Release Notes

OmniStack 6200

Software Version 1.0.2.45 / Boot Version 1.0.0.11

These release notes accompany release 1.0.2.45 software and 1.0.0.11 boot version for the OmniStack 6200 family hardware. They provide important information on individual software features and hardware modules. Since much of the information in these release notes is not included in the hardware and software user manuals, it is important that you read all sections of this document before installing new hardware or loading new software.

Note: References to OmniStack 6200 family hardware include model numbers: OS-LS-6212, OS-LS-6212P, OS-LS-6224, OS-LS-6248, OS-LS-6224U, OS-LS-6224P and OS-LS-6248P. Where an item is unique to a specific platform, its model number is used.

Contents

Related Documentation

These Release Notes should be used in conjunction with the OmniStack 6200. The following are the titles and descriptions of the OmniStack 6200 family documentation.

OmniStack 6200 Family Getting Started Guide

Describes the hardware and software procedures for getting an OmniStack 6200 Family switch up and running.

OmniStack 6200 Family User Guide

Includes detailed description of the OmniStack 6200 Family switches, and directions on how to manage them. Topics include system overview, system configuration, device specifications, using WebView to manage the device, and using CLI to manage the device.

System Requirements

Memory Requirements

OmniStack 6200 Release 1.0.2.45 requires 128 MB of SDRAM. This is the standard configuration shipped on all 6200 platforms.

Configuration files and the compressed software images—including web management software (WebView) images—are stored in flash memory. During the boot process, you will see the SDRAM and flash memory size.

Power Supply Requirements

The OS6200 platforms are all equipped with an internal power supply, capable of providing power to the platform. The OS-LS-6212P, OS-LS-6224P and OS-LS-6248P are Power over Ethernet enabled devices, with different power consumption requirements.

Note: It is recommended to use an external Redundant Power Supply when deploying an OS-LS-6224P or OS-LS-6248P, so that Powered Devices connected to the platform are assured enough power. For more information, refer to the *OmniStack 6200 Family Getting Started Guide* and *OmniStack 6200 Family User Guide*.

Upgrading Software Versions

Instructions for upgrading image files and boot files are available in the *OmniStack 6200 User Guide*, and on the Customer Support website along with the most recent software version (http://eservice.ind.alcatel.com).

Merging OS6200 Stacks

You cannot merge two OS6200 stacks unless they are running identical versions of software. Alcatel recommends the following steps to merge two separate stacks:

Upgrade one or both (if necessary) stacks so they are running the same software.

Confirm that both stacks are running the same software with the **show versions** Privileged Exec command.

Connect the two stacks together into one stack. Refer to *OmniStack 6200 Family Getting Started Guide* for cabling guidelines.

Use the **show stack** command to confirm that the stacks have been successfully merged.

New Hardware Supported

This software release adds support for the OS-LS-6212, OS-LS-6212P and OS-LS-6224U models of the OmniStack 6200 family.

New/Modified Software Supported

This version introduces the functionality of loading the PoE software from the flash onto the PoE controller would be executed automatically by the software. During the initiation of the system, whenever differences would be encountered between the software on the flash and the software loaded on the controller then the software from the flash will be loaded on the MCU with no user intervention.

New/Modified CLI Commands Supported

Note: None were added in the latest versions since 1.0.1.23.

The following CLI commands are modified or newly introduced for Version 1.0.1.23. All CLI commands are described in the CLI Reference Guide.

CLI Command	Modification Description
spanning-tree bpdu	The new parameter "bridging" is added, to specify that when STP is disabled globally, tagged and untagged BPDU packets are flooded, according to their VLAN id.
switchport mode	The new parameter "customer" is added, to specify that the port is connected to customer equipment. This configuration is applicable when the device is in a provider network. This command is used for Triple Play configuration (Multicast TV VLAN).

CLI Command	Description of Functionality
switchport customer vlan	This new command is used to set the port's VLAN when the interface is in customer mode.
switchport customer multicast-tv vlan	This new command is used to configure ports to be capable of receiving multicast transmissions from a VLAN that is not the customer port's VLAN, while maintaining the Layer 2 segregation from subscribers on different customer port VLANs.
ip igmp snooping map cpe vlan	This new command is used to map CPE VLANs to Multicast TV Vlans
show ip igmp snooping cpe vlans	This new command is used to display the CPE VLANs to Multicast TV VLANs mappings.

