Release Notes

OmniStack 6200

Software Version 1.7.0.22/ Boot Version 1.0.0.12

These release notes accompany release 1.7.0.22 software and 1.0.0.12 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 1.7.0.22 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.alca-tel.com).

Upgrading to Alcatel OS6200 versions starting from 1.5.0.xx require upgrading to boot version of 1.0.0.12 as well.

Merging OS6200 Stacks

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

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

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

New HW version is released. The minimum software requirement is SW version 1.5.1.7.

New/Modified CLI Commands Supported

The following CLI commands are modified or newly introduced for Version 1.7.0.22. All CLI commands are described in the CLI Reference Guide.

CLI Command	Description of Functionality
dot1x legacy-supp-mode	Use the **dot1x legacy-supp-mode** interface configuration command in multiple session mode to enable 802.1x switch to send periodic EAPOL request identity frame according to tx timeout period. This is the default behavior
snmp-server community **snmp-server community-group**	Added the [mask | prefix-length]parameter after the existing ipv4-address parameter to allow filtering SNMP access community by using IP address and Mask

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
ARP Inspection Statistics	all
IP Source Guard Statistics	all
DVA for 802.1x	all
Protected ports	all

New Supported Features

Feature	Platform
802.1x – enable/disable sending periodic EAPOL request identity	all
SNMP community access by network	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.

LBD – LoopBack detection

Feature allows bridges to automatically detect and prevent L2 forwarding loops on port either in the absence of other loop-detection mechanisms like STP/RSTP/MSTP or when the mechanism can't detected it. Sometimes the BPDUs based loop detection can't be used due to the following facts:
-There is a client's equipment that drops or cuts the BPDUs
-The STP protocol is restricted on edge Network

The feature detects that a port has been looped back to the local system. If a loop-back is detected, the port is disabled (forced down) and the appropriate Error Log is issued. Note that loops may also exist between different ports. The implementation doesn't distinguish between these two events (it is the user responsibility to enable this feature on access links only). User also can monitor the ports status through special control implemented in CLI/WEB/NMS (SNMP)

Protected Ports

The Protected Ports feature provides layer-2 isolation between ports that share the same broadcast domain (VLAN). The feature defines 2 types of ports:

-Protected ports: Can send traffic only to uplink ports (protected port can be only FE ports)
-Uplink ports: Can send traffic to any port (uplink can be only GE ports)

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.

STP Root Guard

Network administrators may want to prevent devices outside of the core of the network from being assigned the spanning tree role of “root”. Spanning Tree Root Guard is used to prevent an unauthorized device from becoming the root of a spanning tree.

STP BPDU Guard

BPDU Guard is used as a security mechanism to protect the network from invalid configurations.

BPDU Guard is usually used either when fast link ports (ports connected to clients) are enabled or when STP feature is disabled. When BPDU guard is enabled on a port, the port is shut down if a BPDU message is received and an appropriate SNMP trap is generated..

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 aggre-

gation 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.

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.

L2 Multicast

IGMP Snooping

By default, a Layer 2 switch forwards multicast frames to all ports of the relevant VLAN, essentially treating the frame as if it were a broadcast. While this is functional, in the sense that all relevant ports/nodes will get a copy of the frame, it is potentially wasteful – ports/nodes may receive irrelevant frames only needed by a subset of the ports of that VLAN.

This may be alleviated by explicit system configuration, or by "snooping" (examining the contents of) IGMP frames as they are forwarded by the switch from stations to an upstream multicast router. This allows the switch to conclude which stations are interested in joining a specific multicast group, where they are located and where multicast routers sending multicast frames are located. This knowledge is used to exclude irrelevant ports from the forwarding set of an incoming multicast frame.

IGMP Querier

The IGMP Snooping Querier is used to support L2 multicast domain of snooping switches in the absence of multicast router. A typical example is a local network where the multicast content is provided from a local server, and the router (if exists at all) of that network does not support multicast.

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.

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 user can create one or more access control list. 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.

LLDP and LLDP-MED

802.1ab is an IEEE standard for link layer discovery in Ethernet networks. It provides a method for switches, routers and access points to advertise their identification, configuration and capabilities to neighboring devices that store the data in a MIB (management information base). Link layer discovery allows a network management system to model the topology of the network by interrogating the MIB databases in the devices.

This LLDP-MED provides extensions to the IEEE 802.1AB base protocol provide behavioral requirements for devices implementing the extensions to enable correct multi-vendor interoperation. LLDP-MED can allow auto discovery of LAN policies that enables “plug and play” networking and automated power management of PoE endpoints.

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).

802.1x - MAC Authentication

MAC authentication is an alternative to 802.1X that allows network access to devices (such as printers and IP phones) that do not have the 802.1X supplicant capability. MAC authentication uses the MAC address of the connecting device to grant or deny network access.

