Release Notes
OmniSwitch 6800
Release 5.3.1.R02

These release notes accompany release 5.3.1.R02 software for the OmniSwitch 6800 series 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.

Contents

Related Documentation

These Release Notes should be used in conjunction with the OmniSwitch 6800. The following are the titles and descriptions of the OmniSwitch 6800 user manuals:

Note. User manuals can be downloaded at http://www.alcatel.com/enterprise/en/resource_library/user_manuals.html

- *OmniSwitch 6800 Series Getting Started Guide*

  Describes the hardware and software procedures for getting an OmniSwitch 6800 Series switch up and running.

- *OmniSwitch 6800 Series Hardware User Guide*

  Complete technical specifications and procedures for all OmniSwitch 6800 Series chassis, power supplies, and fans.

- *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.

- *OmniSwitch 6800 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 6800 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 6800 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.

- Technical Tips, Field Notices

  Contracted customers can visit our customer service website at: http://eservice.ind.alcatel.com.

System Requirements

Memory Requirements

- OmniSwitch 6800-24 Release 5.3.1.R02 requires 256 MB of SDRAM and 64MB of flash memory. This is the standard configuration shipped.
- OmniSwitch 6800-48 Release 5.3.1.R02 requires 256 MB of SDRAM and 64MB of flash memory. This is the standard configuration shipped.
- OmniSwitch 6800-U24 Release 5.3.1.R02 requires 256 MB of SDRAM and 64MB of flash memory. This is the standard configuration shipped.
- OmniSwitch 6800-24L Release 5.3.1.R02 requires 256 MB of SDRAM and 64MB of flash memory. This is the standard configuration shipped.
- OmniSwitch 6800-48L Release 5.3.1.R02 requires 256 MB of SDRAM and 64MB of flash memory. This is the standard configuration shipped.

Configuration files and the compressed software images—including web management software (WebView) images—are stored in 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 6800 (-24, -48, -U24) Series

- Miniboot: 5.3.1.91.R02
- BootROM: 5.3.1.91.R02

OmniSwitch 6800 (-24L, -48L) Series

- Miniboot: 5.3.1.91.R02
- BootROM: 5.3.1.91.R02

Note. Field upgrade of existing units is not required. Minimum Miniboot / BootROM: 5.3.1.330.R01.

New Hardware Supported

The following new hardware is supported subject to the feature exceptions and problem reports described later in these release notes.

New Chassis

The following new chassis are available in this release:

Note. See the *OmniSwitch 6800 Series Hardware Users Guide* for more information on OmniSwitch 6800 Series hardware features.

OS6800-24

The OmniSwitch 6800-24 (OS6800-24) stackable workgroup switch has 20 unshared auto-sensing and auto-MDIX copper RJ-45 10/100/1000 Mbps ports (ports 1–20). In addition, the OmniSwitch 6800-24 has four combo ports (ports 21–24) that are shared between four copper RJ-45 10/100/1000 Mbps ports and four SFP 1000 Mbps (1Gbps) ports.

In addition to working as an individual, stand-alone switch, the OS6800-24 can also be linked together with any other member of the OmniSwitch 6800 Series of switches to form a single, high-density virtual chassis known as a *stack* consisting of up to eight (8) switches in *any combination* within the stack.

Note. The OS6800-24 does not support the OS6800-XNI-U2 10 Gigabit module.

OS6800-48

The OmniSwitch 6800-48 (OS6800-48) stackable workgroup switch has 44 unshared auto-sensing and auto-MDIX copper RJ-45 10/100/1000 Mbps ports (ports 1–44). In addition, the OmniSwitch 6800-48 has four combo ports (ports 45–48) that are shared between four copper RJ-45 10/100/1000 Mbps ports and four SFP 1000 Mbps (1Gbps) ports.

In addition to working as an individual, stand-alone switch, the OS6800-48 can also be linked together with any other member of the OmniSwitch 6800 Series of switches to form a single, high-density virtual chassis known as a *stack* consisting of up to eight (8) switches in *any combination* within the stack.

Note. The OS6800-48 supports the OS6800-XNI-U2 10 Gigabit module.

OS6800-U24

The OmniSwitch 6800-24 (OS6800-U24) workgroup switch has 20 unshared 1000 Mbps SFP fiber ports (ports 1–20). In addition, the OmniSwitch 6800-U24 has four combo ports (ports 21–24) that are shared between four 1000 Mbps SFP fiber ports and four auto-sensing and auto-MDIX copper RJ-45 10/100/1000 Mbps ports. The OS6800-U24 also supports the OS6800-XNI-U2 10 Gigabit module.

Note. The OS6800-U24 can operate only in stand-alone mode.

OS6800-24L

The OmniSwitch 6800-24L (OS6800-24L) stackable workgroup switch has 20 unshared auto-sensing and auto-MDIX copper RJ-45 10/100 Mbps ports (ports 1–20), which can be upgraded to 10/100/1000 ports through the purchase of a software license. In addition, the OmniSwitch 6800-24L has four combo ports (ports 21–24) that are shared between four copper RJ-45 10/100/1000 Mbps ports and four SFP 1000 Mbps (1Gbps) ports.

In addition to working as an individual, stand-alone switch, the OS6800-24L can also be linked together with any other member of the OmniSwitch 6800 Series of switches to form a single, high-density virtual chassis known as a *stack* consisting of up to eight (8) switches in *any combination* within the stack.

Note. The OS6800-24L does not support the OS6800-XNI-U2 10 Gigabit module**.**

OS6800-48L

The OmniSwitch 6800-48L (OS6800-48L) stackable workgroup switch has 44 unshared auto-sensing and auto-MDIX copper RJ-45 10/100 Mbps ports (ports 1–44), which can be upgraded to 10/100/1000 ports through the purchase of a software license. In addition, the OmniSwitch 6800-48L has four combo ports (ports 45–48) that are shared between four copper RJ-45 10/100/1000 Mbps ports and four SFP 1000 Mbps (1Gbps) ports.

In addition to working as an individual, stand-alone switch, the OS6800-48L can also be linked together with any other member of the OmniSwitch 6800 Series of switches to form a single, high-density virtual chassis known as a *stack* consisting of up to eight (8) switches in *any combination* within the stack.

The OS6800-48L supports the OS6800-XNI-U2 10 Gigabit module.

Note. The OS6800-48L supports the OS6800-XNI-U2 10 Gigabit module.

New 10 Gigabit Module

The following 10 Gigabit module is available in this release:

OS6800-XNI-U2

The OS6800-XNI-U2 two-port XFP 10 Gigabit module is now available. This module can mix and match different 10 Gigabit XFP transceiver types and is supported on OS6800-48, OS6800-U24, OS6800-48L switches. It is not supported on OS6800-24 or OS6800-24L switches.

The following features are unsupported.

- 802.1x Multi Client Support
- AVLANs
- Group Mobility
- Learned Port Security (LPS)
- Port Monitoring
- User Port/Network Port

Note. The OS6800-XNI-U2 requires Release 5.3.1.R02 or later. In addition, the OS6800-XNI-U2 module is **not** hot swappable.

Note. Compatibility with the OmniSwitch 8800 10 Gigabit Ethernet is supported. Refer to the OmniSwitch CLI Reference Guide and the OmniSwitch 6800 Hardware Users Guide.

New Backup Power Supplies (BPSs)

The following power shelf and BPS are available in this release:

OS6800-BPS-SHLF Power Shelf

The OS6800-BPS backup power supply is a separate, rack-mountable chassis offering power supply bays for up to eight power backup supply modules.

OS6800-BPS 225W Backup Power Supply

The OS6800-BPS 225W backup power supply provides backup power for one OS6800-24 or OS6800-48 switch. Up to eight OS6800-BPS 225 watt power supplies can be installed in the OS6800-BPS-SHLF power shelf.

Note. OS6800-BPS 225W backup power supplies are hot swappable.

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
802.1Q	OS6800	base
802.1d/1w Spanning Tree	OS6800	base
802.1s Multiple Spanning Tree	OS6800	base
802.1x Multiple Client Support	OS6800	base
Access Control Lists (ACLs)	OS6800	base
Authenticated Switch Access	OS6800	base
Authenticated VLANs	OS6800	base security
Basic IP Routing	OS6800	base
Command Line Interface (CLI)	OS6800	base
DNS	OS6800	base
DVMRP	OS6800	base advanced routing
End User Partitioning	OS6800	base
Ethernet Interfaces	OS6800	base
Health Statistics	OS6800	base
HTTP/HTTPS Port Configuration	OS6800	base
Interswitch Protocols (AMAP)	OS6800	all
IP Multicast Switching (IPMS)	OS6800	base
IPX Routing	OS6800	base
Learned Port Security (LPS)	OS6800	base
Link Aggregation	OS6800	base
Multicast Routing	OS6800	base advanced routing
NTP Client	OS6800	base
OSPF	OS6800	base advanced routing
Partitioned Switch Management	OS6800	base
Per-VLAN DHCP Servers	OS6800	base
PIM-SM **PIM-SSM (Source-Specific Multicast)**	OS6800	base advanced routing
Policy Server Management	OS6800	base
Port Mirroring	OS6800	base
Port Monitoring	OS6800	base
QoS/ACL & Layer 3 Security Enhancements	OS6800	base
Quality of Service (QoS)	OS6800	base

Feature	Platform	Software Package
RMON	OS6800	base
Router Discovery Protocol (RDP)	OS6800	base
Secure Shell (SSH)	OS6800	base
Smart Continuous Switching **Hot Swap** **Management Module Failover** **Power Monitoring** **Redundancy**	OS6800	base
SNMP	OS6800	base
Source Learning	OS6800	base
Software Rollback	OS6800	base
Stacking	OS6800	base
Switch Logging	OS6800	base
Text File Configuration	OS6800	base
UDP Relay	OS6800	base
VLANs	OS6800	base
VRRP	OS6800	base
Web-Based Management (WebView)	OS6800	base optional advanced routing optional security

Feature Descriptions

802.1Q

Alcatel's 802.1Q is an IEEE standard for sending frames through the network tagged with VLAN identification. 802.1Q tagging is the IEEE version of VLANs. It is a method of segregating areas of a network into distinct VLANs. By attaching a label, or tag, to a packet, it can be identified as being from a specific area or identified as being destined for a specific area.

