specified first, OSPF (as specified in the configuration file), and 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 an OmniSwitch 6624/6648 switch, 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 81354

RIP task traps when more than 2K RIP routes are sent in the OS6600 Router from a RIP peer. This does not always happen, and may occur very rarely even when the number of IP routes on the OS6600 Router exceeds 2K. The trap happens due to a lack of memory allocation.

Workaround: There is no known workaround at this time. When the trap happens, the CLI console may not be available for access and the OS6600 Router will reboot due to a lack of memory.

PR 84856

An OS6600 series switch learns the source and destination IP address of every forwarded flow, and has a finite space (16K addresses) to store them; they have an aging time of 5 minutes. In certain kinds of DoS attacks, the switch can run out of space to store these addresses, and this will affect routing of new flows.

Workaround: Use the **clear arp-cache** CLI command to cause the switch to delete most, if not all, of the L3 addresses in hardware. All forwarded traffic will have to be re-learned.

PR 88951

On an OS7000 series switch, the IP interface is designed to be decoupled from VLAN management. Therefore, deleting a VLAN doesn't remove the IP interface bound to the VLAN, it only makes the IP interface inactive.

Workaround: There is no known workaround at this time.

PR 90083

On an OS7000 series switch, the IP Service Ports page in WebView is missing port 262, which corresponds to avlan-http-proxy.

Workaround: Use IP Service Types page to enable or disable this service.

PR 92104

Webview or SNMP incorrectly shows the forwarding state of an IP interface as "forwarding", even though the IP interface is administratively / operationally down.

Workaround: Use CLI to reflect the true forwarding status of an IP interface.

PR 92791

Redistributed routes get added to the RIP routing table even though the global rip status is disabled.

Workaround: Disable redistribution status.

IPv6

Problem Reports

PR 86669

IPv6 Router Advertisement decrementing timers are not supported for prefix valid lifetimes or prefix preferred lifetimes.

Workaround: Use IPv6 Router Advertisement fixed timers.

PR 86959

IPv6 debug packet direction options are ignored.

Workaround: IPv6 debug packet direction will always display all the options.

PR 88830

On an OS8800 switch, when RIPng tries to add a route to the kernel, it fails because a static route already exists in the kernel. RIPng is not informed of this event, so RIPng assumes that the RIPng route has been added to the kernel. On deletion of the static route, RIPng does not try to add the route again since it assumes that the route already exists in the kernel.

Workaround: After deleting the static route disable/enable RIPng. The route should then be learned.

PR 90746

IPv6 will not function on an OS6600 series switch after a takeover or failover.

Workaround: After deleting the static route disable / enable RIPng. The route should then be learned.

PR 90942

On an OS7000 series switch, IPv6 does not prevent the addition of an address whose prefix is all zeros. This will result in the unspecified address being added as the subnet router anycast address.

Workaround: Do not add an address whose prefix is all zeros.

PR 91228

On an OS7000 series switch, the system does not detect IPv6 port scanning, nor other IPv6 denial of service attacks.

Workaround: There is no known workaround at this time.

PR 91898

It is possible to add two IPv6 configured tunnels with the same source and destination IPv4 addresses. This is discouraged since it may have some unusual consequences.

Workaround: Create only a single IPv6 configured tunnel with the same source and destination IPv4 addresses. Since multiple IPv6 addresses may be assigned to a single tunnel, more than one with the same IPv4 addresses is never necessary.

PR 92215

Modification of IPv6 interface MTU does not change MTU size in Ripng and hence RIPng update packet size also does not change.

Workaround: There is no known workaround at this time.

PR 92225

The **traceroute** command can usually be stopped while in progress by pressing any key from the console session. However, if a probe returns an error "probe transmission failed", the command does not exit until the configured timeout has expired.

Workaround: There is no known workaround at this time.

PR 92270

IPv6 static and local routes remain in the up state, even when the interface used to reach their destination is down.

Workaround: There is no known workaround at this time.

PR 92663

If a duplicate address is detected, the error message is only shown on the console screen. It neither appears on a telnet session nor saved in the swlog log file.

Workaround: There is no known workaround at this time.

