ALCATEL.LUCENT Enterprise Business Group

IP Networking Portfolio

Network Solutions with OmniStack 6200 Series

Technical Document

Table of Contents

OmniStack LS 6200

The OmniStack LS 6200 switches currently available are:

- **OS-LS-6212**, Chassis that is a Fast Ethernet L2+ stackable, fixed configuration chassis in a 1U form factor consisting of 12 ports 10/100 RJ-45 ports, two 10/100/1000 RJ-45 ports and two combo ports. Combo ports consist of two additional 10/100/1000 RJ-45 and two mini-GBIC ports. MiniGBIC ports support Gigabit or Fast Ethernet MiniGBIC (SFP) optical transceivers, which can be ordered separately. Stacking capability utilizes the two 10/100/1000 RJ-45 ports and standard Ethernet cabling. Optional backup power supported.

- **OS-LS-6212P**, Chassis that is a Fast Ethernet L2+ stackable, fixed configuration chassis in a 1U form factor consisting of 12 ports 10/100 RJ-45 ports with Power over Ethernet, two 10/100/1000 RJ-45 ports and two combo ports. Combo ports consist of two additional 10/100/1000 RJ-45 and two mini-GBIC ports. MiniGBIC ports support Gigabit or Fast Ethernet MiniGBIC (SFP) optical transceivers, which can be ordered separately. Stacking capability utilizes the two 10/100/1000 RJ-45 ports and standard Ethernet cabling. Optional backup power supported.

- **OS-LS-6224**, Chassis which is a Fast Ethernet L2+ stackable fixed configuration chassis in a 1U form factor consisting of 24 10/100 RJ-45 ports, two 10/100/1000 RJ-45 ports and two combo ports. Combo ports consist of two additional 10/100/1000 RJ-45 and two mini-GBIC ports. Mini-GBIC ports support Gigabit Ethernet mini-GBIC (SFP) optical transceivers. Stacking capability uses the two 10/100/1000 RJ-45 ports and standard Ethernet cabling.

- **OS-LS-6224P**, Chassis which is a Fast Ethernet L2+ stackable fixed configuration chassis in a 1U form factor consisting of 24 10/100 RJ-45 ports with power over Ethernet, two 10/100/1000 RJ-45 ports and two combo ports. Combo ports consist of two additional 10/100/1000 RJ-45 and two mini-GBIC ports. MiniGBIC ports support Gigabit Ethernet MiniGBIC (SFP) optical transceivers. Stacking capability uses the two 10/100/1000 RJ-45 ports and standard Ethernet cabling.

- **OS-LS-6248**, Chassis which is a Fast Ethernet L2+ stackable fixed configuration chassis in a 1U form factor consisting of 48 10/100 RJ-45 ports, two 10/100/1000 RJ-45 ports and two combo ports. Combo ports consist of two additional 10/100/1000 RJ-45 and two mini-GBIC ports. Mini-GBIC ports support Gigabit Ethernet mini-GBIC (SFP) optical transceivers. Stacking capability uses the two 10/100/1000 RJ-45 ports and standard Ethernet cabling. **4.4.1, 4.4.2**

- **OS-LS-6248P**, Chassis which is a Fast Ethernet L2+ stackable fixed configuration chassis in a 1U form factor consisting of 48 10/100 RJ-45 ports with power over Ethernet, two 10/100/1000 RJ-45 ports and two combo ports. Combo ports consist of two additional 10/100/1000 RJ-45 and two mini-GBIC ports. Mini-GBIC ports support Gigabit Ethernet mini-GBIC (SFP) optical transceivers. Stacking capability uses the two 10/100/1000 RJ-45 ports and standard Ethernet cabling.

- **OS-LS-6224U**, Chassis which is a Fast Ethernet L2+ stackable fixed configuration chassis in a 1U form factor consisting of 24 ports 100Base-X SFP, two 10/100/1000 RJ-45 ports and two combo ports. Combo ports consist of two additional 10/100/1000 RJ-45 and two mini-GBIC ports. The 24 SFP ports accepts industry standard 100Base-X optical transceivers which are sold separately. MiniGBIC ports support Gigabit or 100FX Ethernet MiniGBIC (SFP) optical transceivers, which can be ordered separately. Stacking capability utilizes the two 10/100/1000 RJ-45 ports and standard Ethernet cabling. Optional backup power supported.

Hardware Overview

10/100 Networking

To stay competitive, 21st century businesses must take advantage of new networking technologies that deliver quick and secure access to vital information from any location. Customers expect and demand that customizable user-centric services be securely provided over an always available environment, and they want to be able to access it from anywhere such as over the Internet. Most enterprise networks have Ethernet-based infrastructures where workgroup switches supply the bulk of switch ports needed, making them an ideal target for performance improvements at attractive prices. With the latest workgroup switch technologies from Alcatel.Lucent, it's possible to provide power-over-Ethernet across your campus for true plug-and-play connectivity for wireless LAN access points, IP phones, and other network devices. Alcatel.Lucent's switches also take advantage of and exploit network intelligence improving user security while reducing operating expenses, capital expenditures, training and day-to-day management costs.

Alcatel.Lucent has designed the OmniStack LS 6200 (OS-LS-6200) family of stackable Ethernet switches to address enterprise and residential networking needs. They are fixed configuration, 10/100 copper or 100BaseX fiber layer-2 switches that deliver the advanced features and services demanded by users. These 12, 24 or 48 ports Fast Ethernet switches provide the same advanced capabilities previously available only in Gigabit-class switches, making them an excellent, inexpensive edge device. The OS-LS-6200s provide wire rate layer-2 forwarding and advanced layer 2-4 services. They also securely support advanced quality of service with advanced user and traffic classification capabilities for exceptional video, voice, and data performance. Every OS-LS-6200 switch comes with two 10/100/1000 copper ports that can be used with standard Ethernet cabling for fault-tolerant dedicated stacking links or as Gigabit ports in a standalone configuration. They also come with two additional Gigabit combo ports that provide ports for upstream connectivity to the network or to high-speed servers. Combo ports provide the user the ability to attach via standard copper Ethernet cabling or fiber using industry standard optical transceivers.

The OS LS 6200 switches deliver network intelligence, improving security for your users while simultaneously reducing operating expenses, capital expenditures, training, and day-to-day management costs.

A compact, one unit (1U) high form factor, all in one stackable design and a comprehensive set of features makes the OS-LS-6200 perfect for:

- Enterprise workgroups / LAN wiring closets
- Edge deployments, small-/medium-sized businesses and branch offices
- Power-over-Ethernet
- Residential Ethernet access distribution devices (MDU) for triple play services delivery

The OmniStack LS 6200 switches currently available are:
OS-LS-6212, OS-LS-6224, OS-LS-6248 which are Fast Ethernet L2+ stackable fixed configuration chassis in a 1U form factor consisting respectively of 12, 24 or 48 10/100 RJ-45 ports, two 10/100/1000 RJ-45 ports and two combo ports.
Combo ports consist of two additional 10/100/1000 RJ-45 and two mini-GBIC ports.
Mini-GBIC ports support Gigabit or 100BASE-FX Ethernet Mini-GBIC (SFP) optical transceivers.
Stacking capability uses the two 10/100/1000 RJ-45 ports and standard Ethernet cabling.
OS-LS-6212P, OS-LS-6224P, OS-LS-6248P, which are Fast Ethernet L2+ stackable fixed configuration chassis in a 1U form factor consisting respectively of 12, 24 or 48 10/100 RJ-45 ports with power over Ethernet, two 10/100/1000 RJ-45 ports and two combo ports.
OS-LS-6224U, which is a Fast Ethernet L2+ stackable fixed configuration chassis in a 1U form factor consisting of 24 x 100BaseX SFP ports, two 10/100/1000 RJ-45 ports and two combo ports. The 24 SFP ports accept industry standard 100Base-X optical transceivers.
The OS LS 6200 family uses a modular external backup power solution that provides redundant chassis and PoE power on a 1:1 basis.

The OS-LS-6200 family complements the existing portfolio of Alcatel.Lucent enterprise fixed-configuration workgroup switches which includes:

- OmniSwitch 6602 family of switches: stackable layer-3 10/100 with Gig uplinks
- OmniSwitch 6800 and 6850 families of switches: stackable layer-3 10/100/1000 capable of 10Gig uplinks. Alcatel.Lucent OmniVista Network Management System supports OS LS 6200.

Alcatel.Lucent's fixed configuration switches are part of the larger Alcatel.Lucent enterprise portfolio that includes the modular-based OmniSwitch 7000 and 9000 series of modular aggregation and core switches. Together, this portfolio offers a complete edge-to-core solution with high availability, intelligent performance, and enhanced security in an easy-to-manage, flexible and scalable package.

Alcatel.Lucent understands the need to offer investment protection and provides a limited lifetime hardware warranty on OS-LS-6200, OS6602, OS6800 and OS6850 families of switches.

Cost effective, enterprise workgroup switch

The OS-LS-6200 family offers small, medium or large enterprise networks a cost-effective and secure means of deploying PoE on every port, providing users mobility across the campus. By providing wire speed
QoS and security to the edge, Alcatel.Lucent is able to ensure a highly available network for important applications such as IP voice communications. The OS LS 6200s support industry-standard CLI, and provide simplified stack management using standard Ethernet cabling. This reduces the complexity and costs associated with training, installation, configuration, and maintenance.

Superior architecture

This switch family also provides a superior architecture with four useable
Gigabit Ethernet ports that support stacking and multi-Gig uplink connectivity without sacrificing user ports.
Since the OS-LS-6212 and OS-LS-6224 are fan-less designs, they are a perfect fit for environments with severe noise restrictions. In addition, the advanced VLAN classification offered by the OS-LS-6200 family improves partitioning of users and applications, greatly improving security and enabling better performance for network applications including voice and video.

Multi-Service operator

The OS-LS-6200 family supports residential network operators at the network's edge with:

- Per service VLAN stacking (Q-in-Q) capability providing scalability for user ser vice differentiation
- A reduced number of VLANs in aggregation
- Interoperability with MPLS/VPLS core network architecture

Through the use of multicast TV VLANs the OS LS 6200s provide extremely efficient bandwidth usage by preventing duplication of TV streams sent between the core and the edge of the network. In addition, it enables multiple TV providers per subscriber.