When enabling a port to accept tagged traffic, one will also need to specify whether only 802.1Q tagged traffic is allowed on the port, or whether the port accepts both tagged and untagged traffic.

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. The flat mode applies a single spanning tree instance across all VLAN port connections on a switch. 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. However, if using 802.1D or 802.1w in the flat mode, the single spanning tree instance per switch algorithm applies.

802.1x Multiple Client Support

Physical devices attached to a LAN port on the 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 over LAN (EAPoL) 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 identity field in Alcatel 802.1x authentication works with all applications that send more than 32 bytes (e.g., Sygate).

Access Control Lists (ACLs)

Access Control Lists (ACLs) are Quality of Service (QoS) policies used to control whether or not packets are allowed or denied at the switch or router interface. ACLs are sometimes referred to as filtering lists.

ACLs are distinguished by the kind of traffic they filter. In a QoS policy rule, the type of traffic is specified in the policy condition. The policy action determines whether the traffic is allowed or denied.

In general, the types of ACLs include:

- *Layer 2 ACLs*—for filtering traffic at the MAC layer. Usually uses MAC addresses or MAC groups for filtering.
- *Layer 3/4 ACLs*—for filtering traffic at the network layer. Typically uses IP addresses or IP ports for filtering; note that IPX filtering is not supported.
- *Multicast ACLs*—for filtering IGMP traffic.

Authenticated Switch Access

Authenticated Switch Access (ASA) is a way of authenticating users who want to manage the switch. With authenticated access, all switch login attempts using the console or modem port, Telnet, FTP, SNMP, or HTTP require authentication via the local user database or via a third-party server. The type of server may be an authentication-only mechanism or an authentication, authorization, and accounting (AAA) mechanism.

AAA servers are able to provide authorization for switch management users as well as authentication. (They also may be used for accounting.) User login information and user privileges may be stored on the servers. The AAA servers supported on the switch are Remote Authentication Dial-In User Service (RADIUS) or Lightweight Directory Access Protocol (LDAP) servers.

Authentication-only servers are able to authenticate users for switch management access, but authorization (or what privileges the user has after authenticating) are determined by the switch. Authentication-only servers cannot return user privileges to the switch. The authentication-only server supported by the switch is ACE/Server, which is a part of RSA Security's SecurID product suite. RSA Security's ACE/Agent is embedded in the switch.

By default, switch management users may be authenticated through the console port via the local user database. If external servers are configured for other management interfaces but the servers become unavailable, the switch will poll the local user database for login information if the switch is configured for local checking of the user database. The database includes information about whether or not a user is able to log into the switch and what kinds of privileges or rights the user has for managing the switch.

Authenticated VLANs

Authenticated VLANs control user access to network resources based on VLAN assignment and a user log-in process; the process is sometimes called user authentication or Layer 2 Authentication. (Another type of security is device authentication, which is set up through the use of port-binding VLAN policies or static port assignment.) The number of possible AVLAN users is 2048.

Layer 2 Authentication is different from Authenticated Switch Access, which is used to grant individual users access to manage the switch.

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

Basic IP Routing

Internet Protocol (IP) is a network-layer (Layer 3) protocol that contains addressing and control information that allow packets to be forwarded on a network. IP is the primary network-layer protocol in the Internet protocol suite. Along with the Transmission Control Protocol (TCP), IP represents the heart of the Internet protocols. IP is associated with several Layer 3 and Layer 4 protocols. These protocols are built into the base code loaded on the switch and they include:

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Bootstrap Protocol (BOOTP)/Dynamic Host Configuration Protocol (DHCP)
- Simple Network Management Protocol (SNMP)
- Telnet
- File Transfer Protocol (FTP)
- Address Resolution Protocol (ARP)
- Internet Control Message Protocol (ICMP)
- RIP I / RIP II

The base IP software allows one to configure an IP router port, static routes, a default route, the Address Resolution Protocol (ARP), the router primary address, the router ID, the Time-to-Live (TTL) Value, IP-directed broadcasts, and the Internet Control Message Protocol (ICMP). In addition, this software allows one to trace an IP route, display Transmission Control Protocol (TCP) information, and display User Datagram Protocol (UDP) information.

Command Line Interface (CLI)

Alcatel’s command line interface (CLI) is a text-based configuration interface that allows you to configure switch applications and to view switch statistics. Each CLI command applicable to the switch is defined in the CLI Reference Guide. All command descriptions listed in the Reference Guide include command syntax definitions, defaults, usage guidelines, example screen output and release history.

The CLI uses single-line text commands that are similar to other industry standard switch interfaces.

DNS

A Domain Name System (DNS) resolver is an internet service that translates host names into IP addresses. Every time you enter a host name, a DNS service must look up the name on a server and resolve the name to an IP address. You can configure up to three domain name servers that will be queried in turn to resolve the host name. If all servers are queried and none can resolve the host name to an IP address, the DNS fails. If the DNS fails, you must either enter an IP address in place of the host name or specify the necessary lookup tables on one of the specified servers.

End User Partitioning (EUPM)

EUPM is used for customer login accounts that are configured with end-user profiles (rather than functional privileges specified by partitioned management). Profiles specify command areas as well as VLAN and/or port ranges to which the user has access. These profiles are typically used for end users rather than network administrators.

Ethernet Interfaces

Ethernet and Gigabit Ethernet port software is responsible for a variety of functions that support Ethernet, Gigabit, and 10 Gigabit Ethernet ports. These functions include initialization of ports, notifying other software modules when a port goes down, configuration of basic line parameters, gathering of statistics for Ethernet and Gigabit Ethernet ports, and responding to administrative enable/disable requests.

Configurable parameters include: trap port link messages, flow control, flow control wait time, line speed, duplex mode, inter-frame gap, combo port type and mode, resetting statistics counters, and maximum and peak flood rates.

Health Statistics

To monitor resource availability, the NMS (Network Management System) needs to collect significant amounts of data from each switch. As the number of ports per switch (and the number of switches) increases, the volume of data can become overwhelming. The Health Monitoring feature can identify and monitor a switch's resource utilization levels and thresholds, improving the efficiency in data collection.

Health Monitoring provides the following data to the NMS:

- Switch-level input/output, memory and CPU utilization levels
- Module-level and port-level input/output utilization levels

For each monitored resource, the following variables are defined:

- Most recent utilization level (percentage)
- Average utilization level over the last minute (percentage)
- Average utilization level over the last hour (percentage)
- Maximum utilization level over the last hour (percentage)
- Threshold level

Additionally, Health Monitoring provides the capacity to specify thresholds for the resource utilization levels it monitors, and generates traps based on the specified threshold criteria.

HTTP/HTTPS Port Configuration

In Release 5.3.1.R02 and later you can configure the default HTTP port and the default Secure HTTP (HTTPS) port for the embedded Web server in the switch.

Interswitch Protocol (AMAP)

Alcatel Interswitch Protocols (AIP) are used to discover adjacent switches and retain mobile port information across switches. By default, AMAP is not enabled.

The Alcatel Mapping Adjacency Protocol (AMAP) is used to discover the network topology of OmniSwitch, OmniS/R and/or OmniAccess switches in a particular installation. Using this protocol, each switch determines which OmniSwitch, Omni S/R and/or OmniAccess switches are adjacent to it by sending and responding to Hello update packets. For the purposes of AMAP, adjacent switches are those that:

- Have a Spanning Tree path between them
- Do not have any switch between them on the Spanning Tree path that has AMAP enabled
- GMAP is not supported

IP Multicast Switching (IPMS)

IP Multicast Switching is a one-to-many communication technique employed by emerging applications such as video distribution, news feeds, conferencing, netcasting, and resource discovery (OSPF, RIP2, BOOTP). Unlike unicast, which sends one packet per destination, multicast sends one packet to all devices in any subnetwork that has at least one device requesting the multicast traffic. Multicast switching also requires much less bandwidth than unicast techniques and broadcast techniques since the source hosts only send one data stream to the ports on which destination hosts that request it are attached.

Destination hosts signal their intent to receive a specific multicast stream by sending a request to do so to a nearby switch using Internet Group Management Protocol (IGMP). The switch then learns on which ports multicast group subscribers are attached and can intelligently deliver traffic only to the respective ports. This mechanism is often referred to as *IGMP snooping* (or *IGMP gleaning*). Alcatel's implementation of IGMP snooping is called IP Multicast Switching (IPMS). IPMS allows OmniSwitch 6800 Series switches to efficiently deliver multicast traffic in hardware at wire speed.

IGMP version 2 (IGMPv2), which handles forwarding by IP multicast destination address only, is supported. Note that IGMP version 3 (IGMPv3), which handles forwarding by source IP address and IP multicast destination, is *not* supported at this time.

IPX Routing

The Internet Packet Exchange (IPX) protocol, developed by Novell for NetWare, is a Layer 3 protocol used to route packets through IPX networks. (NetWare is Novell's network server operating system.)

IPX specifies a connectionless datagram similar to the IP packet of TCP/IP networks. An IPX network address consists of two parts: a network number and a node number. The IPX network number is assigned by the network administrator. The node number is the Media Access Control (MAC) address for a network interface in the end node.

Note. IPX routing is software-based only on OmniSwitch 6800 Series switches.

Learned Port Security (LPS)

Learned Port Security (LPS) provides a mechanism for authorizing source learning of MAC addresses on 10/100 and Gigabit Ethernet ports. Using LPS to control source MAC address learning provides the following benefits:

- A configurable source learning time limit that applies to all LPS ports.
- A configurable limit on the number of MAC addresses allowed on an LPS port.
- Dynamic configuration of a list of authorized source MAC addresses.
- Static configuration of a list of authorized source MAC addresses.
- Two methods for handling unauthorized traffic: Shutting down the port or only blocking traffic that violates LPS criteria.

LPS has the following limitations:

- You cannot configure 802.1x and LPS on the same ports.
- You cannot configure LPS on 10 Gigabit ports.
- You cannot configure LPS on link aggregate and 802.1Q tagged ports.