Feature Summary

Feature	Platform
Power over Ethernet	0S-LS-6212P/24P/48P
Head of Line Blocking	all
Flow Control (IEEE 802.3x)	all
Back Pressure	all
Virtual Cable Testing (VCT)	all
MDI/MDIX	all
Auto-Negotiation	all
Static MAC Address	all
Self-Learning (Dynamic) MAC Addresses	all
Automatic Aging	all
VLAN-Aware MAC Based Switching	all
MAC Multicast Support	all
IGMP Snooping	all
Port Mirroring	all
Broadcast Storm Control	all
VLAN Support	all
802.1Q VLAN Tagging	all
Protocol Based VLAN	all
MAC-Based VLAN	all
IP-Subnet Based VLAN	all
GVRP	all
Q-in-Q	all
Multicast TV VLAN	all
Triple Play - Multicast TV VLAN	all
Spanning Tree	all
Spanning Tree Fast Link	all
Rapid Spanning Tree	all
Multiple Spanning Tree	all
Link Aggregation and LACP	all
Class of Service 802.1p	all
Quality of Service Basic Mode	all
Quality of Service Advanced Mode	all
BootP and DHCP Clients	all
SNMP Versions 1,2, and 3	all
Web-Based Management	all
Configuration File Upload and Download	all
TFTP Transfer Protocol	all
Remote Monitoring	all

Feature	Platform
Command Line Interface	all
Syslog	all
Simple Network Time Protocol	all
Domain Name System	all
Traceroute	all
AMAP	all
SSL	all
SSH	all
Port Based Authentication (802.1x)	all
RADIUS Client	all
Port Security Support	all
TACACS+	all
Password Management	all

Feature Descriptions

General Features

Power over Ethernet

Power over Ethernet (PoE) provides power to devices over existing LAN cabling, without updating or modifying the network infrastructure. Power over Ethernet removes the necessity of placing network devices next to power sources. Power over Ethernet can be used in the following applications:

- IP Phones
- Wireless Access Points
- IP Gateways
- PDAs
- Audio and video remote monitoring

Head of Line Blocking Prevention

Head of Line (HOL) blocking results in traffic delays and frame loss caused by traffic competing for the same egress port resources. HOL blocking queues packets so that the packets at the head of the queue are discarded before packets at the end of the queue. HOL Blocking Prevention avoids this situation. The device is configured so that this mechanism is always active, except when QoS, Flow Control or Back Pressure is enabled on an interface.

Flow Control Support (IEEE 802.3X)

On full-duplex links, flow control enables lower speed devices to communicate with higher speed devices, without having to drop frames when buffers are too full. This is done by requesting that the higher speed device refrains from sending packets. Transmissions are temporarily halted to prevent buffer overflows.

Back Pressure Support

On half-duplex links, the receiving port prevents buffer overflows by occupying the link so that it is unavailable for additional traffic.

Note: Back Pressure and Flow Control cannot work together on the same interface.

Mini Jumbo Frames

Support of mini jumbo frames allows forwarding of packets up to 1632 bytes.

Virtual Cable Testing (VCT)

VCT detects and reports copper link cabling faults, such as open cables and cable shorts.

MDI/MDIX Support

The device automatically detects whether the cable connected to an RJ-45 port is crossed or straight through and adapts the internal wiring of the interface so as to create a working connection. Standard wiring for end stations is Media-Dependent Interface (MDI) and the standard wiring for hubs and switches is known as Media-Dependent Interface with Crossover (MDIX).

Auto Negotiation

Auto negotiation allows the device to advertise modes of operation. The auto negotiation function provides the means to exchange information between two devices that share a point-to-point link segment, and to automatically configure both devices to take maximum advantage of their transmission capabilities.

Auto-negotiation advertisement is supported. Port advertisement allows the system administrator to configure the port speed and duplex advertisement.

Spanning Tree Protocol Features

Spanning Tree Protocol (STP)

802.1d Spanning tree is a standard Layer 2 switch requirement that allows bridges to automatically prevent and resolve L2 forwarding loops. Switches exchange configuration messages using specifically formatted frames and selectively enable and disable forwarding on ports.

Spanning Tree BPDU Mode

BPDU Mode can be set to allow BPDU packets to be flooded, filtered or bridged when STP is disabled.

Fast Link

STP can take up to 30 seconds to converge. During this time, STP detects possible loops, allowing time for status changes to propagate and for relevant devices to respond. 30-60 seconds is considered too long of a response time for many applications. The Fast Link option bypasses this delay, and can be used in network topologies where forwarding loops do not occur.