IPX

Problem Reports

PR 54290

The switch only changes an IPX network field of zero to the appropriate source network when the first zero packet arrives on an OS7000 series switch. After that point, the IPX packets pass 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 an OS7000 series switch. Since WAN connections are not allowed in this release, the WAN state of the interface is always "not enabled".

Workaround: There is no known workaround at this time.

PR 68826

When using the IXIA ScriptMate on an OmniSwitch 8800 switch, IXIA tries to reacquire the link. It detects a timeout and is unable to pass traffic.

Workaround: Configure the IXIA side as non-auto and then there will not be any more link changes.

PR 73198

The MAC-IP binding rule allows IPX traffic to flow along with the classified IP traffic in the VLAN classified to. Other products 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.

PR 91850

IPX statistics are not correct with WebView or SNMP.

Workaround: A **show ipx traffic** command needs to be executed on CLI, so that the statistics can be retrieved from the NIs.

PR 91979

IPX network address cannot be set through SNMP.

Workaround: Use either CLI or WebView to set IPX network address.

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 a 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 the offset is larger than 128 milliseconds continuously for 900 seconds (15 minutes), a time update is 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 an OS7000 series switch.

Workaround: There is no known workaround at this time.

PR 90160

On an OS7000 series switch, when a URL file address is added to an SLB probe, a '/' is added.

Workaround: There is no known workaround. This functionality helps when sending the HTTP GET. Since the parameter is an offset to a file on the HTTP server, we made sure there was a '/' for the GET.

UDP Relay

Problem Reports

PR 77401

On an OS7000 series switch, if the lease time expires for a particular IP address used by one switch, the server is out of new IP addresses, and another switch requests an 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 a larger pool of addresses on the server.

PR 83947

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

Workaround: There is no known workaround at this time.

PR 84359

If a VLAN's router IP address is changed on an OS7000 series switch, 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 series switch, the ip_id field gets changed.

Workaround: There is no known workaround at this time.

PR 84500

On an OS7000 series switch, once a 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 are duplicated with UDP Relay on an OS7000 series switch.

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.

PR 88860

The DHCP forward delay range is incorrect.

Workaround: There is no known workaround at this time.

VRRP

Problem Reports

PR 61934

An OS7000 series switch does not support VRID 0. OmniCore does.

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

PR 62272

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

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 an OS7000 series switch.

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 88251

If there is a port tracking policy and a single VLAN on a port, and if the vlan is disabled, spanning tree marks the port as blocked. VRRP is not notified that the port is unusable and the port tracking policy is not invoked.

Workaround: Configure tracking policies for both the port and the vlan.

PR 89046

With release 5.1.6.R01 the basis for the VRRP implementation is RFC 3768. Packet authentication is no longer utilized in RFC 3768 due to the ineffective level of security it provided. Therefore, the VRRP AUTHENTICATE parameter is no longer available through the CLI or Webview.

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 on the OS7000/8800 series switches.
- Only 128 policy rules on the OS6600 series switches.

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 an OS7000 series switch. 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 an OS7000 series switch 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 an OS7000 series switch, 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

The policy service group is broken by using "source ip port" with "destination ip port" on an OS7000 series switch.

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 an OS7000 series switch.

Workaround: There is no known workaround at this time.

PR 58008

When "classifyl3 bridged" is turned on, on an OS7000 series switch, if a specific Layer 2 DA rule is not matched (or gets dropped due to the Layer 2 SA lookup), then traffic is treated as if it is routed, which includes what was 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 an OS7000 series switch, 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 an OS7000 series switch.

Workaround: There is no known workaround at this time.

PR 60928

An active FTP is not supported with NAT on an OS7000 series switch.

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

PR 61072

Simple NAT rules, on an OS7000 series switch 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 an OS7000 series switch.

Workaround: There is no known workaround at this time.

PR 63285

TCP/UDP fragment classification is not supported on an OS7000 series switch.

Workaround: There is no known workaround at this time.

PR 65449

Reflexive policies, on an OS7000 series switch, 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 of 3 seconds before being accepted on an OS7000 series switch. This is due to the TCP timeout configured on PC/sun IP stack (standard value). The first "open request" hits the switch, but the response of this request cannot be dropped before the reflexive policy is applied. Then, the PC retries 3 seconds later.

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 switch.

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 switch.

Workaround: There is no known workaround at this time.