Link Aggregation (Static and Dynamic)

Alcatel's link aggregation software allows you to combine several physical links into one large virtual link known as a link aggregation group. Using link aggregation can provide the following benefits:

- **Scalability**. You can configure up to 32 link aggregation groups that can consist of 2, 4, or 8 Ethernet-ports.
- **Reliability**. If one of the physical links in a link aggregate group goes down, the link aggregate group can still operate.
- **Ease of Migration**. Link aggregation can ease the transition from a Gigabit Ethernet backbone to a 10 Gigabit Ethernet backbone.
- **Interoperability with Legacy Switches**. Static link aggregation can interoperate with OmniChannel on legacy switches.

Alcatel's link aggregation software allows you to configure the following two different types of link aggregation groups:

- Static link aggregate groups
- Dynamic (802.3ad) link aggregate groups

Multicast Routing

The OmniSwitch 6800 Series supports multicast routing and includes configuration options for multicast address boundaries, the Distance Vector Multicast Routing Protocol (DVMRP), and Protocol-Independent Multicast (PIM).

Multicast traffic consists of a data stream that originates from a single source and is sent to hosts that have subscribed to that stream. Live video broadcasts, video conferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news services are examples of multicast traffic. Multicast traffic is distinguished from unicast traffic and broadcast traffic.

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

DVMRP

Distance Vector Multicast Routing Protocol (DVMRP) is a dense-mode multicast routing protocol. DVMRP—which is essentially a “broadcast and prune” routing protocol—is designed to assist routers in propagating IP multicast traffic through a network. DVMRP works by building per-source broadcast trees based on routing exchanges, then dynamically creating per-source, group multicast delivery trees by pruning the source’s truncated broadcast tree.

PIM-SM
PIM-SSM

Protocol-Independent Multicast (PIM) is an IP multicast routing protocol that uses routing information provided by unicast routing protocols such as RIP and OSPF. PIM is “protocol-independent” because it does not rely on any particular unicast routing protocol. Sparse mode PIM (PIM-SM) contrasts with flood-and-prune dense mode multicast protocols such as DVMRP and PIM Dense Mode (PIM-DM) in that multicast forwarding in PIM-SM is initiated only via specific requests, referred to as *Join messages*.

Protocol Independent Multicast Source-Specific Multicast (PIM-SSM) is a highly-efficient extension of PIM. SSM, using an explicit channel subscription model, allows receivers to receive multicast traffic directly from the source; an RP tree model is not used. In other words, a Shortest Path Tree (SPT) between the receiver and the source is created without the use of a Rendezvous Point (RP).

NTP Client

The Network Time Protocol (NTP) is used to synchronize the time of a computer client or server to another server or reference time source, such as a radio or satellite receiver. It provides client time accuracies within half a second on LANs and WANs relative to a primary server synchronized to Universal Coordinated Time (UTC) (via a Global Positioning Service receiver, for example).

OSPF

Open Shortest Path First routing (OSPF) is a shortest path first (SPF) or link-state protocol. OSPF is an interior gateway protocol (IGP) that distributes routing information between routers in a single Autonomous System (AS). OSPF chooses the least-cost path as the best path. OSPF is suitable for complex networks with a large number of routers by providing faster convergence, loop free routing, and equal-cost multi-path routing where packets to a single destination can be sent to more than one interface simultaneously.

The following features are also supported:

- Graceful (Hitless) Support During Failover, which is the time period between the restart and the reestablishment of adjacencies after a planned (e.g., the users performs the takeover) or unplanned (e.g., the primary management module unexpectedly fails) failover.
- OSPF adjacencies over non broadcast links.
- Continuous forwarding during a graceful restart depends on several factors. If the secondary module has a different router MAC than the primary module, or if one or more ports of a VLAN belonged to the primary module, spanning tree re-convergence might disrupt the forwarding state, even though OSPF performs a graceful restart.

Partitioned Switch Management

A user account includes a login name, password, and user privileges. The privileges determine whether the user has read or write access to the switch, and which command domains and command families the user is authorized to execute on the switch. The privileges are sometimes referred to as *authorization*; the designation of particular command families or domains for user access is sometimes referred to as *partitioned management*.

Available command domains and families are listed in the following table:

Domain	Corresponding Families
domain-admin	file telnet dshell debug
domain-system	system aip snmp rmon web config
domain-physical	chassis module interface pmm health
domain-network	ip rip ospf vrrp ip-routing ipx ipmr ipms
domain-layer2	802.1q vlan bridge stp linkagg ip-helper
domain-service	dns
domain-policy	qos policy slb
domain-security	session avlan aaa

Per-VLAN DHCP Servers

The OmniSwitch allows you to configure the UDP Relay feature based on the VLAN ID of the DHCP request. For the Per-VLAN service, identify the number of the VLAN that makes the relay request. You may identify one or more server IP addresses to which DHCP packets will be sent from the specified VLAN.

Policy Server Management

Policy servers use the Lightweight Directory Access Protocol (LDAP) to store policies that are configured through Alcatel’s PolicyView network management application. PolicyView is an OmniVista application that runs on an attached workstation.

The Lightweight Directory Access Protocol (LDAP) is a standard directory server protocol. The LDAP policy server client in the switch is based on RFC 2251. Currently, PolicyView is supported for policy management.

The switch communicates with the LDAP server to download and manage LDAP policies. The switch has separate mechanisms for managing QoS policies stored in PolicyView and QoS policies configured directly on the switch.

Port Mirroring

You can set up Port Mirroring for any pair of Ethernet ports within the same switch chassis or across several switches within a stack. When Port Mirroring is enabled, the active “mirrored” port transmits and receives network traffic normally, and the “mirroring” port receives a copy of all transmit and receive traffic to the active port. You can connect an RMON probe or network analysis device to the mirroring port to see an exact duplication of traffic on the mirrored port without disrupting network traffic to and from the mirrored port.

One Port Mirroring session is supported in a standalone switch or stack. OmniSwitch 6800 Series switches support “N-to-1” port mirroring where “N” can be a number from 1 to 24 on a standalone switch or a stack. In other words, you can configure up to 24 source ports for a single destination port in a session on a stack.

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. The OmniSwitch 6800 supports one session per switch or stack.

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. See the *OmniSwitch 6800 CLI Reference Guide and the OmniSwitch 6800 Series Network Configuration Guide* for more information.

Quality of Service (QoS)

Alcatel's QoS software provides a way to manipulate flows coming through the switch based on user-configured policies. The flow manipulation (generally referred to as *Quality of Service* or *QoS*) may be as simple as allowing/denying traffic, or as complicated as remapping 802.1p bits from a Layer 2 network to ToS values in a Layer 3 network.

QoS is implemented on the switch through the use of policies, created on the switch or stored in Policy-View.

While policies may be used in many different types of network scenarios, there are several typical types:

- **Basic QoS**—includes traffic prioritization and bandwidth shaping
- **802.1p/ToS/DSCP**—includes policies for marking and mapping
- **Access Control Lists (ACLs)—**ACLs are a specific type of QoS policy used for Layer 2, Layer 3/4, and multicast filtering.

QoS/ACL & Layer 3 Security Enhancements

The following additional ACL features are available for improving network security and preventing malicious activity on the network:

- **ICMP drop rules**—Allows condition combinations in policies that will prevent user pings, thus reducing DoS exposure from pings. Two condition parameters are also available to provide more granular filtering of ICMP packets: **icmptype** and **icmpcode**.
- **BPDUShutdownPorts**—A port group that identifies its members as ports that should not receive BPDUs. If a BPDU is received on one of these ports, the port is administratively disabled.
- **TCP connection rules**—Allows the determination of an *established* TCP connection by examining TCP flags found in the TCP header of the packet. Two condition parameters are available for defining a TCP connection ACL: **established** and **tcpflags**.
- **Early ARP discard**—ARP packets destined for other hosts are discarded to reduce processing overhead and exposure to ARP DoS attacks. No configuration is required to use this feature, it is always available and active on the switch. Note that ARPs intended for use by a local subnet, AVLAN, and VRRP are *not* discarded.

RMON

Remote Network Monitoring (RMON) is an SNMP protocol used to manage networks remotely. *RMON probes* can be used to collect, interpret and forward statistical data about network traffic from designated active ports in a LAN segment to an NMS (Network Management System) application for monitoring and analysis without negatively impacting network performance. RMON software is fully integrated in the software to acquire statistical information.

This feature supports basic RMON 4 group implementation in compliance with RFC 2819, including the **Ethernet Statistics**, **History** (Control & Statistics), **Alarms** and **Events** groups.

Router Discovery Protocol (RDP)

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

Secure Shell (SSH)

The Secure Shell feature provides a secure mechanism that allows you to log in to a remote switch, to execute commands on a remote device, and to move files from one device to another. Secure Shell provides secure, encrypted communications even when your transmission is between two untrusted hosts or over an unsecure network.

The OmniSwitch includes both client and server components of the Secure Shell interface and the Secure Shell FTP file transfer protocol. SFTP is a subsystem of the Secure Shell protocol. All Secure Shell FTP data are encrypted through a Secure Shell channel.

When used as an SSH Server, the following SSH Software is supported on the indicated operating systems:

SSH Software	Supported Operating Systems
OpenSSH	Sun Solaris, Win NT + Cygwin, Mac OSX, Linux Red Hat
F-Secure	Sun Solaris, Win 2000, Win NT, Win XP, Mac OS9
SSH-Communication	Sun Solaris, Win 2000, Win NT, Win XP, Linux Red Hat
PuTTY	Win 2000, Win NT, Win XP, Mac OS9
MAC-SSH	Mac OS9, Mac OSX

When used as an SSH Client, the following SSH Software is supported on the indicated operating systems:

SSH Software	Supported Operating Systems
OpenSSH	Sun Solaris, Win NT + Cygwin, Linux Red Hat, AOS
F-Secure	Sun Solaris, Win 2000, Win NT
SSH-Communication	Sun Solaris, Win 2000, Win NT, Win XP, Linux Red Hat

Smart Continuous Switching

In stacked configurations, one OmniSwitch 6800 switch is designated as the primary "management module" for the stack. Because the stack can be thought of as a virtual chassis, the role of this primary management switch is to monitor and manage the functions of the entire stack.

Similar to chassis-based switches, the stack also includes a secondary, or backup, management module. A stack's secondary switch immediately takes over management functions in the event of a primary switch failure.

All switches in the stack, besides the primary and secondary switch, are considered idle or in pass-through. Idle switches act like Network Interface (NI) modules in chassis-based switches.