IEEE 802.1w Rapid Spanning Tree

Spanning Tree can take 30 seconds for a device to decide which ports are actively forwarding traffic. Rapid Spanning Tree (RSTP) detects network topologies to allow for faster convergence without creating forwarding loops.

IEEE 802.1s Multiple Spanning Tree

Multiple Spanning Tree (MSTP) operation maps VLANs into STP instances. MSTP provides differing load balancing scenario. Traffic assigned to various VLANs is transmitted along different paths within MSTP Regions (MST Regions). Regions are one or more MSTP bridges by which frames can be transmitted.

Link Aggregation

Link Aggregation

Up to eight Aggregated Links may be defined, each with up to eight member ports, to form a single Link Aggregated Group (LAG). This enables:

- Fault tolerance protection from physical link disruption
- Higher bandwidth connections
- Improved bandwidth granularity

A LAG is composed of ports operating at the same speed and at full-duplex.

Link Aggregation and LACP

Link Aggregation Control Protocol (LACP) uses peer exchanges across links to determine, on an ongoing basis, the aggregation capability of various links, and continuously provides the maximum level of aggregation capability achievable between a given pair of systems. LACP automatically determines, configures and binds.

VLAN Supported Features

VLANs are collections of switching ports that comprise a single broadcast domain. Packets are classified as belonging to a VLAN based on either the VLAN tag or a combination of the ingress port and packet contents. Packets sharing common attributes can be grouped in the same VLAN.

Port-Based VLANs

Port-based VLANs classify incoming packets to VLANs based on their ingress port.

IEEE802.1V Protocol Based VLANs

VLAN classification rules are defined on data-link layer (Layer 2) protocol identification. Protocol-based VLANs are used for isolating Layer 2 traffic for differing Layer 3 protocols.

Full 802.1Q VLAN Tagging Compliance

IEEE 802.1Q defines an architecture for virtual bridged LANs, the services provided in VLANs, and the protocols and algorithms involved in the provision of these services.

GVRP Support

GARP VLAN Registration Protocol (GVRP) provides IEEE 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q VLAN tagged ports. When GVRP is enabled, the switch registers and propagates VLAN membership.

IP Subnet-Based VLAN

IP-Subnet based VLAN classification allows packets to be classified according to the packet's source IP subnet in its IP header. This allows for multiple IP subnets to exist on a single port, and for the untagged packets to be assigned to the proper VLAN.

MAC-Based VLAN

MAC-Based VLAN classification allows packets to be classified according to the packet's source MAC address.

Multicast TV VLAN

The Multicast TV VLAN feature provides the ability to supply multicast transmissions to Layer 2-isolated subscribers without replicating the multicast transmissions for each subscriber VLAN. The subscribers are receivers only for the multicast transmissions. Provider VLANs can be defined per port.

Q-in-Q

Encapsulating IEEE802.1Q VLAN tags within an additional 802.1Q enables service providers to use a single Provider VLAN to support customers who have multiple internal VLANs. The Q-in-Q VLAN Tag Termination feature on the sub-interface level preserves VLAN IDs and segregates between traffic in different customer VLANs.

Quality of Service Features

Class of Service 802.1p Support

The IEEE 802.1p signaling technique is an OSI Layer 2 standard for marking and prioritizing network traffic at the data link/MAC sub-layer. 802.1p traffic is classified and sent to the destination. No bandwidth reservations or limits are established or enforced. 802.1p is a spin-off of the 802.1Q (VLANs) standard. 802.1p establishes eight levels of priority, similar to the IP Precedence IP Header bit-field.

Quality of Service Support

To overcome unpredictable network traffic and optimize performance, Quality of Service (QoS) can be enforced throughout the network to ensure that network traffic is prioritized according to specific criteria. The switch supports two modes of QoS: basic and advanced.

Quality of Service Basic Mode

In basic QoS mode, it is possible to activate a trust mode. In addition, a single access control list can be attached to one or more interfaces.

Quality of Service Advanced Mode

Advanced Quality of Service mode specifies flow classification and assigns rule actions that relate to bandwidth management. These rules are grouped into a policy, which can be applied to an interface.

Device Management Features

BootP and DHCP Clients

BootP enables initial setup parameters to be received from a network server upon system startup. DHCP service is an on-going process. DHCP is an extension to BootP.

SNMP Alarms and Trap Logs

The system logs events with severity codes and timestamps. Events are sent as SNMP traps to a Trap Recipient List.

SNMP Versions 1, 2 and 3

Simple Network Management Protocol (SNMP) over the UDP/IP protocol controls access to the switch. A list of community entries is defined, each of which consists of a community string and its access privileges. There are 3 levels of SNMP security, they are read-only, read-write and super user. Only a super user can access the community table.