In multiple session mode - support for both compliant 802.1x devices (such as Windows Vista) and non-compliant 802.1x devices (such as Windows XP SP2).

Allowing user to configure – per interface, to enable or disable 802.1x switch to send periodic EAPOL request identity frame according to Tx timeout period. Periodic transmission is needed in multiple session mode in order to verify authentication for devices that do not follow 802.1x standard behavior. Disabling periodic sending of frame allows better support for devices that follow the 802.1x standard behavior.

802.1x – BPDU Flooding

According to IEEE802.1x standards 802.1x BPDUs should never be forwarded. The 802.1x BPDUs should be handled by the switch in case 802.1x is enabled on the port, or should be discarded by the switch in all other cases.

This feature enables the switch to bridge 802.1x BPDU packets as data packets.

802.1x – DVA

RFC 3580 provides definitions of Radius attributes for the 802.1X Authentication. Those attributes are typically used to: Send parameters (E.g. port number) from the Authenticator to the Radius server in order to add information to the authentication decision.Send supplicant’s attributes from the Radius server to the Authenticator.

This feature enables the switch to assign port to VLAN according to Radius server decision.

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.

DHCP Snooping

DHCP snooping is a DHCP security feature that provides network security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding database, also referred to as a DHCP snooping binding table. DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. DHCP snooping differentiates between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch.

DHCP Option 82

Relay agent information option (option-82) in the DHCP protocol enables a DHCP relay to send the port number of a client that requested an IP address. The Relay agent information option specifies the port number from which the client’s packet was received.

IP Source Address Guard

IP source guard is a security feature that restricts IP traffic on non-routed, Layer-2 interfaces by filtering traffic based on the DHCP snooping binding database and on manually configured IP source bindings. IP source guard can be used to prevent traffic attacks caused when a host tries to use the IP address of its neighbor. In addition this feature provides counting information for entries added for validation.

Dynamic ARP Inspection

Dynamic ARP inspection is a security feature that validates ARP packets in a network. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks. In addition this feature provides statistics of dropped/forwarded packets.

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

Fixed Problem Reports

AMAP

Alcatel 0000505/Alcatel PR 127670/CQ 116805 (Version 1.7.0.22)

AMAP on OS62xx doesn't detect new devices 6400, 9000E and 6855

Status: This issue was fixed

Layer 2

Problem Reports

Alcatel 0000487/Alcatel PR 130511/CQ 114971 (Version 1.7.0.22)

STP doesn't detect loops on ports if 802.1x is enabled

Status: This issue was fixed

Quality of Service

Problem Reports

none.

General

Problem Reports

Alcatel 0000469/Alcatel PR 1435827/CQ 113254(Version 1.7.0.22)

DVA does not work well with WinXP if automatic authentication during power up is used

Status: This issue was fixed, user needs to set interface EAP sending mode to non legacy mode using interface mode command: "**no dot1x legacy-supp-mode"**

Alcatel 0000504/Alcatel PR 132939 /CQ 116723(Version 1.7.0.22)

In multiple sessions mode device sends EAP requests every 30 seconds although PC is already authenticated

Status: This issue was fixed, user needs to set interface EAP sending mode to non legacy mode using interface mode command: "**no dot1x legacy-supp-mode"**

Alcatel 0000514/Alcatel PR 134178 /CQ 116670 (Version 1.7.0.22)

DHCP discover with option 82 coming from untrusted ports are being dropped

Status: This issue was fixed.

Alcatel 0000515/Alcatel PR 134220 /CQ 116893 (Version 1.7.0.22)

OS6200 doesn't respond to gratuitous ARP request

Status: This issue was fixed.

User Interface

Problem Reports

Alcatel 0000507/Alcatel PR 135749 /CQ 116315 (Version 1.7.0.22)

Management access list is removed when upgrading from 1.5.0.x to 1.7.x

Status: This issue was fixed.

Alcatel 0000508/Alcatel PR 136098 /CQ 116321 (Version 1.7.0.22)

The command "map subnet.." generates an error when using subnet addresses

Status: This issue was fixed.

Alcatel 0000519/Alcatel PR 136095 /CQ 116900 (Version 1.7.0.22)

Device Crash when using SNMP to configure trap settings in stack

Status: This issue was fixed.

Alcatel 0000522/Alcatel PR 135140 /CQ 116950 (Version 1.7.0.22)

A fatal error occurs when ACL is applied to all the interfaces

Status: This issue was fixed.

Alcatel 0000531/Alcatel PR ---- /CQ 117396 (Version 1.7.0.22)

A fatal error occurs when using Omnivista for certain SNMP queries

Status: This issue was 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

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

Web Based Interface

Problem Reports

Command Line Interface

Problem Reports

PR 76387

Display issue, TCAM Resources page shows incorrect information – all units are displayed in the window even if a unit is not present.