The stack provides support for all idle switches during primary switch failover. In other words, if the primary switch in the stack fails or goes offline for any reason, all idle switches will continue data transmission during the secondary switch's takeover process.

SNMP

The Simple Network Management Protocol (SNMP) is an application-layer protocol that allows communication between SNMP managers and SNMP agents on an IP network. Network administrators use SNMP to monitor network performance and to solve network problems. SNMP provides an industry standard communications model used by network administrators to manage and monitor their network devices. OmniSwitch 6800 Series switches support SNMPv1, SNMPv2, and SNMPv3.

Source Learning

Source Learning builds and maintains the MAC address table on each switch. New MAC address table entries are created in one of two ways: they are dynamically learned or statically assigned. Dynamically learned MAC addresses are those that are obtained by the switch when source learning examines data packets and records the source address and the port and VLAN it was learned on. Static MAC addresses are user defined addresses that are statically assigned to a port and VLAN.

In addition, Source Learning also tracks MAC address age and removes addresses from the MAC address table that have aged beyond the configurable aging timer value.

Accessing MAC Address Table entries is useful for managing traffic flow and troubleshooting network device connectivity problems.

Software Rollback

The directory structure inherent in an OmniSwitch 6800 Series switch allows for a switch to return to a previous, more reliable version of image or configuration files.

Changes made to the configuration file may alter switch functionality. These changes are not saved unless explicitly done so by the user. If the switch reboots before the configuration file is saved, then the certified directory is re-loaded and changes made to the configuration file prior to the reboot are lost.

Likewise, new image files should be placed in the working (non-certified) directory first. New image or configuration files can be tested to decide whether they are reliable. Should the configuration or images files prove to be less reliable than their older counterparts in the certified directory, then the switch can be rebooted from the certified directory, and "rolled back" to an earlier version.

Once the contents of the working directory are established as good files, then these files can be saved to the certified directory and used as the most reliable software to which the switch can be rolled back to in an emergency situation.

Note. It is not necessary to reboot an entire OS6800 stack for synchronization of the configuration.

Stacking

OmniSwitch 6800 and OmniSwitch 6800L switches use global module identifiers—referred to as *tokens*—for budgeting stack ASIC resources. Each stack offers 32 tokens, with each module added to the stack using a specific number of these tokens. For a list showing the number of tokens used by each module type, refer to the table below.

Module Type	Tokens Used	Maximum Allowed per Stack
OS6800-24	2	8
OS6800-24L	2	8
OS6800-48	4	8
OS6800-48L	4	8
OS6800-48 with 10 Gigabit uplink	6	5
OS6800-48L with 10 Gigabit uplink	6	5
OS6800-U24	2	N/A
OS6800-U24 with 10 Gigabit uplink	4	N/A

Note. Synchronization of switches in a stack can take up to 20 minutes in some configurations.

Note: During bootup of a stack, once 32 tokens have been used, it will put the remaining switches in pass-through mode.

Switch Logging

The Switch Logging feature is designed to provide a high-level event logging mechanism that can be useful in maintaining and servicing the switch. Switch Logging uses a formatted string mechanism to process log requests from applications. When a log request is received, Switch Logging verifies whether the Severity Level included with the request is less than or equal to the Severity Level stored for the appropriate Application ID. If it is, a log message is generated using the formatting specified by the log request and placed on the Switch Log Queue, and Switch Logging returns control back to the calling application. Otherwise, the request is discarded. The default output device is the log file located in the Flash File System. Other output devices can be configured via the Command Line Interface. All log records generated are copied to all configured output devices.

The Command Line Interface can be used to display and configure Switch Logging information. Log information can be helpful in resolving configuration or authentication issues, as well as general errors.

Text File Configuration

The text file configuration feature allows you to configure the switch using an ASCII-based text file. You may type CLI commands directly into a text document to create a *configuration file*. This file resides in the switch's file system. You can create configuration files in the following ways.

- You may create, edit and view a file using a standard text editor (such as Microsoft NotePad) on a workstation. The resulting configuration file is then uploaded to the switch.
- You can invoke the switch's CLI **snapshot** command to capture the switch's current configuration into a text file.
- You can use the switch's text editor to create or make changes to a configuration file.

UDP Relay

The User Datagram Protocol (UDP) is a connectionless transport protocol that runs on top of IP networks. UDP is used for applications that do not require the establishment of a session and end-to-end error checking. Email and file transfer are two applications that could use UDP. UDP offers a direct way to send and receive datagrams over an IP network and is primarily used for broadcasting messages. The UDP Relay feature allows UDP broadcast packets to be forwarded across groups and VLANs that have IP routing enabled. UDP Relay ensures that the DHCP mechanism is operational and it allows you to use nonroutable protocols in a routing environment. UDP Relay is configured using the IP helper set of commands.

VLANs

In a flat bridged network, a broadcast domain is confined to a single LAN segment or even a specific physical location, such as a department or building floor. In a switch-based network, such as one comprised of Alcatel switching systems, a broadcast domain—or *VLAN*— can span multiple physical switches and can include ports from a variety of media types. For example, a single VLAN could span three different switches located in different buildings and include Ethernet, Gigabit, 802.1q tagged ports or a link aggregate of ports.

Initially all switch ports are non-mobile and are assigned to VLAN 1. When additional VLANs are created on the switch, ports are assigned to the VLANs so that traffic from devices connected to these ports is bridged within the VLAN domain. Switch ports are either statically or dynamically assigned to VLANs.

Static port assignment applies to both mobile and non-mobile (fixed) ports. Fixed ports are also statically assigned to *secondary* VLANs by defining 802.1Q tagged VLANs for the port. In addition, ports can belong to a link aggregate of ports. Dynamic assignment applies only to mobile ports and requires the additional configuration of VLAN rules. When traffic is received on a mobile port, the packets are examined to determine if their content matches any VLAN rules configured on the switch. Rules are defined by specifying a port, MAC address, protocol, network address, binding, or DHCP criteria to capture certain types of network device traffic. It is also possible to define multiple rules for the same VLAN. A mobile port is assigned to a VLAN if its traffic matches any one VLAN rule.

VRRP

The Virtual Router Redundancy Protocol (VRRP) is a standard router redundancy protocol supported in IP version 4. It is based on RFC 2338 and provides redundancy by eliminating the single point of failure inherent in a static default route environment.

VRRP allows routers on a LAN to back up a static default route with a virtual router. VRRP dynamically assigns responsibility for a virtual router to a physical router (VRRP router) on the LAN. The virtual router is associated with an IP address (or set of IP addresses) on the LAN. A virtual router master is elected to forward packets for the virtual router's IP address. If the master router becomes unavailable, the highest priority backup router will transition to the master state.

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

Note. The *OmniSwitch 6800 Series Network Configuration Guide* incorrectly states that the maximum number of virtual routers is 7. The correct number is 255.

Web-Based Management (WebView)

The switch can be monitored and configured using WebView, Alcatel's web-based device management tool. The WebView application is embedded in the switch and is accessible via the following web browsers:

- Internet Explorer 6.0 and later for Windows NT, 2000, XP, 2003
- Netscape 7.1 for Windows NT, 2000, XP
- Netscape 7.0 for Solaris SunOS 5.8

WebView contains modules for configuring all software features in the switch. Configuration and monitoring pages include context-sensitive on-line help.

Supported Traps

The following traps are supported in 5.3.1.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	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	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 alaStackMgrSlotNINumber 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 alaStackMgrSlotNINumber 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 alaStackMgrSlotNINumber 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	A File Written Trap is sent when the amount of data requested by the user has been written by the port monitoring instance.

Unsupported Software Features

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

Feature	Platform	Software Package
Interswitch Protocols (GMAP)	OS6800	base
OSPF Database Overflow (RFC 1765)	OS6800	base advanced routing
Policy-Based Routing	OS6800	base

Unsupported Features on the OS6800-XNI-U2

Feature	Platform	Software Package
802.1x Multi Client Support	OS6800	base
AVLANs	OS6800	base
Group Mobility	OS6800	base
Learned Port Security (LPS)	OS6800	base
Port Monitoring	OS6800	base
User Port/Network Port	OS6800	base

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**
IPMS	**ip multicast hardware-routing (not supported on 6800 switches)**
NTP	**no ntp server all**
QoS	**qos classify fragments** **qos flow timeout** **show policy classify destination interface type** **show policy classify source interface type**

Unsupported MIBs

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

Feature	MIB
Interswitch Protocols (GMAP)	**All MIBs are unsupported.**
Quality of Service (QoS)	**IETF_P_BRIDGE**

Unsupported MIB Variables

MIB Name	Unsupported MIB variables	
AlcatelIND1AAA	aaauProfile	
AlcatelIND1Bgp	alaBgpGlobal alaBgpPeerTable alaBgpAggrTable alaBgpNetworkTable alaBgpRedistRouteTable alaBgpRouteTable alaBgpPathTable alaBgpDampTable alaBgpRouteMapTable alaBgpAspathMatchListTable alaBgpAspathPriMatchListTable alaBgpPrefixMatchListTable alaBgpCommunityMatchListTable alaBgpCommunityPriMatchListTable alaBgpDebugTable	
AlcatelIND1Dot1Q	qPortVlanForceTagInternal	
AlcatelIND1GroupMobility	vPortIpBRuleTable vMacIpBRuleTable vMacPortProtoBRuleTable vCustomRuleTable	
AlcatelIND1Health	healthDeviceTemperatureCmmCpuLatest healthDeviceTemperatureCmmCpu1MinAvg healthDeviceTemperatureCmmCpu1HrAvg healthDeviceTemperatureCmmCpu1HrMax	
AlcatelIND1Ipms	alaIpmsForwardSrcIpAddr alaIpmsForwardSrcIfIndex	
AlcatelIND1LAG	alclnkaggAggEniActivate alclnkaggSlotTable	
AlcatelIND1Pcam	alcatelIND1PCAMMIBObject s alaCoroL3HrePerModeTable alaCoroL3HrePerCoronadoSta tsTable alaCoroL3HreChangeTable	
AlcatelIND1Port	esmPortCfgLongEnable esmPortCfgRuntEnable esmPortCfgRuntSize esmPortPauseSlotTime	alcether10GigTable