Web Based Management

With web based management, the system can be managed from many web browser platforms. Refer to User Guide for more information. The system contains an Embedded Web Server (EWS), which serves HTML pages through which the system can be monitored and configured. The system internally converts web-based input into configuration commands, MIB variable settings and other management-related settings.

Configuration File

The device configuration is stored in a configuration file. The Configuration file includes both system wide and port specific device configuration. The system can display configuration files in the form of a collection of CLI commands, which are stored and manipulated as text files.

TFTP Trivial File Transfer Protocol

The device supports boot image, software and configuration upload/download via TFTP.

Remote Monitoring

Remote Monitoring (RMON) provides comprehensive network traffic monitoring capabilities (as opposed to SNMP which allows network device management and monitoring). RMON is a standard MIB that defines current and historical MAC-layer statistics and control objects allowing real-time information to be captured across the entire network.

Command Line Interface

Command Line Interface (CLI) syntax and semantics conform as much as possible to common industry practice. CLI is composed of mandatory and optional elements. The CLI interpreter provides command help guidance in addition to command and keyword completion to assist user and shorten typing.

Syslog

Syslog is a protocol that enables event notifications to be sent to a set of remote servers where they can be stored, examined and acted upon. The system sends notifications of significant events in real time and keeps a record of these events for after-the-fact usage.

SNTP Client

The Simple Network Time Protocol (SNTP) assures accurate network Ethernet Switch clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server.The device supports SNTP client, so that the time can be received from an SNTP server.

Domain Name System

Domain Name System (DNS) converts user-defined domain names into IP addresses. Each time a domain name is assigned the DNS service translates the hostname into a numeric IP address. For example, www.ipexample.com is translated to 192.87.56.2. DNS servers maintain domain name databases and their corresponding IP addresses. The device supports a DNS client.

Traceroute

Traceroute discovers IP routes that packets were forwarded along during the forwarding process. The CLI Traceroute utility can be executed from either the user-exec or privileged modes.

AMAP

The AMAP protocol enables a switch to discover the topology of other AMAP-aware devices in the network. The protocol allows each switch to determine if other AMAP-aware switches are adjacent to it.

Security Features

SSL

Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data through privacy, authentication, and data integrity. It relies upon certificates and public and private keys.

Port Based Authentication (802.1x)

Port based authentication allows for authenticating system users on a per-port basis via an external server. Only authenticated and approved system users can transmit and receive data. Ports are authenticated via the Remote Authentication Dial-In User Service (RADIUS) server using the Extensible Authentication Protocol (EAP).

Port Security Support

Port Security increases network security by limiting access on a specific port only to users with specific MAC addresses. These addresses are either manually defined or learned on that port. When a frame is seen on a locked port, and the frame source MAC address is not tied to that port, the protection mechanism is invoked.

RADIUS Client

RADIUS is a client/server-based protocol. A RADIUS server maintains a user database, which contains per-user authentication information, such as user name, password and accounting information.

SSH

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH version 2 is currently supported. The SSH server feature enables an SSH client to establish a secure, encrypted connection with a device. This connection provides functionality that is similar to an inbound telnet connection. SSH uses RSA and DSA Public Key cryptography for device connections and authentication.

TACACS+

TACACS+ provides centralized security for validation of users accessing the device. TACACS+ provides a centralized user management system.

Password Management

Password management provides increased network security and improved password control. Passwords for CLI, SSH, Telnet, HTTP, HTTPS, and SNMP access are assigned security features.

Unsupported CLI Commands

The following CLI commands are not supported or have the noted non-supported functionality in this release of the software:

Software Feature	Unsupported CLI Commands
Unit ID Number Modification from Software	stack change unit-id

CLI Command	Lacking Functionality
show qos map	The help is incorrect for this command.
show policy map	After executing the command with a class name that exists in the system, the device also shows other policies that exist in the system.

Fixed Problem Reports

Problems Fixed for Version 1.0.2.45

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

Layer 2

Problem Reports

PR 87026

After adding around 180 VLAN to Multi Spanning Tress instances, the 6200 switch crashes and reboots with fatal error messages.

Status: This issue is fixed.

PR 87455

The following error message was reported during AMAP handshaking process:
AMAP-E-DB_OVERFLOW_FAIL: IP ADDR: Database, overflow.

Status: This issue is fixed.