PR 67882

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

Workaround: There is no known workaround at this time.

PR 68472

OS6624 and OS6648 switches do 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 a PC connected through the 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 an OS7000/8800 switch is 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 69252

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

Workaround: There is no known workaround at this time.

PR 72325

On an OS6624/6648 switch, 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 switch, 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 matches 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 switch, it is not possible to create a L3 ACL on a source, and another on a destination, because currently the OS6600 cannot link up the source and destination.

Workaround: There is no known workaround at this time.

PR 76901

On an OS6624/6648 switch, the QoS 5.1.4.R01 configuration file is not compatible when certain rules are used. A boot.cfg.1.err file may be generated upon bootup.

Workaround: Based on the errors generated in the boot.cfg.1.err file, the user has to edit the boot.cfg file and remove all the unsupported features. Features that were supported in QoS 5.1.4.R01 on an OS6600 series switch, but are currently not supported are as follows: 1. TOS/DSCP to 802.1p Stamping rule not supported. 2. 802.1p to TOS/DSCP mapping rule not supported. 3. No Interface Type support in a L3 policy condition.

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 switches link aggregation ports.

Workaround: There is no known workaround at this time.

PR 84386

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

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

PR 84425

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

Workaround: There is no known workaround at this time.

PR 90119

On an OS7000 series switch, Ethertype based conditions will only affect Ethernet II encapsulated packets.

Workaround: There is no known workaround at this time.

PR 90141

On an OS6600 series switch, the DSCP to priority table is not being updated correctly. Thus, the user cannot change the priority of a flow based on its TOS value.

Workaround: Use the DSCP value to change flow priority (e.g., policy condition c dscp 30).

PR 92153

When a switch is only bridging a packet that is routed by an external router, and when this routed packet has to go through the same NI from where it originated before reaching its final destination, the following symptom can be seen: If "QoS ClassifyL3 bridged" is enabled, the NI's HRE learns the IP Source Address on two different ports, and therefore the packet never reaches its destination. Please refer to TechTip 2077 for more details.

Workaround: Use a different NI to connect the external router, or disable "QoS ClassifyL3 bridged" on the switch. Please refer to TechTip 2077 for more details.

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 the 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 an OS8800 switch.

Workaround: Configure a Suppress value less than 1600 seconds.

PR 72300

An AS number cannot be used with command: **ip bgp confederation neighbor**.

Workaround: There is no known workaround at this time.

DVMRP

Problem Reports

PR 56990

Tunnel destined flows are not displayed in the **show ip multicast forwarding** CLI command on an OS7000 series switch. 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.

PR 90878

On an OS7000 series switch, by administratively disabling a DVMRP-configured IP interface via the command "**ip interface <ifname> admin disable**", and then re-enabling that same IP interface via **ip interface <ifname> admin enable**, DVMRP is not automatically re-enabled.

Workaround: To get DVMRP operational again on that specific interface, re-issue the **ip dvmrp interface <ifname>** command. (This is the command initially used to configure DVMRP on the interface.) If the IP interface becomes disabled due to other events, such as disabling ports, the DVMRP command does not need to be re-issued.

Multicast Routing

Problem Reports

PR 55446

Multicast routing does not handle large multicast bursty traffic on an OS7000 series switch.

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 80757

Only a single client on a given port for a given multicast group is shown in the group membership, displays on an OS6600/OS7000 switch.

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 an OS7000 series switch. 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

One cannot unload and reload OSPF on an OS7000 series switch.

Workaround: There is no known workaround at this time.

PR 58676

The OSPF default cost is the same for fast Ethernet and the gigabit interface on an OS7700/7800 switch.

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 an OS7000 series switch.

Workaround: There is no known workaround at this time.

PR 69890

OSPF virtual links will not form an adjacency with gateD switches if MD5 is configured on an OS6600/ OS7000 series switch.

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 an "enabled/disabled" status. The presence or absence of a range itself is equivalent to the "enabled/disabled" state on an OS7000 series switch.

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 an OS7000 series switch, RIP and OSPF MD5 authentication is not interoperable between AOS and XOS (GateD) & OmniCore.

Workaround: Use Clear Text or SIMPLE authentication.