MIB Name	Unsupported MIB variables
AlcatelIND1QoS	alaQoSPortPdiTable alaQoSSlotPcamTable alaQoSPortProtocolTable alaQoSSlotProtocolTable alaQoSSlotDscpTable alaQoSRuleReflexive alaQoSAppliedRuleReflexive alaQoSActionSourceRewriteIpAddr alaQoSActionSourceRewriteIpAddrStatus alaQoSActionSourceRewriteIpMask alaQoSActionTable alaQoSActionSourceRewriteNetworkGroup alaQoSActionTable alaQoSActionSourceRewriteNetworkGroupStatus alaQoSActionTable alaQoSActionDestinationRewriteIpAddr alaQoSActionTable alaQoSActionDestinationRewriteIpAddrStatus alaQoSActionTable alaQoSActionDestinationRewriteIpMask alaQoSActionTable alaQoSActionDestinationRewriteNetworkGroup alaQoSActionTable alaQoSActionDestinationRewriteNetworkGroupStatus alaQoSActionTable alaQoSActionLoadBalanceGroup alaQoSActionTable alaQoSActionLoadBalanceGroupStatus alaQoSActionTable alaQoSActionPermanentGatewayIpAddr alaQoSActionTable alaQoSActionPermanentGatewayIpAddrStatus alaQoSActionTable alaQoSActionAlternateGatewayIpAddr alaQoSActionAlternateGatewayIpAddrStatus alaQoSAppliedActionSourceRewriteIpAddr alaQoSAppliedActionSourceRewriteIpAddrStatus alaQoSAppliedActionSourceRewriteIpMask alaQoSAppliedActionSourceRewriteNetworkGroup alaQoSAppliedActionSourceRewriteNetworkGroupStatus alaQoSAppliedActionDestinationRewriteIpAddr alaQoSAppliedActionDestinationRewriteIpAddrStatus alaQoSAppliedActionDestinationRewriteIpMask alaQoSAppliedActionDestinationRewriteNetworkGroup alaQoSAppliedActionDestinationRewriteNetworkGroupStatus alaQoSAppliedActionLoadBalanceGroup alaQoSAppliedActionLoadBalanceGroupStatus alaQoSAppliedActionPermanentGatewayIpAddr alaQoSAppliedActionPermanentGatewayIpAddrStatus alaQoSAppliedActionAlternateGatewayIpAddr alaQoSAppliedActionAlternateGatewayIpAddrStatus alaQoSPortDefaultQueues alaQoSPortAppliedDefaultQueues alaQoSConfigNatTimeout alaQoSConfigAppliedNatTimeout alaQoSConfigReflexiveTimeout alaQoSConfigAppliedReflfexiveTimeout alaQoSConfigFragmentTimeout alaQoSConfigAppliedFragmentTimeout alaQoSConfigClassifyFragments alaQoSConfigAppliedClassifyFragments
AlcatelIND1Slb	slbFeature slbClusterTable slbServerTableg
AlcatelIND1StackManager	alaStackMgrStatsTable
AlcatelIND1SystemService	systemUpdateStatusTable

MIB Name	Unsupported MIB variables	
AlcatelIND1VlanManager	vlanIpxNet vlanIpxEncap vlanIpxRipSapMode vlanIpxDelayTicks vlanSetMultiRtrMacStatus	vlanIpxStatus vlanSetIpxRouterCount
AlcatelIND1WebMgt	alaIND1WebMgtRFSConfigTable alaIND1WebMgtHttpPort alaIND1WebMgtHttpsPort	
IEEE_802_1X	dot1xAuthDiagTable dot1xAuthSessionStatsTable dot1xSuppConfigTable dot1xSuppStatsTable	
IETF_BGP4	bgpRcvdPathAttrTable bgp bgpPeerTable bgp4PathAttrTabl	
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	
IETF_MAU (RFC 2668)	rpMauTable rpJackTable broadMauBasicTable ifMauFalseCarriers ifMauTypeList ifMauAutoNegCapability ifMauAutoNegCapAdvertised ifMauAutoNegCapReceived	
IETF_OSPF (RFC 1850)	ospfAreaRangeTable	
IETF_OSPF_TRAP	ospfTrapControl	
IETF-PIM	pimRPTable	

MIB Name	Unsupported MIB variables
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
IETF_SNMP_TARGET (RFC 2573)	snmpTargetAddrTable snmpTargetParamsTable snmpTargetSpinLock
IETF_SNMP_USER_BASED_SM (RFC 2574)	usmUser
IETF_SNMP_VIEW_BASED_ACM (RFC 2575)	vasmMIBViews

Fixed Problem Reports

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

Switch Management

General

Fixed Problem Reports

PR 86910

XON-XOFF handshaking on the console port is always disabled after rebooting.

PR 87338

Health statistics for hybrid ports using copper are too low.

Command Line Interface (CLI)

Fixed Problem Reports

PR 83187

The CLI command **debug chassis hello timers** may cause the CMM to reboot on the Stacking chassis.

PR 85228

An expanded **ip debug** command is not available.

PR 85419

When **show ni <n>** or **show module long** CLI commands are used, GBIC information is displayed so that one may mistake it for the daughter board information.

PR 86694

vlan <vid> stp < on | off> : This command still has an affect and is left in for backwards compatibility.

PR 86980

Normally, typing **ip dvmrp prune-timeout** would reset the DVMRP prune timeout value to its default value of 30.

PR 87612

When the password for a user is longer then 47 characters, the error message "internal error" is displayed on the console.

PR 87613

The OS6800 Client 5.3.1.R01 does not allow user names greater than 31 characters, 5.3.1.R02 allows 64 characters.

PR 87998

If the CLI session times out on a telnet session with more enabled, the switch will lock up.

PR 91136

A VLAN whose Spanning Tree is disabled doesn't retain the name if it is changed.

RMON

Fixed Problem Reports

PR 87683

The RMON object etherStatsPkts65to127Octs and other similar objects from RFC 1757 contains both TX and RX packet counts.

Web-based Management (WebView)

Fixed Problem Reports

PR 81893

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

PR 82309

The virtual Open Shortest Path First interface status is not displayed in WebView.

PR 83215

In WebView, System > System Mgmt > Switch Logging > Logging Output page:

1. When unchecking the check box of "Log to a Remote Host" and clearing "IP Address" box, the IP Address still is displayed.
2. When modifying the "IP Address" without first unchecking the check box of "Log to a Remote Host", the IP Address will not be changed.

PR 86248

WebView doesn't show the running priority of virtual router.

PR 87035

Problem 1: Autonegotiation cannot be disabled through the Modify Page of WebView if flow control is untouched.
Problem 2: When autonegotiation is disabled, the subsystem changes the speed to 100 and duplex to half (which is correct), but doesn’t change the maximum frame and flood rate, which are dependent on the speed. So, when we try to reenable auto negotiation through the Modify Page of WebView.

PR 87479

WebView does not display root path cost and next best root path cost properly.

PR 87494

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

PR 87565

The BPDU switching flag does not get applied after reboot.

PR 87774

When autonegotiation is disabled, the subsystem makes the speed 100, and duplex half, but doesn't change the floodrate and max frame size which are speed dependent. This causes the problem when autonegotiation is being reenabled through the Modify Page.

PR 87917

AVLAN and AAA check boxes are mixed up when selecting family privileges for a user.

PR 90287

Enabled Web based AVLAN authentication on Windows platform, when a http proxy server is configured.

PR 91274

Fixed auto-redirection for Web based AVLAN authentication.

Layer 2

Bridging

Fixed Problem Reports

PR 87516

When forced hybrid mode (e.g. forced-fiber) is used for hybrid ports, the user should not plug in an active link on the second media (e.g. copper, other than the one which is forced). The OS6800 may confuse it with the second media link (if present and active) as link UP, even when the forced media link goes down. The OS6800 may not report a link down for forced media in this case.

PR 87666

When the max frame size of 1518 is set in configuration, and the switch is rebooted, it doesn't get applied. The problem is only with this value management (WebView).

PR 87717

If the mobile-tag option is configured, we do not drop tagged DHCP frames.

Ethernet Interfaces

Fixed Problem Reports

PR 87854

On a hybrid (combo) port, if the mode is preferred fiber and the speed of the configured active media (which in this case is fiber) is changed to auto, the error message pops up indicating this is invalid (which is correct). But, for subsequent commands where the speed is set to auto, no error message comes, this is just a cosmetic issue.

Interswitch Protocols (AMAP)

Fixed Problem Reports

PR 87961

AMAP discovery hello packet is not sent out on link aggregation ports.

IP Multicast Switching (IPMS)

Fixed Problem Reports

PR 87924

IP Multicast traffic transmitted and received on Ethernet SNAP networks is not supported.

PR 91332

Under some cicumstances, multicast traffic egressing on a 10G port of the OS6800 was replicated improperly. This was because a bug in the multicast software on NI was rearranging the replication table incorrectly.

PR 91432

Previously, if the switch received a query on port p1, and received reports for group G on ports p1 and p2, then the switch would not proxy report on p2 onto p1. This was acceptable because in a steady environment one would not see this kind of reporting. But, after a topology change, the switch can see a query on a new port while the query from the old port still exists in its database. This caused the proxying to be delayed until the old query and report were removed from the database. The whole process took 510 seconds at least. With the fix, the proxy report received on p2 onto p1. This has reduced the recovery time to at most 125 seconds.

Spanning Tree

Fixed Problem Reports

PR 88606

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

PR 89948

If Spanning Tree is disabled and the unit is rebooted, then Spanning Tree will be enabled again.

PR 90887

BPDUs coming from a non-designated port were not transmitted to other aggregate ports in other slots, causing the Spanning Tree state machines that were waiting for the agreement bit to get stuck in listening state.

PR 91149

Failure to check for the correct non-edge status between bridge links could lead to a temporary loop during link up.

VLANs

Fixed Problem Reports

PR 86932

When a VLAN that has a rule configured is deleted, the user might see an error message on the console.

Layer 3

Basic IP Routing

Fixed Problem Reports

PR 85465

When an Aggregate Summary Area Address Range is created for a non-backbone area on an Area Border Router, and the interfaces from this ABR to that non-backbone area are deleted, the Area Address Range is still considered Active when it really should be Inactive.