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

Feature Exceptions

- Ten management sessions can be simultaneously opened on the device per the following types: 1 Console connection, 5 Telnet/SSH sessions, 4 HTTP/HTTPS sessions.
- Default console connection baud rate is 9600.
- Running configuration files and startup configuration files are managed in the Master Unit. These files are always synchronized between the Master Unit and the Backup Master Unit. However, the backup configuration file is saved only on the Master Unit, and is not synchronized with the Backup Unit.

XModem Download

Problem Reports

PR AL009 / 44202

Downloading a new software image using XModem may result in faulty behavior.

Workaround: Use the Web-based Interface or CLI interface to download a new software image.

Web Based Interface

Feature Exceptions

- A blank field name can be recognized as a name. However, it is recommended not to leave field names blank, as this may interfere with web functionality.

Problem Reports

PR 39065R

When using Netscape or Linux, if a web session is open on a management session, then subsequent opening of another web session on the same management station does not require user authentication as long as the first session is active.

Workaround: There is no known workaround at this time as this is Netscape behavior.

PR 39377R

Web performance may be impacted by heavy usage of the device. For example, web performance may be slowed due to heavy traffic to the CPU, or heavy generation of IGMP packets.

Workaround: There is no known workaround at this time.

PR 41553R

Display of large tables may take a long time to display.

Workaround: If there is a lot of data in a table, it is recommended to use the CLI to display the information.

PR 47499

The Web-Based Interface gets stuck after configuring more than one option on the Layer 2 --> STP --> General Screen.

Workaround: Refresh the screen and reconfigure.

PR 47662

A runtime error results when trying to display dynamic addresses using the Layer 2 --> Dynamic Addresses screen.

Workaround: Use the CLI to display Dynamic Addresses, when there is a large number of addresses.

PR 46987

The idle timeout for login is only 1 minute.

Workaround: There is no known workaround.

Problem Reports

PR 64388

EWS: Fiber ports won't display in the Zoom page

Workaround: Use the CLI interface to achieve this functionality.

Problem Reports

PR 64359

EWS: QOS Advanced; DSCP-DP is missing from the WEB

Workaround: Use the CLI interface to achieve this functionality.

Command Line Interface

Problem Reports

PR 39375

Console history size is not included in the configuration file.

Workaround: There is no known workaround at this time.

PR 47007R

Due to irrelevance to this platform, the CLI command port monitor vlan tagging has been removed from this software version. If this command was inadvertently used in previous version, then loading a configuration file with this command results in failure of copy operation.

Workaround: Prior to downloading the new software image, remove the command from the configuration file, either by negating the command, or by copying the configuration file to a TFTP server and editing the file.

PR 39804D

The timeout for TFTP is set by default to 5 seconds. This time is too short to download a file.

Workaround: Define a longer timeout for the TFTP server.

Problem Reports

PR 66265

When creating an IP address on a stack configuration and changing the "ip internal-usage-vlan" there is a fatal error on unit 2.

Workaround: Use the commands in reverse order in order to make this scenario work.

RMON

Problem Reports

PR 39814R

Oversize and Jabbers counters count only packets above 1632 bytes.

Workaround: There is no known workaround at this time.

PR 39486R

The Alarm Packets with Errors Receive does not function. The counter does not count CRC errors.

Workaround: There is no known workaround at this time.

PR 39868R

Drop events are not accumulated.

Workaround: There is no known workaround at this time.

SNMP

Problem Reports

PR 47342

It is not possible to assign a Remote Engine ID (required for SNMPv3) using the Web Based Interface.

Workaround: Use the CLI command to configure a Remote Engine ID.

SNTP

Problem Reports

PR 58202

Display of time is not working correctly for some time zones.

Workaround: Use the CLI command to view time.

Stacking

Feature Exceptions

- A blank field name can be recognized as a name.
- A single unit in a stack is displayed as a ring topology even if no stacking links are attached. Note that this is actually functional behavior, since the system is configured as a stack with a single unit.
- When ports from the master and backup master dynamically join a LAG (through LACP), and the master unit fails, the ports from the backup master do not become active. This is due to standard LACP behavior. According to the 802.3ad standard, when the PORT_DISABLED state is entered, the port retains the LAG ID parameters. Therefore, only a change of link state triggers a change to the parameters.

Layer 2

Flow Control

Feature Exceptions

Flow control does not operate across the stack.

Flow control does not operate on Gigabit Ethernet ports.

Port Security - 802.1x Single Host Mode

Feature Exceptions

Port security and 802.1x Single Host Mode cannot be enabled simultaneously on the same interface.