OmniStack LS 6212 & 6212P

- **OS-LS-6212**, Chassis that is a Fast Ethernet L2+ stackable, fixed configuration chassis in a 1U form factor consisting of 12 ports 10/100 RJ-45 ports, two 10/100/1000 RJ-45 ports and two combo ports. Combo ports consist of two additional 10/100/1000 RJ-45 and two mini-GBIC ports. MiniGBIC ports support Gigabit or Fast Ethernet MiniGBIC (SFP) optical transceivers, which can be ordered separately. Stacking capability utilizes the two 10/100/1000 RJ-45 ports and standard Ethernet cabling. Optional backup power supported.
- **OS-LS-6212P**, Chassis that is a Fast Ethernet L2+ stackable, fixed configuration chassis in a 1U form factor consisting of 12 ports 10/100 RJ-45 ports with Power over Ethernet, two 10/100/1000 RJ-45 ports and two combo ports. Combo ports consist of two additional 10/100/1000 RJ-45 and two mini-GBIC ports. MiniGBIC ports support Gigabit or Fast Ethernet MiniGBIC (SFP) optical transceivers, which can be ordered separately. Stacking capability utilizes the two 10/100/1000 RJ-45 ports and standard Ethernet cabling. Optional backup power supported.

OmniStack LS 6212 & 6212P

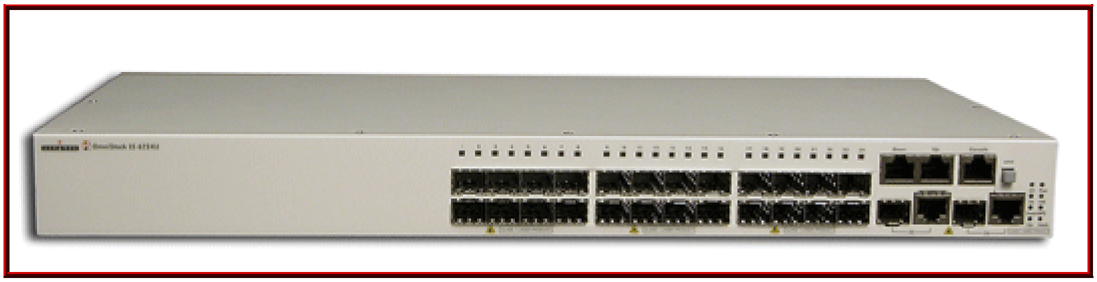
OmniStack LS 6224 & 6224P

- **OS-LS-6224**, Chassis which is a Fast Ethernet L2+ stackable fixed configuration chassis in a 1U form factor consisting of 24 10/100 RJ-45 ports, two 10/100/1000 RJ-45 ports and two combo ports. Combo ports consist of two additional 10/100/1000 RJ-45 and two mini-GBIC ports. Mini-GBIC ports support Gigabit Ethernet mini-GBIC (SFP) optical transceivers. Stacking capability uses the two 10/100/1000 RJ-45 ports and standard Ethernet cabling.
- **OS-LS-6224P**, Chassis which is a Fast Ethernet L2+ stackable fixed configuration chassis in a 1U form factor consisting of 24 10/100 RJ-45 ports with power over Ethernet, two 10/100/1000 RJ-45 ports and two combo ports. Combo ports consist of two additional 10/100/1000 RJ-45 and two mini-GBIC ports. MiniGBIC ports support Gigabit Ethernet MiniGBIC (SFP) optical transceivers. Stacking capability uses the two 10/100/1000 RJ-45 ports and standard Ethernet cabling.

OmniStack LS 6224 & 6224P

OmniStack LS 6224U

- **OS-LS-6224U**, Chassis which is a Fast Ethernet L2+ stackable fixed configuration chassis in a 1U form factor consisting of 24 ports 100Base-X SFP, two 10/100/1000 RJ-45 ports and two combo ports. Combo ports consist of two additional 10/100/1000 RJ-45 and two mini-GBIC ports. The 24 SFP ports accepts industry standard 100Base-X optical transceivers which are sold separately. MiniGBIC ports support Gigabit or 100FX Ethernet MiniGBIC (SFP) optical transceivers, which can be ordered separately. Stacking capability utilizes the two 10/100/1000 RJ-45 ports and standard Ethernet cabling. Optional backup power supported.



OmniStack LS 6224U

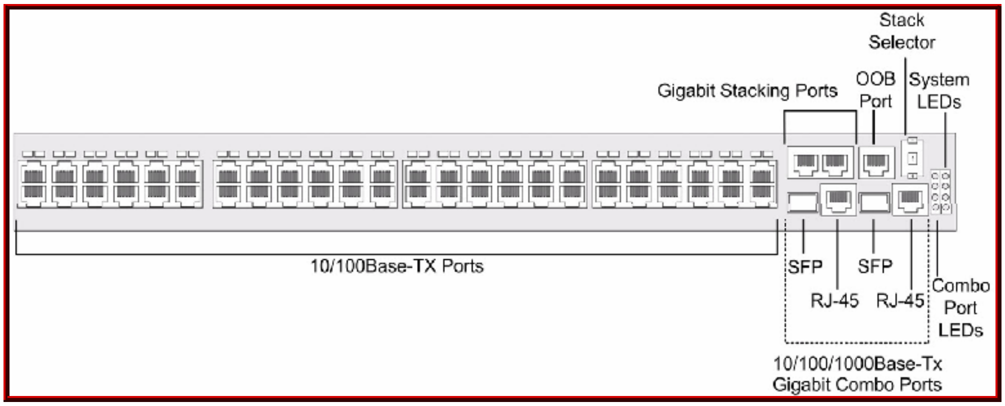
OmniStack LS 6248 & 6248P

- **OS-LS-6248**, Chassis which is a Fast Ethernet L2+ stackable fixed configuration chassis in a 1U form factor consisting of 48 10/100 RJ-45 ports, two 10/100/1000 RJ-45 ports and two combo ports. Combo ports consist of two additional 10/100/1000 RJ-45 and two mini-GBIC ports. Mini-GBIC ports support Gigabit Ethernet mini-GBIC (SFP) optical transceivers. Stacking capability uses the two 10/100/1000 RJ-45 ports and standard Ethernet cabling.
- **OS-LS-6248P**, Chassis which is a Fast Ethernet L2+ stackable fixed configuration chassis in a 1U form factor consisting of 48 10/100 RJ-45 ports with power over Ethernet, two 10/100/1000 RJ-45 ports and two combo ports. Combo ports consist of two additional 10/100/1000 RJ-45 and two mini-GBIC ports. Mini-GBIC ports support Gigabit Ethernet mini-GBIC (SFP) optical transceivers. Stacking capability uses the two 10/100/1000 RJ-45 ports and standard Ethernet cabling.

OmniStack LS 6248 & 6248P

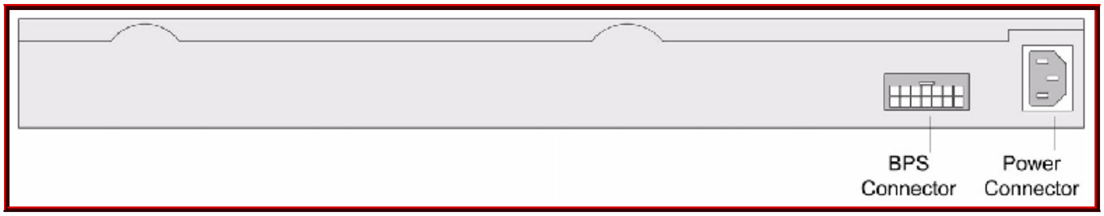
Front & Rear Panels

OS-LS-6200 models include 12-, 24- and 48- port versions with PoE derivatives and a 24- port 100Base-X SFP version, a space saving design, innovative and cost effective 1:1 backup chassis and PoE power, and a feature set that is capable of supporting converged applications and emerging security solutions.



Power Supply Receptacles

There are two power receptacles on the rear panel of the switch. The standard power receptacle is for the AC power cord. The receptacle labeled "BPS" is for the optional Backup Power Supply.



The height of all OmniStack LS 6200 models is 1RU (Rack Unit). The above figures illustrate the front and rear panel design of the OmniStack LS 6200. The front panel includes a number of LEDs that indicate the basic status of the unit and are intended to assist in local fault diagnosis. The status of the more complex parameters is accessed by the management applications.

User ports

The OS-LS-6200 Series supports 12, 24 or 48 10/100BaseT RJ-45 ports (with or without PoE capability) on the front panel. Each copper port is capable of auto-MDI/MDI-X sensing. The OS-LS-6200 Series also supports a 24- port 100Base-X SFP version.

Stacking ports

The OS-LS-6200 is equipped with two 10/100/1000 copper RJ-45 ports. OS-LS-6200 supports a fault tolerant looped stacking configuration. In a standalone configuration, these ports can be used as normal network ports.

Mix and match any model up to eight units high supporting fault tolerant stack loop. The copper RJ-45 10/100/1000 ports used for stacking use standard Category 5 Ethernet cabling and RJ-45 connectors for dedicated stacking between elements supporting one primary plus one secondary management entity.

Combo ports

The OS-LS-6200 is equipped with two Gigabit Ethernet SFP (mini-GBIC) plus two 10/100/1000 RJ-45 combo ports. They are located on the front panel. Users determine whether the mini-GBIC or 10/100/1000 ports will operate. The mini-GBIC ports support full duplex mode only. The Small Form Factor Pluggable (SFP) transceiver slots are shared with two of the RJ-45 ports (Ports 25~26/49~50). In its default configuration, if an SFP transceiver (purchased separately) is installed in a slot and has a valid link on its port, the associated RJ-45 port is disabled and cannot be used. The switch can also be configured to force the use of an RJ-45 port or SFP slot, as required.
SFP (Mini-GBIC) ports support 100Base FX fiber optic transceivers for 100Mbps fiber or 1000BaseX Gigabit fiber connectivity.
Note: All OmniStack LS 6200 Models "Combo" MiniGBIC ports support the SEP-100-LC-xxxx SFP Transceivers.