PR 81856

On OS6600 series switches, the 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

With Catalina versions prior to 1.3, the number of collisions are capped at 5 in the Layer 3 PCAM table. As a result, there may be some thrashing of IPMS PCAM entries, possibly leading to OSPF instability. The version of the Catalina is determined by running the **show ni** command.

Workaround: The immediate workaround is to disable the limitation.

PR 90742

On the OS6600 series, OSPF ECMP gateways are not correctly computed when there is more than one point-to-point or point-to-multipoint interface between a pair of OSPF routers.

Workaround: There is no known workaround at this time.

PIM-SM

Problem Reports

PR 73783

On an OS7000 series switch, 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 an 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 series switch.

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

tPimsm: 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: There is no known workaround at this time.

PR 75062

When running in a mixed environment consisting of OS7000's and Cisco's, the OS7000 PIM-SM 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 an OS7000 series switch, 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 88043

IXIA automation tests consisting of 1023 flows and 1023 group memberships can result in IPMRM error messages scrolling on the console, when the RP is manually deleted and then added again (using the **ip pimsm crp-address** command).

Workaround: Set 'ip mroute debug-level 0' so that the messages don't appear on the console.

PR 92679

Using Static-RP Configuration and then changing the max-rps may cause tpimsm to suspend.

Workaround: If using static-rp configuration, the max-rps needs to be configured before defining/enabling any of the static-rp set.

Security

Feature Exceptions

- The Mac OS X 10.3.x is supported for AVLAN web authentication using JVM-v1.4.2

General

Problem Reports

PR 89262

On an OS7000 series switch, NESSUS reports bogus "Vulnerabilities". Basically, NESSUS collects all those known attacks/vulnerablities into their test suites.

For Example,

NESSUS sends: http://<switch-address>/cgi/bin/guestbook.cgi

WebView/HTTP-Server's response: Prompts user for the default switch login page (which is the normal operation for our embedded server).

Since our HTTP server replies with some form of an HTTP response, NESSUS mistakenly concludes that the HTTP server is vulnerable to this attack.

Workaround: There is no known workaround at this time.

802.1X

Problem Reports

PR 70452

On an OS7000 series switch, even after the PC is successfully authenticated to a port, the status on the PC shows 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 an OS6624/6648 switch, 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/OS8800 platform, which can support more than one VLAN per port.

Workaround: There is no known workaround at this time.

PR 90855

The **no aaa authentication 802.1x** CLI command does not work properly.

Workaround: Put onex port in the Force Authorized mode first before executing the command.

PR 92093

When using the XP service pack 2 native 802.1x client and some version of Steelbelted RADIUS, the XP 802.1x client will not always be able to "successfully" authenticate.

Workaround: Use pure XP without any service pack or with Steel-belted RADIUS Service Provider Edition 4.70.661.

PR 92652

When a port is in the 802.1x forced authorized mode, the relay agent does not flood DHCP packets to the same VLAN as the 802.1x client.

Workaround: This is a limitation, if only 802.1x is configured. Once the DHCP server is on a different VLAN, then it works.

PR 92719

When an 802.1x port is configured with direction=both and port control = force-authorized, no DHCP traffic is allowed to broadcast out to the 802.1x client VLAN. This is because port control is applied to both incoming and outgoing broadcast traffic.

Workaround: When an 802.1x port is configured with direction=in and port control = force-authorized, DHCP traffic is allowed to broadcast out to the 802.1x client VLAN. This is because port control is only applied to incoming traffic.

PR 92818

If the 802.1x port port-control is changed from force-authorized and then changed back to auto, the Guest VLAN feature may not work.

Workaround: Manually use admin down/up to reset the port.

PR 92863

When an 802.1x guest VLAN PC is moved from a Hub to a Guest VLAN port, it may not be able to send/receive traffic until the MAC address is aged out on the hub port.

Workaround: There is no known workaround at this time.

Authenticated Switch Access

PR 59686

If a user kills an HTTP session, the table still displays 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 a HTTP session. Telnet and FTP sessions are removed from the table properly.

PR 63104

During a takeover, switch management sessions (HTTP, FTP, and Telnet) are closed on an OS7000 series switch. Therefore, 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 an OS6624/6648 switch, 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 supports 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 an OS7000 series switch 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 an OS7000 series switch, 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 Windows XP 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 download.