Duplex Configuration

Problem Reports

PR 48385R

Per standard, an auto negotiation link should revert to half duplex when connected to a (negotiation disabled) forced full link. This creates a duplex mismatch.

Duplex mismatches should be avoided in ALL network configurations, as they result in traffic degradation, collisions and overall performance issues.

In the Alcatel OS-6200, the duplex mismatch may also cause a port to lock up.

When a duplex mismatch is detected, the user is warned of this potential problem on the given interface with the following message: "*You may need to set interface n to force full duplex and appropriate speed to match partner link configuration.*"

Workaround: It is recommended to avoid configuring a port to auto-negotiation or Half Duplex when the other side is configured to Full Duplex. If the user configures in such a way, the user will be warned of the duplex mismatch upon its detection. The user should then fix the configuration.

Interswitch Protocols (AMAP)

Feature Exceptions

- The AMAP protocol uses the default VLAN (1) on all interconnected ports to communicate with neighbors. The default VLAN on the port(s) must be enabled.
- AMAP only runs on VLAN 1. AMAP does not run on any other VLAN even if an IP address is configured on it. A port that has an IP address configured on it is not a member of the default VLAN and AMAP will therefore not run on this port.

Problem Reports

PR 41521

The AMAP database may be deleted in the following circumstances:

AMAP data change.

Transmission of second cycle of "hello" packets.

Workaround: There is no known workaround at this time.

PR 39222D

There is a problem with sending and understanding the "local virtual port number" and "remote virtual port number" to OmniVista due to an inconsistency between local and remote virtual port numbers.

Status: This issue is fixed so that OmniVista version 2.4.1 recognizes the OS-6200.

Link Aggregation

Feature Exceptions

- Please refer to the Link Aggregation chapters of the OmniStack 6200 User, which includes instructions for configuring LAGs.
- When ports on the master and backup are configured as LACP members of a LAG and the master fails, the LACP protocol stops working. This behavior is per standard but may be unexpected by the user.

For more information, please contact Customer Support via email at support@ind.alcatel.com.

Problem Reports

PR 39528R

When transmitting ARP requests or replies to a channel group, only the second packet is inserted in the ARP table.

Workaround: There is no known workaround at this time.

MAC Address Learning

Feature Exceptions

- The number of MAC addresses supported on an OS6200 series switch is 8K.
- In a stack configuration, few extra MAC addresses of the backup or slave switches are learned.

Spanning Tree

Feature Exceptions

- The default cost of LAGs and GE interface is the same. If the default path cost method is short, these interfaces are assigned a cost of 4. If the default path cost method is long, they are assigned a cost of 20,000.

VLANs

Feature Exceptions

- The number of VLANs on an OS6200 is 255; some VLANs may be reserved for internal usage
- By default, unknown multicast traffic is flooded into the VLAN. However, this stops once at least one member joins. This is expected behavior, but may be undesirable. To avoid this situation, the user can create a multicast group with no members, which causes this specific multicast group not to be flooded. For

example, in order to disable the flooding of group 01:00:5e:01:02:03 on VLAN 1 use the following command:

```
console (config)# interface vlan 1
console(config-if)#bridge multicast address 01:00:5e:01:02:03
```

Multicast

Feature Exceptions

- Q-in-Q IGMP control packets are not double tagged on FE ports.

Problem Reports

PR 48658R

The device does not identify IGMP packets, which are double tagged, as IGMP packets. If a double-tagged IGMP query is sent from a router to a tagged port, the device does not learn the MRouter on the ingress port. If the query is sent with a single tag, the MRouter is learned.

Workaround: Connect querier directly to the provider port. Alternatively, send only single-tagged IGMP packets.

PR 48657R

Client source addresses are not learned in the Address Database when IGMP packets are sent.

Workaround: This does not affect multicast forwarding functionality since the MAC multicast forwarding is not based on the MAC multicast destination, and not the unicast MAC address destination. Further, this is typically a lab scenario. In real networks, the SMAC is learned via other traffic sent by the stations.