Transceivers

Gigabit Ethernet Transceivers (SFP MSA)	
SFP-GIG-EXTND	Extended 1000Base-SX Gigabit Ethernet optical transceiver (SFP MSA). Supports multimode fiber over 850nm wavelength (nominal) with an LC connector. Reach of up to 2 km (based on grade and condition of fiber) on 62.5/125 µm MMF or 550m on 62.5/125 µm MMF. Requires SFP-GIG-EXTND or GBIC-GIG-EXTND at the remote termination. [Formerly known as GE-EXTND-SFP]
SFP-GIG-LH40	1000Base-LH Gigabit Ethernet optical transceiver (SFP MSA). Supports single mode fiber over 1310 nm wavelength (nominal) with an LC connector. Typical reach of 40Km on 9/125 µm SMF.
SFP-GIG-LH70	1000Base-LH Gigabit Ethernet optical transceiver (SFP MSA). Supports single mode fiber over 1550nm wavelength (nominal) with an LC connector. Typical reach of 70 Km on 9/125 µm SMF. [Formerly known as MINIGBIC-LH-70]
SFP-GIG-LX	1000Base-LX Gigabit Ethernet optical transceiver (SFP MSA). Supports single mode fiber over 1310nm wavelength (nominal) with an LC connector. Typical reach of 10 Km on 9/125 µm SMF. [Formerly known as MINIGBIC-LX]
SFP-GIG-SX	1000Base-SX Gigabit Ethernet optical transceiver (SFP MSA). Supports multimode fiber over 850nm wavelength (nominal) with an LC connector. Typical reach of 300m on 62.5/125 µm MMF or 550m on 50/125 µm MMF. [Formerly known as MINIGBIC-SX]
100BASE-FX Ethernet Transceivers	
SFP-100-BX20LT	100Base-BX SFP transceiver with an SC type interface. This bi-directional transceiver is designed for use over single mode fiber optic on a single strand link up to 20KM point-to-point. This transceiver is normally used in the central office (OLT) transmits 1550nm and receives 1310nm optical signal
SFP-100-BX20NU	100Base-BX SFP transceiver with an SC type interface. This bi-directional transceiver is designed for use over single mode fiber optic on a single strand link up to 20KM point-to-point. This transceiver is normally used in the client (ONU) transmits 1310nm and receives 1550nm optical signal
SFP-100-LC-MM	100Base-FX SFP transceiver with an LC type interface. This transceiver is designed for use over multimode fiber optic cable.
SFP-100-LC-SM15	100Base-FX SFP transceiver with an LC type interface. This transceiver is designed for use over single mode fiber optic cable up to 15KM.
SFP-100-LC-SM40	100Base-FX SFP transceiver with an LC type interface. This transceiver is designed for use over single mode fiber optic cable up to 40KM.

10/100/1000BASE-T Ports

There are two types of RJ-45 ports, Ethernet ports that operate at 10 Mbps, 100 Mbps or 1000 Mbps, half or full duplex, and Fiber ports that operate at 1000 Mbps, full duplex. Because all ports on this switch support automatic MDI/MDI-X operation, you can use straight-through cables for all network connections to PCs or servers, or to other switches or hubs. Each of these ports supports auto-negotiation, so the optimum transmission mode (half or full duplex), and data rate (10, 100, or 1000 Mbps) can be selected automatically. If a device connected to one of these ports does not support auto-negotiation, the communication mode of that port can be configured manually.
Each port also supports auto-negotiation of flow control, so the switch can automatically prevent port buffers from becoming saturated.

100BASE-FX

Each 100BASE- FX port is capable of operating with 100Mbps full auto-negotiation with flow control capability.
The OS-LS-6224U supports 24 x 100BASE-FX ports on the front panel.

Console Port

There is one RS232 port for console connection. It provides a RJ45 (console interface management port) connector with DTE interface on default to connect to terminal. Special crossover cable needed for modem connection. Default rate baud is 115200 bps; the user can change the rate from 115200 down to 2400 bps. This console interface is configured as DTE for operation, diagnostics, status, and configuration information. The ship kit includes RJ-45 to DB-9 connector adapter.

The main AC-to-DC Power Supply

The OmniStack LS 6200 chassis supports one main built-in internal AC-to-DC power supply.
The power supply for the OS-LS-6212 provides up to 30 watts of DC output power.
The power supply for the OS-LS-6224, OS-LS-6224Uand OS-LS-6248 provides up to 54 watts of DC output power.
The power supply for the OS-LS-6212P (PoE based) provides up to 130 watts of DC output power.
The power supply for the OS-LS-6224P (PoE based) provides up to 225 watts (available 180 watts) of DC output power.
The power supply for the OS-LS-6248P (PoE based) provides up to 465 watts (available 375 watts) of DC output power.

Backup Power System

The OmniStack LS 6200 switch supports an external backup power system.

- Backup Power Supply (BPS)
    - OS-LS-62BP (126W): OS-LS-6200 modular AC backup power supply. Provides backup power to one non-PoE switch. Ships with chassis connection cable and country specific power cord.
    - OS-LS-62BP-P (510W): OS-LS-6200 modular AC backup power supply. Provides backup power to one OS-LS- 6200 PoE capable switch. Ships with chassis connection cable and country specific power cord.
    - OS-LS-62BP-DC (100W): OS-LS-6200 modular DC backup power supply. Provides backup power to one non-PoE OS-LS-6200 switch. Ships with chassis connection cable.

OmniStack LS 6200 Chassis Technical Specifications

OmniStack LS 6200 Dimensions & Weight	OS-LS-6212/6212P/6224/6224U: 17.32 in. x 9.05 x 1.73 in., , 44 x 23 x 4.4 cm (W x D x H) OS-LS-6224P/48/48P: 17.32 x 12.99 x 1.73 in., 44 x 33 x 4.4 cm, (W x D x H) Form factor: 1 RU (Rack Unit) high and 19" rack mountable Unit Weight: OS-LS-6212: 2.65kg, 5.84lbs OS-LS-6212P: 3.0kg, 6.61lbs OS-LS-6224U: 3.5kg, 7.7lbs OS-LS-6224: 3.0 kg, 6.61 lbs OS-LS-6224P: 4.45 kg, 9.81 lbs OS-LS-6248: 4.1 kg, 9.01 lbs OS-LS-6248P: 5.5 kg, 12.13 lbs
Connectors/cabling	• Management: one RJ-45 console interface configured as DTE for operation, diagnostics, status, and configuration information. Ship kit includes RJ-45 to DB-9 connector adapter • AC power connector and BPS connector on rear of chassis
Number of power supplies	OmniStack LS 6200 family supports one internal AC power supply for chassis power and an external connector on rear of chassis for use with the backup power supply solution
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-6212P, 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 OmniSwitch 6200 Family Getting Started Guide and OmniSwitch 6200 Family User Guide.
The **Main** Power Supply options Power supply status is communicated through the physical LED, CLI, WEB UI and SNMP agent OmniStack LS 6200 family supports one internal AC power supply for chassis power and an external connector on rear of chassis for use with the backup power supply solution	The OmniStack LS 6200 chassis supports one required main built-in internal AC-to-DC power supply in a non-redundant configuration. **Non-PoE Option:** **OS-LS-6224 and OS-LS-6248 and OS6224U:** Input Voltage: 100~240VAC Frequency: 50Hz~60Hz. Input Current will be less than 2.0A (rms) at 115VAC (rms) and 60Hz. Input Current will be less than 1.0A (rms) at 230VAC (rms) and 50Hz. Output Power: this power supply provides up to 54 watts of DC output power Output Voltage & Current: 12VDC@4.5Amps Minimum efficiency: 85% **OS-LS-6212:** Input Voltage: 100~240VAC Frequency: 50Hz~60Hz. Input Current is 0.75Amps @100VAC Input Current is 2.5Amps @load max Output Power: this power supply provides up to 30 watts of DC output power Output Voltage & Current: 12VDC@2.5Amps **PoE Option:** **OS-LS-6212P:** Input Voltage: 100~240VAC Frequency: 50Hz~60Hz. Input Current will be 3.3amps (rms) max. Output Power: this power supply provides up to 130 watts of DC output power Output Voltage & Current: 12VDC@2.5Amps and 48VDC@2.7Amps maximum **OS-LS-6224P (PoE based):** Input Voltage: AC 100~240V Frequency: 50Hz~60Hz. Input current will be less than 2.9A(rms) at 100VAC(rms) / 60Hz. Input current will be less than 1.3A(rms) at 230VAC(rms) / 50Hz. Output Power: the power supply provides up to 225 watts of DC output power maximum Note: the available output power is 180watts Output Voltage & Current: 12VDC@3.75Amps and 50VDC@3.6Amps maximum Minimum efficiency: 85% **OS-LS-6248P (PoE based):** Input Voltage: 100~240VAC Frequency: 50Hz~60Hz. Input Current: 8 Amps maximum Output Power: the power supply provides up to 465 watts of DC output power maximum Note: the available output power is 375watts Output Voltage & Current: 12VDC/7.5Amps and 50VDC/7.5Amps maximum Minimum efficiency: 85%

	The main P/S fail-over to the backup P/S is transparent to the users and without a reboot of the switch. The fail-over time is negligible.
The **Backup** Power Supply Options **• OS-LS-62BP (126 Watt)** **• OS-LS-62BP-DC (100 Watt)** **• OS-LS-62BP-P (510 Watt)**	The OmniStack LS 6200 switch supports an external backup power system. **Backup Power Supply (BPS)** **OS-LS-62BP (126W): OS-LS-6200 modular AC backup power supply. Provides backup power to one non-PoE switch. Ships with chassis connection cable and country specific power cord.** **Non-PoE Option: OS-LS-6212, OS-LS-6224, OS-LS-6224U, and OS-LS-6248** Input Voltage: 100~240VAC Frequency: 50Hz~60Hz. Input current will be less than 1.8A (rms) at 115Vac (rms) and 60Hz. Input current will be less than 0.9A (rms) at 230Vac (rms) and 50Hz. Output Power: this power supply provides up to 126 watts of DC output power Output Voltage & Current: 12VDC@10.5Amps Minimum efficiency: 75% **OS-LS-62BP-P (510W): OS-LS-6200 modular AC backup power supply. Provides backup power to one OS-LS-6200 PoE capable switch.** **Ships with chassis connection cable and country specific power cord.** **PoE Option: OS-LS-6212P, OS-LS-6224P & OS-LS-6248P (PoE based)** Input Voltage: AC 100~240V Frequency: 50Hz~60Hz. Input current will be less than 10A(rms) at 115VAC(rms) and 60Hz. Input current will be less than 5A(rms) at 230VAC(rms) and 50Hz. Output Power: the power supply provides up to 510 watts of DC output power maximum Note: the available output power is 380watts Output Voltage & Current: 12VDC@10.8Amps and 50VDC@7.6Amps maximum Minimum efficiency: 75% **OS-LS-62BP-DC (100W): DC-to-DC Optional Backup Power Supply** **OS-LS-6200 modular DC backup power supply. Provides backup power to one non-PoE switch. Ships with chassis connection cable.** **Non-PoE Option: OS-LS-6212, OS-LS-6224, OS-LS-6224U, and OS-LS-6248** Input Voltage: 40 to 72VDC (Nominal input voltage is expected to be 48Vdc) Input current will be 3.2A Max. at 40Vdc. and 1.8A Max. at 72Vdc Output Power: this DC-to-DC power supply option provides 100 watts of DC output power Output Voltage & Current: 12VDC@8.3Amps Minimum efficiency: 85%
Backup Power Supply Cable Length	The Backup Power Supply cable from the BPS to the switch is 2 meters.
The internal AC-to-DC Main Power Supply **PoE** Parameters	**The main Power Supply maximum PoE Output parameters:** OS-LS-6200 PoE models support IEEE 802.3af standard Default: Max 15.4 watts per port per IEEE 802.3af standard OS-LS-6212P: 75 watts (PoE Power budget) available for PoE power 75watts/12 ports = max 6.25 watts simultaneously available for PoE power per port OS-LS-6224P: 180 watts (PoE Power budget) available for PoE power 180watts/24 ports = max 7.5 watts simultaneously available for PoE power per port OS-LS-6248P: 375 watts (PoE Power budget) available for PoE power 375watts/48 ports = max 7.8 watts simultaneously available for PoE power per port
Maximum Power Consumptions	OS-LS-6212: 26.2 W OS-LS-6212P: 135W max OS-LS-6224: 33.1W OS-LS-6224P: 225W max OS-LS-6248: 51.5W OS-LS-6248P: 465W max OS-LS-6224U: 54W Note: The estimated power consumption figures already include the P/S 85% efficiency.
Power plug type	North America: NEMA 5-15-P (US), C22.2, No. 42 (Canada) United Kingdom / Ireland: BS 1,363, Europe: CEE 7/7 Japan: JIS 8,303, Australia: AS 3,112, India: BS 546, Italy: CIE 2,316 Switzerland / Liechtenstein: SEV 1011 Denmark / Greenland: SRAF 1,962 / D816 / 87, Argentina: AR1-10P
Electrical Requirements	OmniStack switch has the following general electrical requirements: • Each switch requires one grounded AC power source for each power supply installed. • Grounded AC power source must be 110V for North American installations (220V international). • Each supplied AC power cord is 2 meters (approximately 6. 5 feet) long. Do not use extension cords. Redundant Circuit Recommendation: If possible, it is recommended that the main and back up power supplies be plugged into AC sources on separate circuits. With redundant AC, if a single circuit fails, the switches back up power supply (on a separate circuit) will likely be unaffected and can therefore continue operating.