Workaround: this is only display issue. No workaround.

PR 78035

Display issue, Show ip igmp snooping learns mrouter even when igmp snooping is disabled.

Workaround: this is only display issue. No workaround currently.

PR 78045

QOS trust mode per port is displayed in CLI "show qos interface Ethernet" although it can not be disabled or enabled by administrator.

Workaround: this is only display issue. No workaround currently.

BOOT

Feature Exceptions

- In the boot menu stack sub menu and the auto unit ID is not supported for this version.

Stacking

Feature Exceptions

- 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.

Problem Reports

PR 76998

When adding duplicated unit #1 to a stack - unit is resets with fatal error.

Workaround: There is no known workaround at this time. Note this is not a practical configuration.

Layer 2

Flow Control

Feature Exceptions

- Flow control does not operate across the stack.
- Flow control does not operate on Gigabit Ethernet ports.

Interswitch Protocols (AMAP)

Feature Exceptions

- AMAP only runs on default VLAN (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.

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.

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. The following of unknown multicast 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, when there are not group members, use the following command:
  console (config)# interface vlan 1
  console(config-if)#bridge multicast address 01:00:5e:01:02:03

Q-in-Q

Feature Exceptions

- Spanning tree must be disabled on customer ports if MSTP is enabled globally on device.
- 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 (802.1p) is applied to the outer VLAN tag. Therefore 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 on FE ports for double-tagged frames.
- On double tagged egress traffic, only the outer tag VPT is remarked.
- The Ethertype of both the inner and outer tags of Q-in-Q packets is always 0x8100. Other provider ethertypes are not supported.
- Classification according to Inner VLAN is not supported on Giga Ethernet port.

IGMP Snooping

Feature Exceptions

- When IGMP is moving from V2 to V3 - when VLAN is in IGMPv2 mode and receives aV3 query - it waits X seconds (x=RSVD value in query packet translated to seconds) after which it flushes group address and moves to V3 mode. Delay is to allow switch to determine if there are still any other V2 routers on network - in which case it will not change its mode.

- Due to the flushing - reports that host send in reply to the first V3 query are not "kept" by the switch - and therefore you have flooding for up to 125 seconds (query interval) - until next time hosts respond to query. Few first reports and responses to the IGMP v3 query would not be registered due to delay in table flushing.
  This scenario is usually a "controlled" maintenance scenario (inserting V3 Multicast router into network) - so it should not have a significant impact.
- IGMP Querier in v3 does not support sending Specific query upon receiving a Leave message.

Multicast TV VLAN

Feature Exceptions

- A provider VLAN cannot be assigned on a Multicast TV VLAN.
- Provider VLANs cannot be assigned per port/VLAN.
- Multicast TV VLAN is not working when connected VLAN is in IGMP v3 mode.
- Guest VLAN can not be enabled together with MTV mapping on the same port.

Private VLAN Edge

Feature Exceptions

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

Host

MTU

Feature Exceptions

- The MTU of the Switch when “transmit” packets from CPU (actually it is management or protocol packets) is 1518 bytes, when system for “receive” and “forwarding” supported 1632. The reason is to prevent possible miss-connectivity that can happen when setting the MTU of the system to 1632 Bytes: whenever the system sends out frames that need to be fragmented, e.g: HTTP, the packets will be fragmented to 1632 Bytes segments. However, most Ethernet NICs support up to 1518 Bytes.

Quality of Service

Feature Exceptions

- **The following command: port storm-control include-multicast unknown-unicast is not supported in this version and should be removed from configuration file when upgrading from version 1.0**
- 1K policy rules (892 rules are available post system initialization), conditions and actions are supported on the OS6200 series switches. Feature interactions may result in availability of fewer than this number, in certain scenarios.
- Policy map can have only up to 256 rules per unit.
- Egress Rate Shaping should not be configured on FE ports configured as Half Duplex.
- 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.
- In FE ports on the egress the “trust cos-dscp” is applied by default (if it’s IP traffic it’s prioritized according to DSCP else according to VPT). However in Giga ports, by default all traffic is assumed as best effort. In QOS advanced egress GE port

don't prioritize traffic according to DSCP but in best effort. This behavior is different than FE ports. In order to prioritize traffic according to “cos-dscp” the user should use a policy map and apply the “trust cos-dscp” rule in the policy.

- For packets received untagged on ingress port, the VPT on the output may differ from default CoS value set on the input port, due to default VPT-to-Queue mapping.
- The ACL entries are always 2 entries aligned on chip. If you create an ACL with 1 rule it occupies 2 entries in H/W.

Problem Reports

PR 74839

In QOS Advanced mode the User Priority of a traffic that arrives from FE port is reset to priority 2, In QOS advanced mode all the traffic that will ingress FE ports will be assigned with User Priority 2.