Q-in-Q

Feature Exceptions

- Spanning tree must be disabled on customer ports if MSTP is enabled.
- GVRP cannot be enabled on customer ports.
- IP Interface cannot be defined on a customer port or on VLANs that have customer ports as members.
- The size of the packet includes the double tag, so that the actual size of Q-in-Q packet is smaller than 1632 bytes.
- Quality of Service is applied to ingress Q-in-Q customer port single tagged traffic after the provider tag is added. Therefore, the same rules apply to single-tagged traffic incoming to customer ports, as for double-tagged traffic coming in to trunk ports.
- DSCP priority is not supported for double-tagged frames.
- Double tagged ingress traffic is prioritized based on the outer tag VPT.
- On double tagged egress traffic, only the outer tag VPT is remarked.
- Classification by the inner VLAN tag of Q-in-Q traffic is not supported.
- Q-in-Q IGMP control packets are not double tagged on FE ports.
- The Ethertype of both the inner and outer tags of Q-in-Q packets is always 0x8100. Other provider ethertypes are not supported.

Problem Reports

PR 46903

The user is not prevented from enabling MSTP even though ports are in customer mode.

Workaround: Refrain from enabling MSTP when there are ports in customer mode.

PR 46899

It is possible to configure an IP interface on a VLAN that has a customer port member. However, this configuration is not actually applied.

Workaround: Refrain from defining IP interfaces on VLAN with customer ports.

Multicast TV VLAN

Feature Exceptions

- Packets cannot be classified based on the inner tag.
- A provider VLAN cannot be assigned on a Multicast TV VLAN.
- Provider VLANs cannot be assigned per port/VLAN.

Private VLAN Edge

Feature Exceptions

- As noted in the User Guide, a Private VLAN Edge uplink can only be a GE port.

Quality of Service

Feature Exceptions

- 1K policy rules, conditions and actions are supported on the OS6200 series switches. Feature interactions may result in availability of fewer than this number, in certain scenarios.
- Egress Rate Shaping should not be configured on ports configured as Half Duplex.
- Quality of Service is applied to ingress Q-in-Q customer port single tagged traffic after the provider tag is added. Therefore, the same rules apply to single-tagged traffic incoming to customer ports, as for double-tagged traffic coming in to trunk ports.
- DSCP priority is not supported for double-tagged frames.
- Double tagged ingress traffic is prioritized based on the outer tag VPT.
- On double tagged egress traffic, only the outer tag VPT is remarked.
- Classification by the inner VLAN tag of Q-in-Q traffic is not supported.

Problem Reports

PR 39281R

Burst configuration for egress traffic shaping is not supported on FE ports, even though it is possible to configure it. Refer to the *OS6200 User Guide* for more information.

Workaround: Disregard traffic shaper burst configuration on FE ports, as this parameter is relevant only on GE ports. Support for CLI configuration of these parameters on FE ports will be removed in a future software version.

PR 41903R

When configuring the system to work in Advanced Quality of Service Mode, the system remains in "Trust DSCP" mode and not as indicated in user documentation.

Workaround: There is no known workaround at this time.

PR 39101D

When the device is configured with system-wide trust DSCP, the VPT value is always overwritten.

Workaround: When configuring the device with system-wide trust DSCP, avoid configuring an ACL with a rule based on the Class of Service (VPT) value.

PR 39110D

If traffic shaping is set on a port running in half duplex mode, the queue reserved for Control Traffic gets stuck. This may affect traffic forwarding on the device.

Workaround: Prior to setting traffic shaping on a port, ensure that it is running in Full Duplex mode.

PR97170 / AL0011

The Advanced Quality of Service commands "set queue", "set cos" and "trust" do not affect behavior if the destination port is an FE port.

Workaround: Traffic can be prioritized on FE ports in one of the following ways:

- In QoS Basic Mode, if the traffic is tagged traffic, it is possible to set the VLAN Priority Tag (VPT) of the packet with a high priority value (e.g., 7). This way, the packet is marked with the high-priority value as it ingresses the port. The packet is then assigned to the high-priority queue, and receives priority treatment. This works only if the trust mode is set to VPT (per default).
- If the system is set to Basic QoS mode, and the device is in Trust DSCP mode, then changing the DSCP value of the packet to a higher value achieves the desired results.
- If the system is set to Advanced QoS mode, it is possible to use the same structures (ACLs, Class Maps and Policies), and to set the DSCP value of the packet to a high value (using the CLI Policy Map Configuration mode command set dscp), rather than directly assigning the traffic flow to a specific queue. This ensure that the packet is assigned to the highest queue. NOTE: This will change the DSCP value of the packet.

Problem Reports

PR 66131

Can not bind a port to channel group after you configured acl on it.

Workaround: First bind the port to channel group and then define ACL on it.

Problem Reports

PR 66244

Can not delete deny rule from management ACL.

Workaround: Use the CLI interface instead.