Heat Dissipation	The heat dissipation per unit is depended on the chassis configuration. Be sure to distinguish between the “maximum heat dissipation”, and the “actual heat dissipation” figures per your environmental requirements. **(1 watt ~ 3.41214 BTU/hr.)** **The maximum heat dissipation:** OmniStack LS 6200 chassis (OS-LS-6212 & OS-LS-6212P): Total maximum system power consumption: 26.2 watts Total maximum heat dissipation per this specific configuration: 26.2 watts x 3.41214 BTU/hr. = **89.39 BTU/hr.** OmniStack LS 6200 chassis (OS-LS-6224 & OS-LS-6224P): Total maximum system power consumption: 33.5 watts Total maximum heat dissipation per this specific configuration: 33.5 watts x 3.41214 BTU/hr. = **114 BTU/hr.** OmniStack LS 6200 chassis (OS-LS-6248 & OS-LS-6248P): Total maximum system power consumption: 51.5watts Total maximum heat dissipation per this specific configuration: 51.5 watts x 3.41214 BTU/hr. = **176 BTU/hr.** OmniStack LS 6200 chassis (OS-LS-6224U): Total maximum system power consumption: 54watts Total maximum heat dissipation per this specific configuration: 54 watts x 3.41214 BTU/hr. = **184.25 BTU/hr.**
Safety	The OmniStack LS 6200 is certified with: ▪ CSA/NRTL o UL 60950 o CSA 22.2 No. 60950 ▪ TUV/GS (EN60950) ▪ CB (IEC 60950) ▪ CE Mark
Electrostatic Discharge (ESD)	The chassis has been thoroughly tested to withstand ESD test voltage conditions at any point on the enclosure using the test setups and conditions in accordance with IEC 61000-4-2 (EN61000-4-2).
Electromagnetic Compatibility / EMC	The OmniStack LS 6200 is certified with the following standards: CE Marking per EMC Directive CE Mark: ▪ EN50081-1: o EN55022 Class A ▪ EN50082-1: o IEC 1000-4-2/3/4/5/6/8/11 ▪ EN55024: 1998 ▪ EN60555-2 Class A ▪ EN60555-3 FCC Part 15 (CFR 47) Class A VCCI -V3/97.04, Class A
Environmental	The OmniStack LS 6200 complies with the following standards: Operating Temperature: Operating: 0 to 45°C (32 to 113 °F) Storage: -40 to 70 °C (-40 to 158 °F Humidity: 5%to 95%(Non-condensing) Vibration: IEC 68-2-36,IEC 68-2-6 Shock: IEC 68-2-29 Drop: IEC 68-2-32
Environment compliancy	• RoHS - Restriction on Hazardous Substances in Electrical and Electronic Equipment • WEEE - Waste Electrical and Electronic Equipment
Acoustic Noise	Less than 50dBa
Warranty, Service & Support Chassis and power supplies are protected with a limited lifetime hardware warranty. Warranty is limited to the original owner, and will be provided for up to five years after the product’s End-of-Sales announcement. Faulty parts will be replaced via a five-business day AVR (Advance Replacement) RMA.	**Lifetime Limited Warranty:** Limited to the original owner, and will be provided for up to five years after the product’s End-of-Sales announcement. Faulty parts will be replaced via a five-business day AVR (Advance Replacement) RMA. **SupportBasic:** One year 7x24 phone support, includes eService web access and free software releases **SupportPlus:** One year 7x24 phone support, includes eService web access, free software releases and next business day arrival of replacement hardware **SupportTotal:** (Available only in N. America) One-year 7x24 phone support, software releases, eService Web access, same day 4-hour on site hardware replacement (labor and parts) 7 days a week, 24 hours a day. Excludes NMS and Authentication Services software. Please contact your local Alcatel.Lucent sales representative for additional service and support information.

OmniStack LS 6200 Series – Features Overview

The OmniStack LS 6200 provides wire rate layer-2 forwarding and advanced layer 2-4 services. The OS-LS-6200 supports advanced quality of service and security for outstanding voice and video quality in a secure environment with its advanced user and traffic classification capabilities. On the hardware side the OS-LS-6200 supports 12, 24 and 48-port configurations of Fast Ethernet ports (with or without PoE). In addition to the Fast Ethernet ports, every OS-LS-6200 switch comes complete with two 10/100/1000 copper ports that can be used with standard Ethernet cabling for fault-tolerant dedicated stacking links or as normal Gigabit ports in a standalone configuration. Each OS-LS-6200 switch also comes with two additional Gigabit capable combo ports that provide Gigabit speed capable ports for connectivity upstream into the network or to high-speed servers. Combo ports provide the user the ability to attach via standard copper Ethernet cabling or fiber using industry standard optical transceivers. Alcatel.Lucent provides Lifetime Limited Warranty with this switch to the original owner, and will be provided for up to five years after the product's End-of-Sales announcement.	
The OmniStack 6200 series supports seven platforms:	• OS-LS-6212 – Ethernet based switch with 12 RJ-45 10/100Base-TX ports, two Gigabit combo uplink ports (with SFP or 10/100/1000Base-TX interfaces) and two ports full-duplex Gigabit stacking • OS-LS-6212P – Ethernet based switch with 12 RJ-45 10/100Base-TX ports providing standard-based Power over Ethernet, two Gigabit combo uplink ports (with SFP or 10/100/1000Base-TX interfaces) and two ports full-duplex Gigabit stacking • OS-LS-6224 – Ethernet based switch with 24 RJ-45 10/100Base-TX ports, two Gigabit combo uplink ports (with SFP or 10/100/1000Base-TX interfaces) and two ports full-duplex Gigabit stacking (optional DC power source) • OS-LS-6224P – Ethernet based switch with 24 RJ-45 10/100Base-TX ports providing standard-based Power over Ethernet, two Gigabit combo uplink ports (with SFP or 10/100/1000Base-TX interfaces) and two ports full-duplex Gigabit stacking • OS-LS-6248 – Ethernet based switch with 48 RJ-45 10/100Base-TX ports, two Gigabit combo uplink ports (with SFP or 10/100/1000Base-TX interfaces) and two ports full-duplex Gigabit stacking (optional DC power source) • OS-LS-6248P – Ethernet based switch with 48 RJ-45 10/100Base-TX ports providing standard-based Power over Ethernet, two Gigabit combo uplink ports (with SFP or 10/100/1000Base-TX interfaces) and two ports full-duplex Gigabit stacking • OS-LS-6224U – Ethernet based switch with 24 100Base-FX external SFP ports, two Gigabit combo ports with associated Mini-GBIC slots or RJ-45 ports and two 1000Base-T stacking ports All devices have a management port, which is used for debugging and management purposes. This switch provides a broad range of features for switching. It includes a management agent that allows you to configure the features listed in this manual. The default configuration can be used for most of the features provided by this switch. However, there are many options that you should configure to maximize the switch's performance for your particular network environment.
Software Releases	Software Releases: GA Release 1.0.0.38 and Subsequent Releases: 1.0.1.14 & 1.0.1.23 & 1.0.2.36
Memory Requirements	OmniSwitch 6200 Release 1.0.1.23 requires 128 MB of SDRAM. This is the standard configuration shipped on all OS-LS-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.
The OmniStack LS 6200 positioning	Enterprise workgroups / LAN wiring closets Edge deployments and branch offices Ubiquitous power over Ethernet Edge devices for content rich Ethernet-based services to the unit
The OmniStack LS 6200 Switch Processing Scheme	Supports store-and-forward forwarding scheme & wire-speed layer-2 switching
The MAC Address Table	Support up to 8K MAC address entries, aging and static MAC addresses
Buffer Architecture	Supports up to 16MB Buffers
Flash memory & SDRAM	16M Flash memory & 128MB SDRAM
Packet memory	6MB per Packet Processor
CPU Type	OS-LS-6224/24P & OS-LS-6248/48P: The MPC8247 CPU (266 MHz) w/100M SDRAM Clock OS-LS-6212/12P & OS-LS-6224U: The MPC8248 CPU (266 MHz) w/100M SDRAM Clock
Network Interfaces	
Data rate	10Mbps / 100Mbps / 1000 Mbps (triple speed) and 1000Mbps full-duplex
Jumbo Frames **4.1.7**	The switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames up to 9000 bytes. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields. To use jumbo frames, both the source and destination end nodes (such as a computer or server) must support this feature. Also, when the connection is operating at full duplex, all switches in the network between the two end nodes must be able to accept the extended frame size. And for half-duplex connections, all devices in the collision domain would need to support jumbo frames. Enabling jumbo frames limits the maximum threshold for broadcast storm control to 64 packets per second.
User Ports/Interfaces OS LS 6200: 12 or 24 or 48 10/100BaseT RJ-45 ports on the front panel. Each copper port is capable of auto-MDI/MDI-X sensing.	12, 24 and 48 x 10//100BaseT RJ-45 ports plus 2 10/100/1000BaseT (for stacking or user ports) + 2 combo ports. Combo ports consist of 2 additional 10/100/1000BaseT RJ-45 ports, plus 2 MiniGBIC ports. Combo ports either can be used on a one-for-one basis. Each RJ-45 port is capable of auto-MDI/MDI-X sensing. The 10/100/1000BaseT ports will operate in full/half duplex mode when the