This will cause the Intra-Area Summary Route with the Gateway set to 127.0.0.1 to be present in the Open Shortest Path First Routing Table, though the Area Address Range is Inactive because there are no matching Intra-Area Routes for the Address Range.

UDP Relay

Fixed Problem Reports

PR 87515

When the bootup option is turned on in the IP HELPER CLI command, even if the default VLAN is disabled, the DHCP request still goes out.

Quality of Service (Includes ACLs and NAT)

Fixed Problem Reports

PR 87958

If the user defines a single policy that specifies an 802.1p stamping action and rate-limiting action simultaneously, the OS6800 will affect only the 802.1p stamping action. The traffic will not be rate limited.

Advanced Routing

DVMRP

Fixed Problem Reports

PR 87738

When dynamically loading DVMRP on a switch with many PIMSM interfaces that are already enabled and operational, it's possible to see messages on the console similar to this:
tDvmrp-: dvmrpRecvIpmrmProto: Non-existent V236 for Proto 8.

OSPF

Fixed Problem Reports

PR 87988

When 20,000 or more AS-External LSAs are max-aged (flushed due to not being refreshed by originating ASBR) simultaneously at the same time, high CPU utilization by OSPF task may cause loss of adjacency with neighboring OSPF routers.

PR 87996

If more than one OSPF interface has been configured for MD5 authentication, WebView does not show all the interfaces.

PR 90093

When aggregating routes redistributed into OSPF, the gateway address of the redistributed route is not set to 0, resulting in OSPF trying to use different forwarding addresses for the corresponding AS-External Link State Aggregate.

PR 91491

When external routes have a forwarding address, and there is a change in the OSPF internal path to the forwarding address, the external route SPFcalculations are not re-run, resulting in the loss of one of the ECMP nexthops to the external destination.

PIM-SM

Fixed Problem Reports

PR 84167

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

PR 88356

The switch locks up when PIM-SM is enabled.

Security

AVLAN

Fixed Problem Reports

PR 87362

When a PC is connected to an AVLAN port and the PC's link is unplugged and moved to a different port on the network, AVLAN is not able to detect that the PC is moved and thus always show as connected.

General

Fixed Problem Reports

PR 87109

For HTTP AVLAN multi-language support, in /flash/switch/label.txt, each length of the textual field cannot be longer than 255. Otherwise, it will cause a memory corruption and the switch will not come up properly after reboot.

PR 90092

If the DHCP server is on the same VLAN as the PC, the PC is not able to get an IP address from the DHCP server.

Policy Server Management

Fixed Problem Reports

PR 87947

Using PolicyView, the user can create policies specifying "destination vlan" as a policy condition parameter. The QoS manager on the OS6800 rejects the policy, but PolicyView is not aware of this and thus there is no feedback to the user.

System

Chassis Supervision

Fixed Problem Reports

PR 87956

When the CPU is at 100% utilization, the message "ERROR" may be seen following flash synchronization. The only side-effect is waiting a few seconds for the console prompt to return following the message.

PR 90574

This is a status message sent when the CSM certification is done.

General

Fixed Problem Reports

PR 83540

NTP synchronized time does not include daylight savings time.

PR 87373

The MTU option is not supported on the OS6800.

PR 87611

Changing the error message when a user name or password greater than 31 characters was entered. Currently the error message displayed is "Authentication failure : Invalid login or password".

PR 91009

The VLAN remains operational even if the NI, with the only active ports in the VLAN, is powered down.

Redundancy/Hot Swap

Fixed Problem Reports

PR 87549

When a takeover is performed, mobile VLANs on certain NI ports might not be communicated to the CMM.

PR 87778

When takeover happens, a bogus message is sent to the new secondary with an invalid message type. Most of the time, the message is discarded due to the un-recognized message type.

Stack Manager

Fixed Problem Reports

PR 87355

Egress mirroring is supported across the stack up to a stack of 3 elements. A redundant stacking cable is required (i.e. stack must be in a ring/loop configuration). In a stack of more than 3 elements, egress mirroring is supported only within an element, and is not supported across the stack.

Please Note: This limitation does not apply to ingress mirroring; ingress mirroring is supported across the stack, up to a stack of 8 elements.

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 83127

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

Workaround: The issue is cosmetic and doesn't affect performance of the switch.

PR 85206

From the CLI, the user cannot specify the type of the LDAP server. Even if the user specifies the field as "Microsoft" the display shows it as Netscape.

Workaround: The user need not specify any type of information. The type of server is automatically detected by the switch. Even if the user does specify, and it displays as "Netscape" it is a display error. No error in functionality.

PR 86842

On the secondary CMM during a takeover, a "SESMGR_CLISHELL_TERMINATE" will be seen.

Workaround: This is not a problem, but part of a design that supports the synchronization of configuration without reloading all stacks.

PR 87400

The CLI session on the secondary will timeout at the default setting of 10 minutes.

Workaround: This is due to the boot.cfg not being parsed on the secondary. There is no known work around at this time.

PR 87642

The CLI command to specifically disable 802.1x or AVLAN authentication on a port will disable either of the authentication options configured on the port.

Workaround: There is no known workaround at this time.

PR 90479

The IPX network rule encapsulation **E2** and **ETHERNET2** are redundant. WebView uses the encapsulation **ETHERNET2** only. To avoid confusion, the redundant encapsulation **E2** has been removed from the CLI command; the **ETHERNET2** encapsulation will remain.

Workaround: There is no known workaround at this time.

PR 90828

Configuring port number 65535 using https returns a binding error.

Workaround: Use ports 1024-65534.

PR 90863

If a telnet session is killed while in the middle of displaying a long show command, the console connection is lost and the system dies after about 60 seconds.

Workaround: Do not kill a session while in the middle of displaying a long show command.

RMON

Problem Reports

PR 87692

RMON counts oversized (1519 to 9216 bytes) packets as dropped, even though they are forwarded.

Workaround: There is no known workaround at this time. CLI classifies the same packets as error packets.

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.

PR 88312

Some collisions do not appear in RMON statistics.

Workaround: There is no known workaround at this time.

SNMP

Problem Reports

PR 82635/86533

Fan information is unavailable via SNMP or WebView.

Workaround: Use CLI to determine fan information.

PR 83761

Switch user cannot be created via SNMP.

Workaround: There is no known workaround at this time.

PR 85235

TemperatureCmm family SNMP variables show in AdventNet are not available in OS6600 and OS6800. As a result, the SNMP Agent treats these variables as non-existent on these platforms.

Workaround: Not applicable.

PR 87084

SNMP test returns an out of range value for aipAMAPVoiceVlan.

Workaround: There is no known workaround at this time.

Web-based Management (WebView)

Feature Exceptions

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

Problem Reports

PR 66619

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

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

PR 68906

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

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

PR 79700

The status field in the OSPF Hosts page always displays “**ERR("0")**” instead of “Active” or “Not in Service”.

Workaround: Use the **show ip ospf host** CLI command to display the current status.

PR 80236

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

Workaround: The user click must click the refresh button in order to see the directory contents on the screen.

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 85654

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

Workaround: read-write and read-only behave the same.

PR 87094

After using WebView to apply the Spanning Tree protocol disable on VLAN 1, to disable flat spanning tree, the Spanning Tree menu still shows the Spanning Tree Protocol to be enabled. However, the Spanning Tree is really disabled.

Workaround: Using the VLAN WebView commands and CLI commands will show the correct Spanning Tree protocol status.

PR 87561

When the hybrid port is configured in preferred mode, and if the non preferred media (or inactive media) has the link up, then WebView doesn't show the operational status correctly.

Workaround: Use CLI or SNMP to get the operational status of the port.

PR 87645

The smallest time granularity a user can provide is one day.

Workaround: There is no known workaround at this time. The user might specify expiration time in days.

PR 87665

Moving a directory into a directory with a directory of the same name results in an ambiguous error.

Workaround: There is no known workaround at this time.

PR 87807

WebView: Physical > Health > LED Status table shows on "Status" row Primary for all stacked switches.

Workaround: Please ignore values shown on this page and get the correct status from Physical > CMM > Hardware "Status" row.

PR 87952

When one pushes the file action button without a file selected, an error does not appear. Also, when multiple files are selected, an error does not appear.

Workaround: There is no known workaround at this time. Only one file can be selected, but if either of the above two cases occurs, the user does not see an error.

PR 87955

Remote System File Management: Performance Status shows "System Error" after listing the files.

Workaround: The error is purely cosmetic and does not effect functionality.

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 88019

In WebView, the Networking > IP > Routes > EMP page is not applicable to this product.

Workaround: Ignore the page.

PR 88140

In WebView, after using the **Clear Statistics** button on the Physical > Health > Slice page, the table may not show correctly (everything is cleared including slot/slice information).

Workaround: This issue is due to timing; the page shows up while the table is in the midst of being populated, so refreshing the table should allow for the slot and slice information to come up normally.

PR 88325

On the chassis home page an OS6800-U24 shows as an OS6800-U24 with 24 copper ports.

Workaround: There is no known workaround at this time. This is a small cosmetic difference.

PR 88558

When creating a static ARP with the wrong port number (e.g. the port is not active in the VLAN for which you are creating the ARP) the subsystem returns a warning. WebView does not act on the warning and the user is not informed about the misconfiguration.

Workaround: There is no known workaround at this time.

PR 89167

In WebView, on the Physical > Ethernet > Statistics > Traffic page, data might be different from the CLI output from **show interfaces traffic**.

Workaround: Please refer to the CLI output.

PR 89576

In WebView, the Networking > IP > OSPF > Interfaces > Area page shows the wrong value for **Priority** on the table.

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

PR 90085

In WebView, on the Policy > Policy > Conditions > All modify page, the **Source Port** might not be modified.

Workaround: Use the Conditions > Slot/Port Modify page instead.

PR 90420

On the OS6800, the LEDs do not blink.

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

PR 90424

In WebView, on the Physical > Health > LED Status page, it displays primary for all devices in the stack.

Workaround: Refer to the WebView, Physical > Chassis Management > Stack > Topology page.

PR 90425

In WebView, on the Physical > Health > Slice Statistics page, after using the button **Clear Statistics**, it may not show all information (accessing the table too soon).

Workaround: Refresh the page and the data should show as expected.