Performance

Problem Reports

PR 57607

On specific scenario which execute burst of traffic which is combined from the following traffic structure:

Stream 1:

Packet Size: 1411 (including CRC)

Number of bursts: 1

Packets per burst: 6000

Single SA to Single DA

Data pattern: Fixed 00 00

Stream 2:

Packet Size: 65 (including CRC)

Number of bursts: 1

Packets per burst: 100,000

Single SA to Single DA

Data pattern: Fixed 00 00

The following results occur:

1. The number of packet loss does not change; no matter the amount of packets sent in the test (~8 packet drops per port when sending 1000 frames or when sending 100,000 frames).

2. When changing the order in the flows (sending first the short packets and then the long packets) there are no drops.
3. When the test is change to continuous mode (instead of a single burst) there are no drops.
4. When the test is change to continuous burst mode (instead of a single burst) there are no drops.
5. When increasing the buffer limit settings to maximum the number of packet loss was reduced to 1.

The problem occurs due to the way the IXIA generates the traffic at the very beginning of the test.

Workaround: There is no known workaround at this time.

Problem Reports

PR 66124

While connecting a stand alone unit to the network using a single 100MB link and performing an FTP transfer from one PC while pinging the server, packets are lost.

Security

Feature Exceptions

- Telnet and SSH sessions are disconnected if no username is configured. This is expected behavior, in order to prevent security breaches in the absence of a default username. No security mechanism is in place in the device prior to configuration of a username using the console interface. Refer to the 6200 User Guide for information on defining usernames and passwords.

Unknown Unicast Storm Control

Problem Reports

PR 39873R

Known unicast packets are counted with unknown unicast packets.

Workaround: Avoid configuring storm control on unknown unicast packets.

Port Monitoring

Feature Exceptions

- With broadcast traffic, the traffic is replicated to the analyzer only once instead of one per mirror port. This issue is related to the way the Opal was designed and implemented. For monitoring (analyzing) purposes only one destination port for the frames per 88E6095 device (Opal) can be defined. Frames that are transmitted out are copied to the port defined monitor. When a packet arrives and the following conditions exist: One, it is targeted to a group of ports members of the same VLAN, which are connected to the same Opal device, and second, the group of port is analyzed on the same port. Then when the Opal device triggers the packet for first time it copies the packet once to the monitoring port. This is done for all the

ports, which are members of the same VLAN. Therefore, in case it is a broadcast the Opal replicates the packet to the analyzer only once. It means that for each Opal we will get one replication of the packet.

Hardware and Environmentals

Feature Exceptions

- When the OS-LS-6224P or OS-LS-6248P reaches a state of Power over Ethernet overload, there is not enough power to provide to all Powered Devices connected to the switches. The device disconnects ports according to power management definitions, leaving connected those ports with higher priority. If all ports are configured with the same priority, then the ports are disconnected in the order in which they had been connected.
- Only Finisar SFPs support Optical Transceivers
- When using the web-based interface to perform Virtual Cable Testing, the page must be refreshed following the test, in order to view the results.
- As a result of negotiation if a port is disabled, the status of the port would remain as up.

Fiber Ports

Problem Reports

PR 39272D

Fiber ports support 100 Base-FX fiber (single mode and multimode) or 1000-Base LX/SX fiber. Some fiber ports made by specific vendors may have inconsistent behavior. Normally, when a fiber link is inserted into the combo port, it takes precedence over the copper port. In some instances, when a 100 SFP fiber link connects two devices, precedence is given to the first present link, even if it is a copper link.

The Fiberxon fiber links function as designed with the Alcatel OS-LS-6200.

Problem Reports

PR 66218

The commend "show fiber-ports optical transceiver" show N/A (Not Available) on mixed stack when the master is not 24fx

Stacking Ports Labels

Problem Reports

PR 39802D

The stacking ports are incorrectly labeled “down” on the up port, and up on the “down” port.

Status: The issue is fixed.

RPS Indication

PR 47144

The show system CLI command does not indicate status of the Redundant Power Supply.

Workaround: There is no known workaround at this time.

Front Panel Labels

PR 39803D

The GE Ports are labeled 49 and 50 on the OS-LS-6248 and OS-LS-6248P. The GE Ports are labeled 25 and 26on the OS-LS-6224 and OS-LS-6224P. The CLI refers to these interfaces as g1 and g2.

Workaround: There is no known workaround at this time.

PR 64775

First 4 LED are amber instead of green

PR 65009

The front panel of the 6224C displays 6224u

Port Channel

PR 58272

Negotiation does not work in port channel, unless configured to off and back on.

Workaround: There is no known workaround at this time.

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.