	speed is 10/100Mbps. When operating in 1000Mbps only full duplex mode is supported The 10/100/1000BASE-T ports support auto-sensing, and auto-negotiation. Auto-negotiating 10/100/1000 ports automatically configure port speed and duplex settings Auto MDI/MDIX automatically configures transmit and receive signals to support straight through and crossover cabling for connection to various network devices
MDI/MDIX Support	The device automatically detects whether the cable connected to an RJ-45 port is crossed or straight through. 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 also supported. Port advertisement allows the system administrator to configure the port speed and duplex advertised.
Uplink capabilities (Combo ports)	• OS LS 6200: Two Gigabit Ethernet SFP (mini-GBIC) plus two 10/100/1000 RJ-45 combo ports are located on the front panel. Users determine whether the mini-GBIC or 10/100/1000 ports will operate. The mini-GBIC ports support full duplex mode only. • SFP (mini-GBIC) ports support 100Base FX fiber optic transceivers for 100mb fiber connectivity
Stacking ports	• OS LS 6200: Two 10/100/1000 copper RJ-45 ports. OS LS 6200 supports a fault tolerant looped stacking configuration. In a standalone configuration, these ports can be used as normal network ports.
Indicators	• LEDs per port: • 10/100: link/activity, PoE power • Combo: Link/activity • 10/100/1000: Link/activity • System LEDs: • OK (Diagnostics) • PWR (Internal power supply status) • FAN (Fan status) • TEMP (Over-Temp.) • RPU (Backup power status) • Stack (Status)
Gigabit Ethernet Transceivers (SFP MSA) **Compliant with "SFP-MSA", IEEE 802.3z, and hot swappable & hot insertable:**	
SFP-GIG-EXTND	Extended 1000Base-SX Gigabit Ethernet optical transceiver (SFP MSA). Supports multimode fiber over 850nm wavelength (nominal) with an LC connector. Reach of up to 2 km (based on grade and condition of fiber) on 62.5/125 µm MMF or 550m on 62.5/125 µm MMF. Requires SFP-GIG-EXTND or GBIC-GIG-EXTND at the remote termination. [Formerly known as GE-EXTND-SFP]
SFP-GIG-LH40	1000Base-LH Gigabit Ethernet optical transceiver (SFP MSA). Supports single mode fiber over 1310 nm wavelength (nominal) with an LC connector. Typical reach of 40 Km on 9/125 µm SMF.
SFP-GIG-LH70	1000Base-LH Gigabit Ethernet optical transceiver (SFP MSA). Supports single mode fiber over 1550nm wavelength (nominal) with an LC connector. Typical reach of 70 Km on 9/125 µm SMF. [Formerly known as MINIGBIC-LH-70]
SFP-GIG-LX	1000Base-LX Gigabit Ethernet optical transceiver (SFP MSA). Supports single mode fiber over 1310nm wavelength (nominal) with an LC connector. Typical reach of 10 Km on 9/125 µm SMF. [Formerly known as MINIGBIC-LX]
SFP-GIG-SX	1000Base-SX Gigabit Ethernet optical transceiver (SFP MSA). Supports multimode fiber over 850nm wavelength (nominal) with an LC connector. Typical reach of 300m on 62.5/125 µm MMF or 550m on 50/125 µm MMF. [Formerly known as MINIGBIC-SX]
100 FX Ethernet Transceivers	
100Base-FX fiber optic transceiver options supported (Maintenance Software Release) The OmniStack LS 6200 hardware can support 100Base-FX transceivers using the SFP (mini-GBIC) ports. Software support will be provided in a maintenance release.	**SFP-100-LC-MM**: 100BASE-FM short haul multimode 62.5/125µm and 50/125µm fiber, supports distances up to 2km; uses LC connectors, full duplex **SFP-100-LC-SM15**: 100BASE-FS long haul single mode 9/125µm fiber, supports distances up to 15 km; uses LC connectors, full duplex **SFP-100-LC-SM40**: 100BASE-FS long haul single mode 9/125µm fiber, supports distances up to 40 km; uses LC connectors, full duplex
SFP-100-BX20LT	100Base-BX SFP transceiver with an SC type interface. This bi-directional transceiver is designed for use over single mode fiber optic on a single strand link up to 20KM point-to-point. This transceiver is normally used in the central office (OLT) transmits 1550nm and receives 1310nm optical signal
SFP-100-BX20NU	100Base-BX SFP transceiver with an SC type interface. This bi-directional transceiver is designed for use over single mode fiber optic on a single strand link up to 20KM point-to-point. This transceiver is normally used in the client (ONU) transmits 1310nm and receives 1550nm optical signal
SFP-100-LC-MM	100Base-FX SFP transceiver with an LC type interface. This transceiver is designed for use over multimode fiber optic cable.
SFP-100-LC-SM15	100Base-FX SFP transceiver with an LC type interface. This transceiver is designed for use over single mode fiber optic cable up to 15KM.
SFP-100-LC-SM40	100Base-FX SFP transceiver with an LC type interface. This transceiver is designed for use over single mode fiber optic cable up to 40KM.

Availability Features	
Key High Availability Features Supported	• IEEE 802.1w rapid recovery spanning tree allows sub-second failover to redundant link • IEEE 802.1d spanning tree for loop free topology and link redundancy • IEEE 802.1s multiple spanning tree • Fast-forwarding mode on user ports to bypass 30-second delay for spanning tree • Static and 802.3ad dynamic link aggregation that supports automatic configuration of link aggregates with other switches. • Broadcast Storm Control • Redundant 1:1 power **4.4.5** • Redundant Management & Fabric (in a stacking configuration) • Stacking (up to 8 units) • Fault tolerant loop stack topology • Optional DC power based OS LS 6200 chassis (non-PoE models only)
Power Supplies 1:1 backup power	The OmniStack LS 6200 supports one AC-to-DC power supply for primary power and one optional 2nd AC-to-DC or DC-to-DC power supply for backup (N+1 backup hot-swappable & hot insertable optional backup power supply). The Backup Power System—OS-LS-OS6200-BPS Optional DC power based OS6200 chassis (non-PoE models only)
Fans	The following models support three fixed fans: • OS-LS-6248 = Fans • OS-LS-6212P = Fans • OS-LS-6224P = Fans • OS-LS-6248P = Fans • OS-LS-6224U = Fans **The following models use a fan less design:** • **OS-LS-6212 = Fan less** • **OS-LS-6224 = Fan less**
Stacking Topology & Redundancy	Fault tolerant loop stack topology The devices operate in a Ring topology. A stacked Ring topology is where all devices (up to eight units) in the stack are connected to each other forming a circle. Each device in the stack accepts data and sends it to the device to which it is attached. The packet continues through the stack until it reaches its destination. The system discovers the optimal path on which to send traffic.
Management & Fabric Redundancy	In a stacking configuration, one unit acts as a Master proving the main management and fabric switching functionality, while a 2nd unit acts as a backup.
Source learning and 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. It is possible to configure BPDU packets to be flooded, filtered or bridged when STP is enabled.	Source Learning is responsible for creating, updating, and deleting source and destination MAC Address entries in the MAC Address Table. Spanning Tree: • Support of **single STP (IEEE 802.1D)**. The initial convergence time is 45 sec and reconvergence time is also 45 sec per IEEE 802.1D standard • **PortFast**: Fast-forwarding mode is also supported (proprietary mechanism): Fast forwarding mode on user ports to bypass 30 second delay for Spanning Tree • **IEEE 802.1w** Rapid Reconfiguration is supported. The initial convergence time is 45 sec and the reconvergence time is less than 1sec per IEEE 802.1w standard • The wire-speed **IEEE 802.1s**: MSTP (802.1s) is an IEEE standard which allows several VLANs to be mapped to a reduced number of spanning-tree instances. This is possible since most networks do not need more than a few logical topologies. Each instance handles multiple VLANs that have the same Layer 2 topology. IEEE 802.1s per VLAN per Spanning Tree allows L2 load balancing on redundant L2 links (up to 32 MSTP instances are supported)
BPDU bridging Mode / Spanning Tree BPDU Mode	It is possible to configure BPDU packets to be flooded, filtered or bridged when STP is disabled. Spanning Tree BPDU Mode: BPDU Mode can be set to allow BPDU packets to be flooded, filtered or bridged when STP is disabled.
BPDU bridging	BPDU bridging allows customer network BPDUs to be transparently bridged across 6200 provider bridge. BPDU bridging can forward all types of BPDUs, including AOS 1x1 per vlan tagged BPDUs.
Fast Link	STP can take up to 60 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 60 seconds for a device to decide which ports are actively forwarding traffic. Rapid Spanning Tree (RSTP) detects network topologies to enable 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. Packets assigned to various VLANs are transmitted along different paths within MSTP Regions (MST Regions). Regions are one or more MSTP bridges by which frames can be transmitted. The standard lets administrators assign VLAN traffic to unique paths.