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, the user may observe the certificate expiration a long time after it really occurs.

Workaround: There is no known workaround at this time.

PR 68485

The policy server load and **policy server flush** commands provoke a flush of the CAM MAC SA, which leads to disconnecting AVLAN users on an OS7000 series switch.

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

PR 76820

On an OS6624/6648 switch, when the user configures the IP helper on the second hop, the PC will not be able to get the IP address after authentication. AOS appears not to be able to learn the MAC, when in fact the PC never gets the IP address, and thus there is no traffic from the PC.

Workaround: Configure IP helper on the first hop.

PR 77107

After HTTP authentication on an OS7000 series switch, MAC OS X resets the link and thus, all MACs learned are flushed on that port. This causes 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 91812

Server information displayed with the **show configuration snapshot aaa** command or saved with the **configuration snapshot aaa <file_name>** command contains hashed (encrypted) password/key information. In order to use a file created with the latter command for configuring servers, password/key information needs to be edited. AAA expects this information encrypted only at boot-up time, while at run time the information should be in plain text. In this particular case, the servers created with the **configuration apply** command could not be used because password/key information is wrong.

Workaround: Always edit password/key information before applying a snapshot file.

PR 91941

When user configure a VLAN as an authentication VLAN before assigning an IP address to the VLAN, the VLAN gets an invalid AVLAN address needed for Telnet and web authentication.

Workaround: Assign an IP address to the VLAN before configuring the vlan as an authentication VLAN.

PR 92532

When the HTTP Proxy server is configured on the browser, the "aaa avlan dns name" only allows a single word, i.e."WebView". A domain is not allowed i.e. WebView.com.

Workaround: There is no known workaround at this time.

Policy Server Management

Problem Reports

PR 63005

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

Workaround: There is no known workaround at this time.

PR 74062

On an OS6624/6648 switch, it is not possible to create a L3 ACL on a source network, and another on a destination network, because currently an OS6600 series switch cannot link up the source and destination.

Workaround: There is no known workaround at this time.

System

General

Problem Reports

PR 51067

A Switch based telnet client only supports a single user at a time on an OS7000 series switch. 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 is 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 an OS7000 series switch. 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, he/she receives 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 an OS7000 series switch.

Workaround: There is no known workaround at this time.

PR 55967

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

Workaround: There is no known workaround at this time.

PR 59510

The time for 10/100 ports to auto-negotiate depends on the number of such ports configured in the system. The more the number of ports configured for auto-negotiation, the longer it takes before they all auto-negotiate. This is observed only at bootup condition.

Workaround: There is no known workaround at this time.

PR 60142

When priority 2 and priority 3 traffic is sent at wire rate on all 384 ports of a switch, 40 percent of the traffic is dropped.

Workaround: Configure the network applications and the switch QoS parameters so that only the highest priority traffic is sent at priority 3 through the switch.

PR 60599

The watch dog does not reboot the switch when the OS7000 locks up, due to a corrupt 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 an OS7000 series switch. Only SNMP GetNext requests work on the entire table, but SNMP get for specific instances fails.

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

PR 60675

The **mac-range** command does not update the routing information upon completion.

Workaround: For the **mac-range** command to take effect (have the chassis use the new macs), the chassis needs to be rebooted. In fact, when the first mac-range changes, the switch must reboot. All VLAN and routing functionalities beyond that point is not be supported.

PR 61018

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

Workaround: There is no known workaround at this time.

PR 61534

The FTP session has problems connecting to a switch, while the certify process is still running.

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

PR 61572

When the protocol reference is not specified in the Ethernet frame, layer 2 traffic is not accepted on an OS7000 series switch.

Workaround: There is no known workaround at this time.

PR 62067

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

Workaround: There is no known workaround at this time.

PR 63605

Some Fweb* images show up in the "loaded m-code" table before an OS7000 series switch 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 dynamically loads 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 the system time on an OS7000 series switch.

Workaround: There is no known workaround at this time.

PR 65248

When an user configures the EMP IP address to "." or 0.0.0.0 in an attempt to clear the address on an OS7000 series switch, it in fact adds 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 an OmniSwitch 8800 switch.

Workaround: There is no known workaround at this time.