Workaround: There is no known workaround at this time.

PR 69079R

When configuring the system to work in Advanced Quality of Service Mode, the FE ports remain in “Trust DSCP-VPT” mode and not as indicated in user documentation.

Workaround: There is no known workaround at this time.

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.
- Known unicast packets are counted with unknown unicast packets.

IP Source Guard

- When configuring IP address on a port which has only one VLAN which was configured with DHCP snooping - since the port is removed from its previous VLAN membership (due to the IP address assignment) - therefore no snooping VLAN exists on the port which causes IP source guard to become inactive.
- When configuring IP address on a truck which has tagged VLANs which was configured with DHCP snooping - since the port remains part of its previous VLAN membership (truck) and therefore IP source guard is still active.
- When MAC Authentication with DVA is enabled with IP Source Guard (and DHCP Snooping) user MUST enable the DHCP Snooping on Guest VLAN too. The reason is that upon MAC authentication the regular packet or NA message MUST be forwarded to CPU. The way to do it is to define DHCP Snooping. In regular situation Host will issue the DHCP request which would be fetched by DHCP Snooping on Guest VLAN, and as a result authenticated and assigned to DVA VLAN. After that all will work in regular manner
-

ARP Inspection

- ARP Inspection feature uses ARP Inspection db (user configuration) and dynamic (learned by DHCP snooping) db for the decision. When ARP packet comes for validation ARP first looking for the IP in local db and if not found goes to DHCP

snooping. ARP packets which validated through DHCP snooping data base counted only according to common forward and drop counters and not with mismatch counter.

Port Security - 802.1x

Feature Exceptions

- Mac based authentication in this version assumes that the password field and the username field both carry the MAC address. This should be defined on the Radius server.
- Port security and 802.1x Single Host Mode cannot be enabled simultaneously on the same interface.
- When port is unauthorized and member in the guest VLAN and port is configured as MAC authentication enabled, MAC will not be learned from this port on the guest VLAN, this is to allow MAC authentication. Upon receiving “authorized MAC” the port will be removed from the guest VLAN and added to static VLAN configuration at that time the MAC will be learned.
  During the period of time till MAC is authorized, traffic to stations on this port will be treated as unknown as long as the port is member in the guest VLAN. In that case traffic to this MAC from the network will be flooded to all ports on the guest VLAN.
  The reason for this behavior is that the MAC authentication is not granted as result of the first frame with the source MAC.
- 802.1x does not work on customer port if traffic is received tagged. According to the standard EAP frames are supposed to be untagged.
- In order to enable Windows users authentication a new mechanism was added to the system. OS6200 sends out multicast EAP-requests every 30sec and forcing all supplicants to reply with EAP-response. Unauthenticated users will be forced into authentication process with pass/fail result. Users who were already authenticated previously on this port will be dropped out of the authentication process. Windows users will not be affected by this, but the result is “un-authenticated interface from (some) client point of view. In fact this will be expected behavior for any 802.1x compliant supplicant.
- Customer port authentication fails. Due to race condition on the CPE in some cases other packet such as AMAP or Spanning Tree traffic is received each time port comes up. Following the 6200 tries to authenticate the source Mac of the AMAP packet, fails and triggers the quiet time period. On that time no Mac can authenticate. Hence, the CPE Mac and the PC Mac are competing on the authentication.
- Per design both in single host mode and multiple host mode there can be only one authorized supplicant per port. The only difference between the modes is if other traffic not belonging to authorized supplicant MAC will pass or not. In case two users are sending authentication packets in multiple hosts. This might cause that one of authentication might be blocked, since when the 2nd client begins another (new) authorization/authentication process. This causes the switch to examine again its state and restart authorization process - sending out EAP request packets. Once the first client receives the EAP request from the switch, it also restarts its authentication process. Since the port can only authorize one client - the 2nd client gets authorized, while the 1st client is "turned off" since it did not complete the process of being authorized by the switch.

Lock Port

Feature Exceptions

- Device does not shut down port or send trap for MAC violation if MAC is learned on another locked port, because it is already in secured state.

Unknown Unicast Storm Control

Problem Reports

PR 74379R

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 mirrored port. 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.
- TX mirrored traffic on FE ports are copied to analyzer always untagged

Hardware and Environmental

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.
- 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.

RPS Indication

Problem Reports

PR 75180R

When connecting the RPS to a PoE box (without disconnecting the main PS), the system reset.

Workaround: There is no known workaround at this time. Connect RPS to device when power is down.

Fiber Ports

Problem Reports

PR 75931

The show fiber-ports optical-transceiver is not working properly for the fast Ethernet ports.

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 38 855 6929
Asia Pacific	+65 6240 8484
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.