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 High bandwidth server connectivity LAG is composed of ports with the same speed, operating at full duplex.	Link aggregation is a way of combining multiple physical links between two switches into one logical link. The aggregate group operates within Spanning Tree as one virtual port and can provide more bandwidth than a single link. It also provides redundancy. If one physical link in the aggregate group goes down, link integrity is maintained. There are two types of aggregate groups: static and dynamic. Static aggregate groups are manually configured on the switch with static links. Dynamic groups are set up on the switch but they aggregate links as necessary according to the LACP. **Two options:** • Static (Cisco EtherChannel compatible) • Dynamic (IEEE 802.3ad-LACP standard) are supported **The following applies to both Static and dynamic implementation:** • Up to eight Aggregated Links may be defined, each with up to eight member ports. • Up to sixteen ports can be defined in LACP. • Only ports of the same type (all FE or all GE) can be members of the same trunk. **Functional Description** The user may aggregate ports into link-aggregation port-groups. Each group is composed of ports of the same speed, set to Full-duplex operations. Ports in a link-aggregation group (LAG), also called an “Aggregated Link” may be of different media types (UTP/Fiber, or different fiber types), provided they are of the same speed. Aggregated Links may be set up manually, by explicit user assignment, or automatically by enabling LACP (Link Aggregation Control Protocol) on the relevant links. In general, except for the obvious necessary changes, an Aggregated Link is treated by the system as a single logical port, in the same manner as any other port in the system. In particular, the Aggregated link has port attributes similar to a “regular” Port – Auto negotiation state, speed, etc.
Link Aggregation and LACP	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, binds and monitors the port binding within the system.
Image Rollback	Supports dual copies of Boot Code, dual copies of Image Code, and dual copies of Configuration
Stacking	
Merging OS6200 Stacks	You cannot merge two OS6200 stacks, unless they are running identical versions of software. Alcatel.Lucent recommends the following steps to merge two separate stacks: 1. Upgrade one or both (if necessary) stacks so they are running the same software. 2. Confirm that both stacks are running the same software with the show versions Privileged Exec command. 3. Connect the two stacks together into one stack. Refer to OmniSwitch 6200 Family Getting Started Guide for cabling guidelines. 4. Use the show stack command to confirm that the stacks have been successfully merged.
Stacking	• **Fully resilient stack, with up to eight (8) units can be stacked** • Support of full duplex links, with 10 Gbps performance • Topology is ring or chain
Stack – Hot Insertion / Removal	Unit can be added or removed from stack, without requiring stack reset.
Resiliency	A single backup unit is supported. In the event of failure of the master unit, the backup unit takes over. The ring topology will fall back to chain topology in the event of failure of a unit, or a link.
Hot-plug	Failure of a unit, hot extraction of a unit, or any stacking link failure causes a topology change, which will be noticed and kept by the Master of the stack. The Master will detect the topology change and will continue to operate the stack normally; it will set all ports of the failed unit(s) to down state – but will keep all port configuration of the failed unit. There will be minimal interruption of service to the master and the slave units that remained connected. During normal operation of the stack, a Unit can be inserted to the stack (or a stacking cable(s) could be reconnected). This would trigger a topology change. The stack will continue to operate normally and will reconfigure the newly inserted unit.
Topology	The Stack Topology can be Ring or Chain. A ring topology is one in which every unit is connected to two other units. A chain topology is one in which two of the units in the stack are connected to a single unit. Support of a chain topology implies that, in the event of failure of one of the units in a stack with a ring topology, the ring topology will fall back to chain topology. There will be no service interruption to the stack. This advantage is possible, due to the duplex stacking links.
Stacking Port	Two 10/100/1000Mbps RJ45 ports are used as stacking port. They are indicated as “Down” and “Up”. The “Down” is for transmitted the traffic and stack management information to the next unit within the stack. While the “Up” port is for receiving the traffic and stack management information from another units in the stack.
Firmware & Configuration Files	
Dual software images	Two firmware images are locally stored on the switch; in the event a firmware upload becomes corrupted the user has a mechanism to revert to the last known good firmware file.
Software upgrades via TFTP	RFC1350; support for firmware upgrades through TFTP
Static assignment of IP addresses	Support for the assignment of static IPv4 IP address to the switch. User can select IP address management method (Static / BootP / DHCP). User can define static IP address, subnet mask and gateway. Recommended maximum number of IP addresses: five (four in-band + one out-of-band)
Configuration uploads and downloads via TFTP	Configuration can be uploaded and downloaded via TFTP

Serial port to support CLI	Out-of-band serial port delivers CLI management interface for local configuration of switch
Security	
Key Security Features Supported	**Advanced Security** • 802.1x port based user authentication with multiple host mode • 802.1x multi-client, multi-VLAN support for per-client authentication and VLAN assignment • 802.1x MAC authentication • 802.1x Multiple Sessions • Transparent 802.1x BPDU Forwarding • Private VLAN edge or port mapping • Guest VLAN provides limited network access for unauthorized clients • MAC addr. Lockdown allows only known devices to have network access preventing unauthorized network device access includes lockdown after a user-configured number of MAC addr. have been learned • DHCP Option 82 and DHCP snooping for IP address allocation control and protection • IP Source Guard and Dynamic ARP Inspection • RADIUS and TACACS+ admin authentication prevents unauthorized switch management **4.1.2** • Secure Shell, Secure Socket Layer and SNMPv3 for encrypted remote management communication • Access control lists to filter out unwanted traffic including denial of service attacks • Access control lists (ACLs) are per port, MAC SA/DA, IP SA/DA, ICMP type and code, Ethertype, TCP/ UDP port **4.4.7** • STP root guard prevents an unauthorized device from becoming the root of a spanning tree. • STP BPDU guard is used to protect the network from invalid configurations.
Local authentication	Authentication support for storing a local password database on the switch for local authentication
Advanced port-based and user-based authentication	Advanced port-based authentication also enables user-based authentication. Specific VLANs in the device are always available, even if specific ports attached to the VLAN are unauthorized. For example, Voice over IP does not require authentication, while data traffic requires authentication. VLANs for which authorization is not required can be defined. Unauthenticated VLANs are available to users, even if the ports attached to the VLAN are defined as authorized. Advanced port-based authentication is implemented in the following modes: ▪ Single Host Mode — Only the authorized host can access the port. ▪ Multiple Host Mode — Multiple hosts can be attached to a single port. Only one host must be authorized for all hosts to access the network. If the host authentication fails, or an EAPOL-logoff message is received, all attached clients are denied access to the network. ▪ Guest VLANs — Provides limited network access to authorized ports. If a port is denied network access via port-based authorization, but the Guest VLAN is enabled, the port receives limited network access. For example, a network administrator can use Guest VLANs to deny network access via port-based authentication, but grant Internet access to unauthorized users. ▪ Unauthenticated VLANS — Are available to users, even if the ports attached to the VLAN are defined as unauthorized.
Access Control Lists (ACLs) L2/L3/L4 ACLs User can setup ACLs based upon L2/3/4 information that can allow/deny based upon the packet header content.	ACLs are a general mechanism to inspect incoming frames and classify them into named logical groups based on various criteria. Each such group may have specific actions that are carried out on each frame classified as a member of that group. ACLs are used for two main purposes: • As a security mechanism, either permitting or denying entry (hence the name Access Control) for frames in a group • As the mechanism to classify (assign) frames into “traffic classes” for which various “Class-of-service” handling actions are to be carried out; This is the classification mechanism which is used in Advanced-mode QoS configuration **IP ACL Classification:** The classification part of the IP ACL identifies flows by any combination of the following fields: • Protocol • Source IP address with wildcard • Destination IP address with wildcard • DSCP. Can be defined as IP precedence • For UDP/TCP: o Source port o Destination port • For ICMP packets: o ICMP code o ICMP type • For IGMP packets o IGMP type **MAC Access Lists:** The MAC lists would support the following fields: • Source MAC address with wildcard • Destination MAC address with wildcard • VLAN • User Priority

	• Ethernet type • Inner VLAN **ACL Actions:** The action part can be one of: • Forward – packet is sent to its destination • Drop – packet is dropped silently • Drop and disable ingress port – packet is dropped, the ingress port is disabled for all incoming and outgoing packets. A notification is sent to the user on terminal, WEB, SNMP, log file. Port can become active again only as a result of user configuration.
IP ACL Classification	**What it is** • Adding wildcard bits to the source port and destination port to classify a range of TCP or UDP ports in the IP ACL **How to use it** • Use ones (1) in the bit position that you want to be ignored • Example o Configure IP ACL to classify packets with destination TCP port range from 80 to 95: o console(config)# ip access-list acl o console(config-ip-al)# permit-tcp any any any 80 dst-port-wildcard 000f • Note: 80 (0x01010000); 95 (0x01011111); wildcard is 0x00001111 (hex 0f) • Show the IP ACL configuration: o console# show access-lists • IP access list acl o permit tcp any any any 80 dst-port-wildcard 000f
Secure Shell (SSHv2) /(SSHv2/Secure Telnet) **4.1.2**	The SSHv2 (embedded SSH client and server) secures management traffic between the client(s) and Switch, or Switch to Switch. The SSH leverages well-known transport and encryption technologies for secure communications and it ensures the network management traffic and events are securely exchanged. 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 un-trusted hosts or over an un-secure network. The OmniStack LS 6200 includes both client and server components of the Secure Shell interface and the Secure Shell Telnet protocol (This feature is implemented to provide security for TELNET transmissions only through encryption). STELNET is a subsystem of the Secure Shell protocol. All Secure Shell TELNET data are encrypted through a Secure Shell channel. Support for Secure Shell (SSH): The switch supports both SSH Version 1.5 and 2.0. The OmniStack LS 6200 supports the OpenSSHv2 client / server implementation and it supports the following types of encryptions: AES, Triple DES (3DES), Blowfish, CAST128, and ARCFOUR
Secure Socket Layer (SSL) with encryption (SSL/HTTPS)	SSL is a protocol that establishes and maintains secure communication between SSL-enabled servers and clients across the Internet. It secures communications to or from the switch for the web-based management.
MAC-Based Port Security (Locked Port) 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.	This feature is used to increase security by limiting access on a specific port only to users with a specific MAC addresses. These addresses are either manually defined on the port, or learned on that port up to the point when it is “locked”. When a frame is seen on a locked port, and the frame’s source MAC address is not tied to that port (either it is learned on a different port, or unknown to the system) the protection mechanism is invoked and can provide various handling options. Support for learning MAC addresses and then disabling learning to effectively lock the MAC addresses that have access to the network. Port lock is supported using controlled learning. Packets received on a locked port, whose source address was not found or previously learned on a different port, are treated in one of the following ways, which can be configured per port: • Forward (Frame is forwarded, but its address is not learned) • Discard • Discard and send an SNMP trap Support for learning a user configured number of MAC addresses on any particular port
MAC-Based Port Security by Number of MACs	This feature is used to increase security by limiting access on a specific port to a user-defined limited number of hosts. These addresses are learned on that port up to the point when it is automatically “locked”, because the maximum number has been reached. When a frame is seen on a locked port, and the frame’s source MAC address is not tied to that port (either it is learned on a different port, or unknown to the system) the protection mechanism is invoked and can provide various handling options.
IEEE 802.1x Port Based Authentication Port based authentication enables 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).	The system implements 802.1x Port Based Authentication as per the standard, in conjunction with an Authentication Server (RADIUS). The authentication server authenticates, using AAA services or RADIUS, each client must be connected to a switch port before any communication (except EAPOL traffic) can take place. The status of the controlled port is a function of the communication between the authentication server and the supplicant. In addition, the user can modify this status. In addition, any access to the LAN is subject to the status of the MAC associated with the port. The switch makes use of the uncontrolled port to communicate with the host attached to the network, using EAPOL protocol exchanges, and communicates with the authentication (RADIUS) server using EAP. EAP types supported for the 802.1X authentication: MD5, PEAP, EAP-TLS, EAP-TTLS