PR 90431

Modify Permanent ARP Entry doesn't change the Slot/Port & Name of the existing entry.

Workaround: Delete the entry and create another permanent ARP entry with a changed slot/port and name.

PR 90439

In WebView, Networking > IP > OSPF > Interfaces page, the priority shown is not correct.

Workaround: Use the modify page to see the correct priority value.

PR 90822

WebView Spanning Tree 1x1 (802.ID & 802.1W) bridge priority modify cannot be changed to a custom number. It allows only multiples of 4096.

Workaround: Use the switch CLI as a work-around.

Layer 2

Autonegotiation

Problem Reports

PR 86826

When autonegotiation is disabled and the speed is forced to 10Mbps, the OS6800 copper port may get confused with a forced 100Mbps link partner and can detect a false link UP. Traffic may not pass in this condition.

Workaround: Enable autonegotiation for this copper port and configure the desired speed and duplex settings.

Bridging

Problem Reports

PR 86261

Ethernet SNAP packets with non-zero OUI will not be classified using the port-protocol rule.

Workaround: If applicable, other rules should be used to classify such packets.

PR 86472

With IP and IPX network address rules, the same MAC address cannot be in two different VLANs.

Workaround: Use protocol rules.

PR 86904

Mobile classification is not working after the default VLAN is changed to mobile VLAN.

Workaround: Toggle the link state.

PR 86905

When the MAC-VLAN table limit is exceeded, an SNMP trap is generated indicating this. No console message is generated.

Workaround: Monitor traps in addition to console logs.

PR 87167

Sometimes the default flood rate appears in the boot.cfg.

Workaround: There is no known workaround at this time.

PR 87543

The trap is not generated when the binding rule violation occurs.

Workaround: There is no known workaround at this time.

PR 90391

When doing an ***snmpget***, qAggregateVlanDescription object returns extra characters.

Workaround: There is no known workaround at this time.

PR 90767

Sometimes Infineon fiber SFPs cause autonegotiation to fail on the OS6800-U24 and the link may not come UP even if the remote end is connected.

Workaround: Unplug the fiber cable from the OS6800-U24 port and plug it back in to bring the link UP.

Ethernet Interfaces

Problem Reports

PR 86997

The OS6800 counts all non-standard size (more than 1518/1522 bytes) packets as InError packets though the OS6800 passes these over sized packets/frames as per max frame size configurations.

Workaround: There is no known workaround at this time.

PR 87081

SNMP walk fails for the IFMau table.

Workaround: There is no known workaround at this time.

PR 87480

Packets dropped can be observed in a stacking configuration.

Workaround: There is no known workaround at this time.

PR 89004

The **show interfacea slot/port accounting** for the OS6800 10Gigabit port may not display correct values if:

1. Packet sizes are between 1024 and 2047

2. Packets are Oversized packets.

Workaround: There is no known workaround at this time.

PR 90220

The OS6800 10Gigabit fiber ports currently support only 10Gigabit speed and full duplex mode.

Workaround: There is no known workaround at this time.

Flow Control

Problem Reports

PR 84367

Presently flow control is not supported on the OS6800.

Workaround: There is no known workaround at this time.

Health Monitor/Management

Problem Reports

PR 85589

In some cases, the bandwidth used for port health computations may be higher than the actual bandwidth.

Workaround: There is no known workaround at this time.

Interswitch Protocols (AMAP)

Problem Reports

PR 70128

AMAP currently works on the default VLAN for tagged ports only. So, if the default VLAN is disabled, AMAP will not work.

Workaround: When using AMAP, make sure that the default VLAN is not disabled.

PR 85640

AMAP traps are not generated when a port transitions from any of the three phases - namely discover, common, and passive. A trap is generated when a link is added or removed.

Workaround: There is no known workaround at this time.

PR 86576/87822

The AMAP Adjacencies Remote Host Device field value sometimes shows **ERR("12")** or **ERR("204")**.

Workaround: There is no known workaround at this time.

IP Multicast Switching (IPMS)

Problem Reports

PR 83765

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

Workaround: There is no known workaround at this time.

PR 84009

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

Workaround: Configure an interface as IGMPv1 through SNMP.

PR 87853

While a multicast stream is being served to a mobile client on port 'p', if either VLAN 'v', different from the mobile VLAN, is configured as the default on that port, or a takeover happens, then the multicast stream will be tagged thereafter.

Workaround: Reconfigure the port's mobility.

```
cli> vlan no port mobile 'p'

cli> vlan port mobile 'p'.
```

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 73953

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

Workaround: There is no known workaround at this time.

PR 90169

Learn Port Security and 802.1x are not compatible on a given port. These 2 features cannot be used on the same port.

Workaround: There is no known workaround at this time.

Link Aggregation

Problem Reports

PR 87824

Dynamic Link Aggregation waits more than the standard time to report remote link synchronization failure.

Workaround: There is no known workaround at this time.

Port Mirroring/Monitoring

Problem Reports

PR 85818

When a stack element is hotswapped with a different module type, and the new module does NOT have the same configuration, the system makes the new module reboot with the synchronized configuration. At this time, the chassis supervision does not show it as a different type of NI, and thus mirror configuration is not deleted as it should be in case of an unlike NI hotswap.

Workaround: Assuming you have a stack of 5, and your intention is to replace slot 5, the first part of the procedure should be to bring the element to the same level of code by inserting the new element in the slot without it being slot 5. Once the new element has been synchronized, the user can reconfigure the slot to be 5 at the next boot up. At this time, the user can remove the old slot 5 and the new element, and restart the new element.

PR 85997

The mirror sessions in boot.cfg are visible in the **show** command even if the ports are not active, or the NI is not present. Once the NI and ports are UP, the session resumes.

Workaround: There is no known workaround at this time.

PR 86338

The system preserves the INGRESS tag format of the packet for EGRESS mirroring also, which makes the mirror packet go out tagged though the real egress packet is not tagged.

Workaround: There is no known workaround at this time.

PR 87173

In case of mirroring multicast routed packets, mirror packets will have the source address as the original source's MAC address instead of the router MAC address.

Workaround: There is no known workaround at this time.

PR 89745

For port monitoring, no trap information is sent when the file size is exceeded on the OS6800.

Workaround: There is no known workaround at this time.

PR 90127

With Mirroring/Monitoring enabled on multiple ports, and the same traffic is passing through these ports, only one copy of the traffic is mirrored/monitored, whichever happens first. This is an ASIC limitation.

Workaround: There is no known workaround at this time.

PR 90257

The captured monitoring frames display the original MAC address instead of the router MAC address in case of IPMS routed packets

Workaround: There is no known workaround at this time. This is a hardware limitation.

Source Learning

Problem Reports

PR 81746

Per VLAN aging is not supported.

Workaround: There is no known workaround at this time.

PR 82177

The delonreset (Delete on Reset) and delontimeout (Delete on Timeout) MAC address types are not supported in this release.

Workaround: There is no known workaround at this time.

PR 83087

The MAC aging time can take up to twice the configured value.

Workaround: There is no known workaround at this time.

PR 86448

The **show mac-address-table** protocol column displays 1+ethertype for AOS. On the OS6800, it shows just the Ethertype. Example: IP protocol is displayed as 10800 for AOS and 800 for the OS6800.

Workaround: There is no known workaround at this time.

PR 87846

The CLI might not respond for 10 to 12 seconds after flushing a large number of MAC addresses (over 8k).

Workaround: There is no known workaround at this time.

PR 87997

When a large number of MAC addresses (over 8k) are learned over an aggregate, and the aging time is set to 60 secs, the CPU utilization stays high.

Workaround: Set the aging time to a higher number.

PR 88691

The system cannot tell which port the MAC is learned from, and therefore, no notification is sent to the CPU once the entry is already in the L2 Table.

Workaround: There is no known workaround at this time.

PR 90807

Sometimes the ARP Table is not cleared or updated when the LinkAgg port is removed and re-connected. This will cause a temporary outage for connection to the switch, but at the most for 5 minutes.

Workaround: Clear the ARP entries.

PR 90809

MAC addresses get learned on slot/port 0/0 for a few seconds over an aggregate after takeover.

Workaround: There is no known workaround at this time.

PR 91841

During the Spanning Tree topology change period, the switches respond time is slow and no MAC address is learned.

Workaround: The system will resume to normal after the Spanning Tree topology change period is over.

Spanning Tree

Problem Reports

PR 87964

The aggregation up message was not received by the Spanning Tree Protocol when the CPU utilization of the switch was high, causing STP state machines not to be in a proper state.

Workaround: Disabling and enabling link aggregation corrects the problem.

PR 89316

Every link-up, we send out a BPDU packet with the Root BridgeID of 0xffff... to elicit a BPDU reply from the adjacent switch in the current Auto-Edge Detection mechanism.

Workaround: Set the stpni_useWorstRootBridgeID=0 in NiDbg, then disable/re-enable the STP instance.

PR 90514

After a takeover, if the OS6800 in a stack that has a root port for a MSTI instance is rebooted, a port in the other OS6800 will become a new root port for that MSTI instance. However, when the OS6800 with the original root port comes backup, Spanning still shows two root ports for the same MSTI instance that could cause network instability.

Workaround: Reboot the OS6800 with the legitimate root port one more time.

VLANs

Problem Reports

PR 88028

If the SNAP header contains "non-zero OUI", the ASIC does not recognize the SNAP frame.

Workaround: Please use the default VLAN or a different mobile rule.

Layer 3

Basic IP Routing

Problem Reports

PR 85432

The following message might be seen when learning the source MAC-addresses of a routed packet, or a packet to the Switch.

"Exceeded Maximum Source Learning Attempts using ARPs for ...."

For a routed packet, or a packet to the Switch, the switch cannot directly learn the MAC-address.

The switch has to send an ARP request to the source IP of that packet, if directly connected, or to the gateway to reach the Source if not directly connected, and wait for an ARP reply in order to learn the MAC-address.

If the ARP reply is not received within 10 seconds, the message will be displayed.

The IP address in the message indicates which host the Switch is sending an ARP Request for.

Workaround: There is no known workaround at this time.