PR 66815

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

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 67889

IXIA Scriptmate automates auto-negotiation test. Hence, the timing for enabling port (PHY and MAC) between IXIA and an OS8800 switch is different. Since the OS8800 switch 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 68905

ColdStartTrap is sent every time a switch is reset.

Workaround: There is no known workaround at this time.

PR 70760

A highly fragmented file system can slow the file system response.

Workaround: Use the **fsck** command on your fragmented file system to improve the file system performance.

PR 72271

When building a new stack using up and running standalone units on an OS6624/OS6648 switch, the 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 73037

If a port on an OS7000 series switch 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 series switch, a "continuous Flash synchro" process may occur if the local "working" and "certified" directories are not "certified".

Workaround: When any stacks are required to be connected to other stacks, make sure the individual stacks are synchronized between themselves locally (Working and Certified) and within each module of the current stack environment.

PR 76349

On an OS7000 series switch, 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 become corrupt after the Certify, Restore, or Flash Synchro process.

Workaround: There is no known workaround at this time.

PR 76658

MAC Server manager has a maximum range of 256 MACs. If the system is configured with a MAC range exceeding 256 MACs, the MAC server is not 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 79859

Firmware version is not shown using SNMP on an OS7000 series switch.

Workaround: There is no known workaround at this time.

PR 80937

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

Workaround: There is no known workaround at this time.

PR 82675

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

Workaround: Make sure the boot flag is set to 0.

PR 83669

The chassis will not be able to bootup when the boot flag is set to 0xb8000 on an OS7000 series switch.

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

PR 84294

The **show running-directory** command shows Running Configuration as Not Available on an OS6600 series switch.

Workaround: This is a display issue only.

PR 84601

On an OS7000 series switch, daylight savings time is not accommodated in several time zones. NTP synchronization is off by one hour.

Workaround: There is no known workaround at this time.

PR 86084

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

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

Workaround: Enable autonegotiation and save the configuration.

PR 90189

The **reload working no rollback-timeout** CLI command causes the switch to generate a coldStart trap when it comes back up again. It should be sending a warmStart trap instead.

Workaround: Ignore this trap.

PR 90193

If the name of a file (1) is the substring of another file (2) on the remote CMM, then an endless flash synchro situation may occur.

Workaround: Inspect the contents of directories from both CMMs, and remove file (2) from the remote CMM.

PR 90574

On an OS6600 series switch, a STR status message is sent when the CSM certification is done.

Workaround: There is no impact to the execution code, only the message 0x222 is logged in the swlog. The user can ignore this message.

PR 91482

On an OS6600 series switch, when max bandwidth rules with either destination ip, source ip, or source network group are applied and modified, we may run into no free BDs issue.

Workaround: There is no known workaround at this time.

PR 91691

Upgrading the OS8800 FPGA can fail due to insufficient flash space if the user has added files to the flash.

Workaround: Upgrade the FPGA via 5.1.5.R04 release or remove all files except those on the original 5.1.6.R01 release. Make sure at least 2.5 Meg of free space is available.

NIs—General

Problem Reports

PR 62573

For the following modules, PAUSE frames are 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 an OS7000/8800 switch, oversubscribing the egress gigabit module at a rate exceeding 3:1, results in higher priority traffic sharing the bandwidth equally with lower priority traffic.

Workaround: There is no known workaround at this time.

PR 73196

The failure of a task on NI may cause unsolicited takeover or reboot of the switch.

Workaround: There is no known workaround at this time.

PR 79427

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

Workaround: Hash should be manually updated.

OmniSwitch 6600 NIs

Problem Reports

PR 90972

The displayed field "coper" is just a typo of the word "copper" on an OS6600 series switch.

Workaround: There is no known workaround at this time.

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 the 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 is 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 are not able to auto detect speed and duplex settings 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 effect. One can reset the NI by executing the **no power ni <num>** command, and then the **power ni <num>** command. One can also execute the **reload working no roll-back** for the setting to 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 an OS7000 series switch.

Workaround: There is no known workaround at this time.

PR 77702

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

Workaround: Use the 8-port Hub NetGear DS108.

PR 80023

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

- Autonegotiation is turned off and the local port is enforced to FULL duplex; or,
- Autonegotiation is turned on, but the speed mismatches other than auto; or,
- Autonegotiation is turned on, but the 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 OS7-ENI-C24 modules.