802.1x - MAC Authentication	**What it is** 802.1x port can not allow access for printers or IP phones that do not have the 802.1x supplicant capability MAC authentication allows user to enable authentication based on the station's MAC address including the devices like printers and IP phones **How to use it** A port must be a member of a guest VLAN Re-authentication must be enabled on the port Must enable "dot1x port-control auto" mode on the port User can enable the MAC Authentication on the port in one of two modes: MAC Only (only MAC Authentication is enabled) MAC + 802.1x (In that case 802.1x takes precedence)* Once authenticated - the port will be taken out from the guest VLAN and will be assigned the port's VLAN values Note 1: Static MAC addresses can not be authorized Note 2: Do not change an authenticated MAC to static address * Client will be authenticated by 802.1x first, then Mac-authentication **Functional Description** 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. To support MAC authentication, the RADIUS authentication server maintains a database of MAC addresses for devices that require access to the network. In order for the feature to be active, 802.1x must be in auto-mode. User then can enable the MAC authentication feature in one of two modes: • MAC Only – Where only MAC authentication is enabled • MAC + 802.1x (In that case 802.1x takes precedence) The feature can be enabled per port. The port must be a member of a guest VLAN prior of activating the feature. (Once the feature is activated and a user is authenticated, the port is taken out the guest VLAN and gets the assigned port's VLAN values). **User Controls** • It is possible to configure MAC authentication on a port. • It is possible to configure MAC authentication + 802.1x on a port. **References, Notes and Limitations** • Refer to notes on 802.1x • Static MAC addresses cannot be authorized. • It is not recommended to change an authenticated MAC to static address. (S/W does not prevent this from happening, currently) • It is not recommended to delete authenticated MAC addresses. (S/W does not prevent this from happening, currently) • Host mode is still defining whether the MAC authentication will be working in a single or multiple modes. (It is recommended to work in a single mode) • Re-authentication always work when enabling this feature • Statistics will be the same as for 802.1x
802.1x – Enhanced Features 802.1x, incl. unauthenticated VLAN & single/multiple host • Standard 802.1x is supported, using external RADIUS server as authenticator. • Unauthenticated VLAN and single/multiple host are supported, using controlled learning. • Guest VLAN is supported.	The following 802.1x feature enhancements described in this section are supported: **Single-host/Multiple-hosts:** Single-host mode enables only the host that has been authorized to get access to the port. Filtering is based on the source MAC address. Multiple-hosts mode enables multiple hosts to be attached to a single 802.1X-enabled port. In this mode, only one of the attached hosts must be authorized for all hosts to be granted network access. If the port becomes unauthorized (re-authentication fails or an EAPOL-logoff message is received), all attached clients are denied access to the network. **Multiple Sessions:** "Multiple sessions" mode enables number of specific hosts that has been authorized to get access to the port. Filtering is based on the source MAC address. **Guest VLAN:** Network administrators may want to give some limited access to the network when the port is unauthorized. Typical applications are: • In some installations there is a requirement that management traffic would be allowed to an unauthorized stations. • In some enterprises there is a requirement to give guests an access to the Internet through the enterprise network. Solution: One of the VLANs in the switch would be the "guest VLAN". The "guest VLAN" would be the "untagged" VLAN of ports in the unauthorized state. The administrator would be able to use this VLAN for guests, or to manage stations that are currently not authorized. The VLAN would be defined with limited access. Guest VLAN can be enabled or disabled system-wide. **Unauthenticated VLANs:** There is requirement that some VLANs in the switch would always be available, even if the port were unauthorized. Typical applications are: • Some types of traffic might not require 802.1x authentication. E.g. IP telephony might not require authentication while data traffic requires.

	Solution: The administrator would be able to define VLANs that authorization is not required for them. Those VLANs would be always available to users, even if the port were unauthorized. These VLANs are defined as “Unauthenticated” VLANs.
802.1x – Multiple Sessions support	**What it is** • 802.1x now supports Multiple Sessions in addition to Single-host and Multiple-hosts o Single-host: only grant access to ONE host that has been authorized o Multiple-hosts: multiple hosts that are attached to a single 802.1x-enabled port will ALL be granted network access as long as one of the attached hosts is authorized o Multiple Sessions: enable number of specific hosts that have been authorized, to get network access (and deny others…) – All authenticated users are classified in the same Vlan on the port • Multiple Sessions Filtering is based on the source MAC address **How to use it** • Must enable dot1x port-control mode to “auto” • System is set to dot1x single-host mode by default • Use “dot1x multiple-hosts authentication” command to enable this feature • Note: command “dot1x multiple-hosts” w/o “authentication” means to enable Multiple Hosts only, which will grant all hosts the network access once one host is authenticated
Transparent 802.1x BPDU forwarding	**What it is** • According to IEEE802.1 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 802.1x BPDU flooding, under user control, to bridge 802.1X BPDUs packets as data packets. **How to use it** • The feature can be enabled only when 802.1X is globally disabled (by the no dot1x system-auth-control global configuration command) • If the port is disabled for 802.1X but 802.1X is enabled globally, 802.1X BPDUs would always be discarded. **802.1X BPDU forwarding description** According to IEEE802.1 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, under user control, to bridge 802.1X BPDUs packets as data packets. The feature can be enabled only when 802.1X is globally disabled (by the no dot1x system-auth-control global configuration command). **User Control:** Enable/Disable 802.1X BPDU flooding. **References, Notes and Limitations** The feature can be enabled only when 802.1X is globally disabled (by the no dot1x system-auth-control global configuration command). If the port is disabled for 802.1X but 802.1X is enabled globally, 802.1X BPDUs would always be discarded.
DHCP Snooping	**What it is** ▪ DHCP snooping is a DHCP security feature that provides o network security by filtering untrusted DHCP messages and o by building and maintaining a DHCP snooping binding database 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 **How to use it** ▪ The administrator has the following controls for enabling/disabling the feature: o Global: enable/disable o Per VLAN: enable/disable ▪ Trusted interfaces are connected to DHCP servers or to switches/hosts that DHCP packet filtering is not required to trust ▪ Untrusted interfaces are connected to untrusted hosts ▪ By default, all interfaces are untrusted when DHCP snooping is enabled. Note: In order to enable DHCP snooping on a VLAN, you must enable DHCP snooping on the switch **Functional Description** 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. **User Controls** The administrator has the following controls for enabling/disabling the feature: • Global enable/disable of the feature. • Per VLAN enable/disable of the feature.

	• The administrator identifies trusted ports • The administrator can determine if to forward or filter DHCP packets, received from untrusted interfaces that the source MAC address and the DHCP client hardware address do not match. (Global setting) • The administrator can determine if to forward or filter DHCP packets, received from untrusted interfaces, with option-82 information • The administrator globally enables the DHCP snooping binding database. • The administrator can manually add and delete entries to the database. After adding an entry, the entry would be added to the DHCP snooping database and to the binding file, if exits. The entry would not be added to the configuration files. The entry would be displayed in the show commands as a “DHCP Snooping (s)” entry. • The administrator can define a manually added entry to be either a dynamic or a static address. When configuring a dynamic address, an expiration date must be assigned to the entry. Time is defined in seconds (10 – 4294967295) • The administrator can define the refresh time (in seconds) of the binding table. Default is 1200 seconds. Range is 600 – 86400 seconds. **References, Notes and Limitations** Enabling DHCP Snooping requires use of TCAM rules. (Per VLAN) (If no TCAM entries are available, the user will get a proper notification).
DHCP Option 82	**What it is** ▪ In residential, metropolitan Ethernet-access environments, DHCP server can centrally manage the IP address assignments for a large number of subscribers ▪ When the DHCP option-82 feature is enabled on the switch, a subscriber is identified by the switch port through which it connects to the network (in addition to its MAC address) ▪ Multiple hosts on the subscriber LAN can be connected to the same port on the access switch and are uniquely identified ▪ If DHCP Option 82 is enabled, the switch adds Relay agent information option (option-82) to messages sent to DHCP server from clients connected to untrusted ports ▪ In DHCP replies from the server, the switch verifies that the server inserted the option-82 data (by inspecting the remote ID and possibly the circuit ID fields), then removes option 82, and forwards the reply only to the relevant port according to the information in option 82. ▪ This feature enables user to control which ports will allow DHCP dynamic configurations on connected PCs **How to use it** ▪ The administrator can globally enable/disable DHCP snooping option 82 ▪ The DHCP snooping option 82 is enabled only on DHCP snooping enabled VLANs **Functional Description** Relay agent information option (option-82) in the DHCP protocol enables a DHCP relay to send the port number of a client, that request an IP address. The Relay agent information option specifies the port number from which the client’s packet was received. The provider switch, when working as a DHCP relay agent, can support this feature. Also DHCP snooping that trap DHCP messages, and add Relay agent information option (option-82) can be implemented. **4.1.5** The option-82 information is the switch MAC address (the remote ID sub-option) and the port identifier, vlan-mod-port, from which the packet is received **User Controls** DHCP relay or DHCP snooping can be enabled on a VLAN. Relay agent information option (option-82) can be enabled on a VLAN. **References, Notes and Limitations** If DHCP relay or DHCP snooping are enabled on a VLAN, and Relay agent information option (option-82) is also enabled on the VLAN, the switch adds Relay agent information option (option-82) to messages from clients to DHCP server. In replies from the DHCP server, the switch removes option 82, and forwards the reply only to the relevant port according to the information in option 82 (Adds security advantage for IP clients that require broadcast answers, by limiting the broadcast to the client’s port).
IP Source (Address) Guard	**What it is** ▪ IP source guard is a security feature that restricts IP traffic on Layer 2 interfaces by filtering traffic based on: o DHCP snooping binding database o 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 ▪ When IP source guard (source IP address filtering) is enabled on a port: o Only traffic with a source IP address that is associated with the port is permitted o Non IPv4 traffic: Permitted (Including ARP) o IP traffic is filtered based on its source IP address as well as its MAC address. o Note: An IP address can be associated with a port as a result of DHCP snooping, or as a result of manual configuration by the administrator **How to use it** ▪ IP source guard can be enabled only on DHCP snooping untrusted interface