PR 85885

From a routed packet, or a packet to the Switch, the switch cannot directly learn the MAC-address of the source. The switch has to send an ARP request to the source IP of that packet, if directly connected, or to the gateway to reach the Source, if not directly connected, and wait for an ARP reply in order to learn the MAC-address. This will be the behavior even if the switch already has the corresponding ARP entry, static or dynamic.

Workaround: 1. Configure a static L2 entry for the source. 2. Make the source originate some L2, ARP or multicast traffic which would cause its MAC address to be learned on the Switch.

PR 87372

Network-Prefix Directed Broadcasts are received by the switch by default.

Workaround: There is no known workaround at this time.

PR 89961

When a switch boots without boot.cfg, and a user does **write memory**, the created boot.cfg will have garbage in the IP service section.

Workaround: Type **ip service all** before **write memory**, or boot with a boot.cfg, which contains **ip service all**.

PR 90601

The static route stays active when the gateway is not reachable, but the interface is still UP.

The traffic will still be routed towards the unreachable gateway.

Workaround: There is no known workaround at this time.

PR 90636

The OS6800 could see 1/24 port changed to a 1/-1 port when we execute a **show arp** command.

Workaround: There is no known workaround at this time.

IPX Routing

Problem Reports

PR 89934

There are occasions when SAP entries may not be deleted when the referring network goes away. As long as the SAP broadcasts continue for that SAP, the SAP entry will remain in the database.

Workaround: If the network for the SAP entry is unreachable, a flush of the SAP table will remove the entry. It will not be relearned until the network is available again.

PR 90480

The IPX network rule does not classify raw IPX (novell) packets.

Workaround: The IPX protocol rule classifies raw IPX (novell) packets based on protocol. Based on the customer's needs, this rule can be used.

UDP Relay

Problem Reports

PR 67896

The SNMP agent returns values from **iphelperVlan** with an invalid SNMP data type.

Workaround: There is no known workaround at this time.

PR 88759

In per-vlan mode, the user is able to configure the DHCP server IP address without entering the VLAN number that is associated with the IP address.

Workaround: There is no known workaround at this time. The user needs to double check the configuration. AOS will not be able to perform the validation if the VLAN ID is also entered.

VRRP

Problem Reports

PR 87501

When a VLAN is configured without an IP router address, the operational state of a VRRP tracking policy for that VLAN may be out of sync with the VLAN's operational state. Since tracking policies exist for the purpose of routed traffic this should not pose a problem.

Workaround: There is no known workaround at this time.

PR 87566

When using a remote IP address VRRP tracking policy, the switch polls the IP address every 10 seconds. This means it can take up to 10 seconds to detect a change in the reachability of the remote ip address and change the VRRP instance priority. Therefore, in the event the remote IP address becomes unreachable, VRRP may not failover immediately. There is currently no CLI to change the poll interval for the IP.

Workaround: There is no known workaround at this time.

Quality of Service (includes ACLs and NAT)

Policy Manager

Problem Reports

PR 81620

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

Workaround: Remove QoS policies before deleting the LDAP server.

PR 90036

If the user does a **qos flush**, the statistics displayed by **show qos port statistics** displays the on-boot statistics. Now, if the user does a **qos revert**, the statistics are not reverted to its pre-flush values.

Workaround: In order to correctly display the statistics after a **qos revert**, the user should re-apply the QoS policies.

Advanced Routing

DVMRP

Problem Reports

PR 87831

If VLAN 'v' is configured as the default VLAN on port 'p', and then is removed from port 'p' when VLAN '1' is disabled, and then 'v' is configured as 802.1q on 'p', then multicast traffic belonging to 'v' and egressing on 'p' will egress untagged.

Workaround: Enable VLAN '1' or configure an active VLAN as the default on 'p'.

OSPF

Problem Reports

PR 81856

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 90742

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 85256

Per the PIM BSR Specification, the bootstrap message must be sent to the ALL-PIM-ROUTERS group by the correct upstream router towards the BSR. If not, the bootstrap message must be dropped. If you are using static-routes, then the static-route must be set to the correct upstream router towards the BSR; otherwise the bootstrap router will not be set correctly.

Workaround: Set the static-route to the correct upstream router towards the BSR.

PR 90544

Pimsm configurations causing (S,G,rpt) prunes and Assert processing to occur simultaneously on an interface may cause flow disruption.

Workaround: Configure the DR's to be on the same switch as the RP avoiding any assert processing or (S,G,rpt) prunes.

Security

Feature Exceptions

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

802.1X

Problem Reports

PR 87329

When the direction is set to both, packets from all other Ethernet ports are blocked from flooding out of an 802.1x port. However, traffic that originates from the CMM is not blocked from flooding out of an 802.1x port even though the direction parameter is set to BOTH.

Workaround: There is no known workaround at this time.

PR 88027

The **show 802.1x** cmd may not display the PAE and backend authenticator state attributes for a particular port after a few takeovers. This is a display issue only and has no adverse effects on the feature itself.

Workaround: There is no known workaround at this time.

PR 90043

With a lot of clients authenticated on a single port, **show 802.1x** users may not display all the clients.

Workaround: There is no known workaround at this time.

PR 90169

Learn Port Security and 802.1x are not compatible on a given port. These 2 features cannot be used on the same port.

Workaround: There is no known workaround at this time.

PR 90812

"onex" task crashes on the new primary after takeover, with ports being config. for reauthentication.

Workaround: Set the reauthentication timer to be anything equal or greater than 300 seconds.

PR 90855

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

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

System

Chassis Supervision

Problem Reports

PR 90033

On a stack of eight OS6800 switches commands **show ni <num>** and **show module long** do not show complete GBIC information if issued after a takeover. GBICs on some stacks may not be shown.

Workaround: There is no known workaround at this time.

PR 90291

Flash Synchro status may be visible to the telnet session.

From the Telnet session, the user may start a Flash Synchro process. Unlike the console, the status of the flash synchro may be displayed.

Workaround: Allow enough time for the Flash Synchro to complete. For example, if 8 stacks, please allow 20 - 25 minutes.

PR 90437

On the OS6800-U24 (Fiber) switch commands **show ni <num>** and **show module long** do not show GBICs in ports 5-24.

Workaround: There is no known workaround at this time.

General

Problem Reports

PR 83497

The Alcatel NTP implementation will not accept a time update from an SNTP server. It appears in the notes for the MSNTP distribution that it is not recommended to be run in server mode. The most serious problem observed is that it sends NTP messages indicating that the local clock has never been synchronized. The default for our NTP implementation is to reject such servers.

Workaround: There is no known workaround at this time.

PR 83759

NTP prefer setting does not force synchronization with the selected 'preferred' NTP server.

Workaround: The 'prefer' argument is not well understood. It is a bit of a misnomer. A preferred server will be chosen for synchronization if it first is among the set of peers that survives sanity checks and normal clock selection procedures. From this set of peers, it would appear that they are all essentially the same statistical quality. The phrase used by ntp.org to describe this vetting is "all things being equal". If a 'preferred' server does not survive the clock selection procedures, it will never become the synchronization peer. Please refer to a more thorough discussion of this variable in the link below:

http://www.eecis.udel.edu/~mills/ntp/html/prefer.html

PR 84375

NTP synchronization with broadcast mode NTP servers is not available on the OS6800 platform.

Workaround: Use Unicast client. It is more accurate.

PR 84841

Broadcast mode is not available on the OS6800 platform.

Workaround: Use NTP in client mode.

PR 86061

A zmodem high CRC error rate is encountered when downloaded at a speed of 115200.

Workaround: The CRC rate varies depending on the line condition. Use a 38400 speed to reduce the CRC rate.

PR 86088

Multiple changes to the system timezone can cause a crash.

Workaround: Do not make unnecessary multiple changes to the system timezone.

PR 87148

The **show microcode** command is only relevant to the version of software present at bootup time.

Workaround: Once new software is installed, run install the CLI command to update this information.

PR 89110

When users enter a system location name with a length of 255, the system reports an exception.

Workaround: Enter a system location name less than 255 in length as specified in the CLI user manual.

Port Manager

Problem Reports

PR 90100

The debug message "PORT-MGR info pm:unknown message from socket 41:0:6:4" might appear at bootup.

Workaround: There is no known workaround at this time.

Stack Manager

Problem Reports

PR 90744

The **Reload all** command does not work on the OS6800-U24 (non-stackable 24-port Fiber).

Workaround: Use the **reload** command instead.

Redundancy / Hot Swap

CMM Redundancy

Problem Reports

PR 87228

After takeover, the switch might not show the complete list of MAC addresses learned.

Workaround: Flush the MAC addresses and learn them again.

PR 87346

On the OS6800, on takeover, if one ECMP route is lost (because of part of the primary unit that is rebooting), the ECMP route remains active for one minute. Traffic originally routed over that path will be dropped for that minute before switching to another ECMP path. That delay is needed because the new primary unit needs some time to enable all VLAN interfaces to come up after takeover.

Workaround: On a simple OSPF setup that does not have Link Aggregation, or has Spanning Tree disabled for the VLANs on which the ECMP gateways exist, the delay can be reduced.

PR 87816

With a large configuration file, following takeover, a stacking setup may lose its primary unit. In most cases, it recovers after about two minutes. Occasionally, the two secondaries remain; there should only be one.

Workaround: Reload the stack.

PR 87936

After takeover, the AVLAN users might be logged out and will need to re-authenticate.

Workaround: There is no known workaround at this time.

PR 87950

When a takeover happens with a configuration of 1024 policy rules/ACLs, the former primary stack that is rebooting might not come up properly.

In that event, the old primary stack stays in an "init" state, and all ports are down even though **show module status** shows the NI is up.

Workaround: From the CLI, reload that unit again with **reload ni slot-number**.

PR 87966

Upon takeover, certain error messages might appear on the console.

Workaround: There is no known workaround at this time.

PR 88033

On a takeover, the GRDROP counts for Layer 3 frames might go up.

Workaround: There is no known workaround at this time.

PR 90265

If the port is not connected (or not linked up), any change in the default ifg configuration can be lost by the switch on takeover. After takeover, all ports where links were not UP, will show ifg config as 0 and will pick up the default ifg configuration when links are made up.

Workaround: Change the Interface ifg configuration only if the port is connected or the link is UP. If the ifg configuration is changed (other than switch default), while the port link was not UP, the ifg needs to be reconfigured after the takeover.

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.