Workaround: There is no known workaround at this time.

OmniSwitch 8800 NIs

OmniSwitch 8800 Feature Exceptions

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

Problem Reports

PR 66750

The maximum aggregate throughput for an OS8-ENI-C24 (10/100) is 2.0 gigabits/sec.

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, a port is enabled. If the port is not enabled yet, any incoming frames are dropped. As a result, statistics between the switch and the 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 goes 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 does not affect the behavior of the switch.

Workaround: There is no known workaround at this time.

PR 76652

On OS8800 switches, when broadcast packets inflow to a port, if they are mixed with different sizes, some smaller size packets could be dropped by the system.

Workaround: There is no known workaround at this time.

PR 80442

An error message “No Such Object available on this agent” is returned for 10G specific tables. This problem only occurs with the SNMP walk application.

Workaround: There is no known workaround at this time.

PR 81010

An OS8-GNI-C24 may encounter some packet loss for small size packets if it is wired traffic (100% traffic inflow).

Workaround: This is an oversubscription condition. Lower the incoming traffic rate.

PR 81727

Unable to set primary Xenpak from WebView or OmniVista.

Workaround: Use the CLI command.

Power over Ethernet

Problem Reports

PR 79947

When using the POE support, the power LEDs do not work.

Workaround: There is no known workaround at this time.

PR 90556

On an OS7000 series switch, a LanPower error message is displayed when removing and inserting NIs.

Workaround: There is no known workaround at this time.

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.
- 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.

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 an OS7000 CMM to fail.

Workaround: There is no known workaround at this time.

PR 62403

Voice conversation drops and IP phones directly connected to an OS7000 series switch 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 in the working directory, the **reload working no rollback-timeout** command has to be issued. This ensures that the NIs are properly reloaded and the new configurations are sent to the NIs.

PR 66098

The user may see the following message on bootup: "*CSM_P1_4 - csCsmCmmCtx.cmmState = 9*" on an OS7000 series switch. 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 Synchronization, and a takeover process is issued (both from the user or from SM detection), stacks will get into an unstable condition.

Workaround: DO NOT perform (manually) a takeover while Flash Synchronization is in progress.

PR 67483

The **copy flash-synchro** command will not work between different release versions of code.

Workaround: Both CMMs 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 the chassis with both CMMs.
5. Perform **copy flash-synchro** from the primary CMM.

PR 68913

In case of a takeover, cmmAUnPlugged and cmmBUnplugged alert traps are not sent on an OS7000 series switch.

Workaround: There is no known workaround at this time.

PR 72041

Synchronization of flash fails 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. The 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 an OS7000 series switch. 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 series switch, 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 79063

Flash Synchronization is successful, but **show running** shows CMMs NOT SYNC when a new folder is created in /working on an OS7000 series switch.

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 a certified stack is connected to a non-certified stack (Primary).

Workaround: Make sure both (working and certified) directories are certified before connecting them to any stacks.

PR 84317

Do not reload the NIs on an OS6600 series switch, in case of takeovers with unsaved configurations due to some limitations. The unsaved running configuration is still applied on the NIs, even though the new primary cannot see that portion of the configuration update. Since the takeover did not reload this NI, the applied group mobility rules are still in effect.

Workaround: Reboot the stack.

PR 85838

5.1.5.R03 releases and later are not backward compatible in terms of flash synchro with 5.1.5.R02 and earlier releases.

Workaround: On dual CMM systems (7000 & 8800 series), once users have upgraded existing releases to 5.1.5.R03 or later, they will have to downgrade each CMM individually if there is a need to downgrade to 5.1.5.R02 or earlier. The individual CMMs will then need to be plugged together.

PR 87051

Reload prompt overrides all other session responses on an OS7000 series switch.

Workaround: Prior to issuing reload or reboot, ensure all sessions are closed. Use the kill command to remove other sessions. Do not issue reload or reboot prompt without fully committed to action.

PR 90540

On an OS8800 switch, after a takeover, a 10G port will not display on the CMM side.

Workaround: There are no interruptions on traffic flows. To display 10G ports, the user needs to reset the 10G NI.

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.