	▪ IP source guard can be enabled with source IP address filtering or with source IP and MAC address filtering. **Functional Description** 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. IP source guard can be enabled only on DHCP snooping untrusted interface. IP source guard can't be configured on routed ports. If IP source guard is enabled on a port then: ▪ DHCP packets allowed by DHCP snooping are permitted. ▪ If source IP address filtering is enabled: o IPv4 traffic: Only traffic with a source IP address that is associated with the port is permitted. o Non IPv4 traffic: Permitted Note: An IP address can be associated with a port as a result of DHCP snooping, or as a result of manual configuration by the administrator. **User Controls** IP Source Guard can be enabled on an interface (port or LAG) and globally. The user can see the list of inactive addresses. The user can set the system to automatically try and activate inactive addresses. (Order will be per IP source guard table) Default is 60 seconds. (Range is 10-600 seconds) If not in auto mode the user can manually try and activate inactive addresses. **References, Notes and Limitations** User must enable DHCP snooping globally and per VLAN in order for IP source guard feature to be activated. When a port is defined as a trusted port, it is possible to configure static IP entries, yet the feature will not work on a trusted port. Only when the port is re-configured to un-trusted port, the filtering will take place. When moving a port from un-trusted mode to trusted, the static IP entries will remain but will the feature will not be active. The user will get a warning message on that. Enabling DHCP Snooping requires use of TCAM rules. (It uses the same lookup used for security and QoS. The number of entries is a multiplication of the security rule by the number of address entries) When the number of entries exceeds the available number of TCAM entries, new address will not be permitted and will be defined as Inactive address. The user can see the list inactive IP addresses. Port security can't be enabled if source IP and MAC address filtering is configured on a port.
Dynamic ARP Inspection (DAI)	**What it is** ▪ 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 ▪ ARP inspection is performed only on ARP untrusted interfaces. o Server port should be configured as a trusted interface **How to use it** ▪ The user can enable/disable globally ARP inspection ▪ The user can enable the feature per VLAN ▪ The switch would perform ARP inspection only to untrusted interfaces ▪ The user can define the maximum number of ARP messages that can be received on an interface ▪ The user can define static ARP binding lists. **Functional Description** ARP provides IP communication within a Layer 2 broadcast domain by mapping an IP address to a MAC address. For example, Host B wants to send information to Host A, but does not have the MAC address of Host A in its ARP cache. Host B generates a broadcast message for all hosts within the broadcast domain to obtain the MAC address associated with the IP address of Host A. All hosts within the broadcast domain receive the ARP request, and Host A responds with its MAC address. However, because ARP allows a gratuitous reply from a host even if an ARP request was not received, an ARP spoofing attack and the poisoning of ARP caches can occur. After the attack, all traffic from the device under attack flows through the attacker's computer and then to the router, switch, or host. A malicious user can attack hosts, switches, and routers connected to your Layer 2 network by poisoning the ARP caches of systems connected to the subnet and by intercepting traffic intended for other hosts on the subnet. **User Controls** The user can enable/disable the feature globally. (DHCP snooping does not need to be activated; in this case, the feature will be active based on static entries only,) The user can enable the feature per VLAN based on DHCP snooping database The user can define trusted/untrusted interfaces (Independent of the trusted/untrusted interfaces defined on DHCP snooping) (ARP inspection is not activated on trusted port) The user can define static ARP binding lists The user can globally configure the system to perform ARP packets header check. (Source MAC field

	in ARP header vs. Source MAC filed in Ethernet header, destination MAC filed will also be checked in ARP reply messages) The user can configure the minimal interval between Syslog messages (Including sending Syslog messages immediately and not to send at all) . Range (in seconds): 0-86400. Default – 5 seconds. (0 – immediate) The user can disable Syslog messaging. Each Syslog message contains: • The receiving VLAN. • The port number. • The source and destination IP addresses • The source and destination MAC addresses. • Date of message. Error type: If it is ARP packet verification error or ARP packet header check error **References, Notes and Limitations** The switch does not check ARP packets that are received on the trusted interface; it simply forwards the packets. For untrusted interfaces: If an ARP static binding list is defined for the packet's VLAN, then search that list if the packet's IP address exists in the list. If the IP address is found and the MAC address in the list matches the packet's MAC address, then the packet is valid. If the IP address is found and the MAC address in the list doesn't match the packet's MAC address, then the packet is not valid. If the packet's IP address was not found in the ARP static binding, and DHCP snooping is enabled for that VLAN then search the DHCP snooping database for the packet's <VLAN - IP address> pair. If the <VLAN - IP address> pair was found, and the MAC address and the interface in the database match the packet's MAC address and ingress interface, the packet is valid. If the packet's IP address was not found in the ARP static binding and in the DHCP snooping the packet is invalid.
Intelligence	
Key Intelligent Features Supported	• **Wire-rate layer-2 forwarding and advanced layer-2 – layer-4 services** • Layer-2 Switching Capacity: o **24-port platforms 6.6 Gbps – 48-port platforms 8.8 Gbps** • Layer-2 Throughput/forwarding rate: o **24-port platforms 9.52 Mpps – 48-port platforms 13.1Mpps** • Store-and-forward mode • Stacking capabilities • Auto MDI/MDIX / Auto MDI/MDIX automatically configures transmit and receive signals to support straight thru and crossover cabling • Auto-negotiation / Auto-negotiating 10/100/1000 ports automatically configure port speed and duplex setting • Duplex mode • Broadcast Strom Control • Head of Line (HOL) Blocking Prevention • Flow Control Support (IEEE802.3X) • Back Pressure Support • Cable Analysis • Optical Transceiver Analysis • Port Controls • MAC Address Support of up to 8K • 255 active VLANs **4.4.6** • 4,094 VLAN tag value support • VLAN-Aware MAC-based Switching • Environmental Monitoring including the Fan Status Support • VLANs, VLAN (802.1Q) Tagging, Private VLAN Edge, Protocol Based VLANs, IP Subnet-based VLANs and MAC-based VLANs, and Port-based VLANs • Per service VLAN stacking (Q-in-Q) • GVRP **4.1.6** • L2 Multicast support including Static Multicast Groups, Multicast VLAN, and IGMP Snooping v1 &2 & 3 o Multicast TV VLAN registration per port for maximum bandwidth efficiency between edge and core. • Packet Storm Control • Spanning Tree o IEEE 802.1d o IEEE 802.1w o IEEE 802.1s o Fast Port

	o BPDU Filtering when STP is disabled o Spanning Tree Protocol (STP) Root Guard o Spanning Tree Protocol (STP) BPDU Guard • System IP Address Management • BootP and DHCP Clients for IP Address Assignments • Jumbo Frames (up to 9000 Bytes) 4.1.7 • Quality of Service Features --- L2/L3/L4 QoS / CoS/QoS Extensive L2/L3/L4 COS/QoS support including Classification, Marking, Mapping, and Rate Limiting To overcome unpredictable network traffic and optimize performance, you can apply Quality of Service (QoS) throughout the network to ensure that network traffic is prioritized according to specific criteria. The switch supports two modes of QoS: basic and advanced. QoS in brief: o 802.1p, TOS, DSCP marking 4.1.8, 4.1.9 o QoS mapping: 802.1p to TOS/DSCP, TOS to 802.1p/DSCP, DSCP to 802.1p/TOS o Classification per port, 802.1p(COS) value, MAC SA/DA, Ethertype, TOS precedence, DSCP value, ICMP code and type, IP SA/DA, IP protocol, TCP/UDP port o Four egress queues per port that support strict and WRR queuing algorithms o Ingress bandwidth rate limiting per port/flow o Egress bandwidth rate limiting per port/queue o Inner VLAN classification o IP ACL Classification
Performance	• Switching capacity: 12.8 Gbps OS-LS-6212/12P/24/24P/24U, 17.6 Gbps OS-LS-6248/48P 4.4.3 • Stacking capacity: 1 Gbps full-duplex per stack port, 4 Gbps aggregate capacity with optimized unicast and multicast forwarding • Wire rate forwarding for 10/100/1000 port speeds, 7.74 Mpps OS-LS-6212/12P, 9.52 Mpps OS-LS-6224/24P, 13.1Mpps OS-LS-6248/48P 4.4.4 • 8 K MAC addresses 4.1.10
Forwarding Modes	The OmniStack LS 6200 provides only the store-and-forward mode for forwarding frames. The entire frame is received and stored in memory before it can be forwarded to the destination port.
User ports	• OS-LS-6200: 12 or 24 or 48-10/100BaseT RJ-45 ports on the front panel. Each copper port is capable of auto-MDI/MDI-X sensing and PoE capability. • OS-LS-6224U: 24 100BaseX fiber ports on the front panel. Each fiber port support external SFP optical transceivers for 100MB fiber connectivity.
Stacking ports	• OS-LS-6200: Two 10/100/1000 copper RJ-45 ports. OS-LS-6200 supports a fault tolerant looped stacking configuration. In a standalone configuration, these ports can be used as normal network ports.
Stacking Support	The OmniStack LS 6200 stack consists of up to eight stackable units. One of the units acts as a stack master, while all other units act as slaves. One of the slaves can also act as a backup stack master. Network managers can remotely manage the entire stack, transparently to the stack topology and the number of units included in the stack. The stack is managed as a single switch. The Stack Topology can be Ring or Chain. A ring topology is one in which every unit is connected to two other units. A chain topology is one in which two of the units in the stack are connected to a single unit.
Combo ports	• OS-LS-6200: Two Gigabit Ethernet SFP (mini-GBIC) plus two 10/100/1000 RJ-45 combo ports are located on the front panel. Users determine whether the mini-GBIC or 10/100/1000 ports will operate. The mini-GBIC ports support full duplex mode only. • SFP (Mini-GBIC) ports support 100Base-X fiber optic transceivers for 100mb fiber connectivity
Auto MDI/MDIX 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).	Normally, Twisted Pair ports must be connected so that the Transmit pair on one end is connected to the Receive pair on the other end, and vice versa. If the cabling is done so that Transmit on one end is wired to Transmit on the other, and Receive is wired to Receive, a link will not be established. Hubs and switches are deliberately wired opposite to the way end stations are wired, so that when a hub or switch is connected to an end station, a "straight through" Ethernet cable can be used, and the pairs will match up properly. When two hubs/switches are connected to each other, or two end stations are connected to each other, a "crossover" cable is used to make sure that the correct pairs are connected. The standard wiring for end stations is known as MDI (Media Dependent Interface), and the standard wiring for hubs and switches is known as MDIX (Media Dependent Interface with Crossover). On certain devices, it is possible for hardware to automatically correct errors in cable selection, making the distinction between a "straight through" cable and a "crossover" cable irrelevant. This capability is known as Auto Cross. Auto MDI/MDIX works only on 10BASE-T/100 BASE-T /1000 BASE-T ports. Auto detection of both crossed and uncrossed cables on all RJ45 ports. This feature is automatically enabled for the entire system.
Auto-negotiation Auto negotiating speed and half/full duplex settings on all ports	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. The device can negotiate for each port configuration of speed, duplex mode and flow control. Each

	port can be configured to perform auto negotiation on speed and duplex modes, as well as on flow control. Flow control can be enabled only if duplex mode is set to full duplex (engineering rule). • The user can configure any or all three capabilities (speed, duplex and flow control) • Speed-duplex capabilities to be advertised can be any combination of the following: 10h, 10f, 100h, 100f, 1000f
Auto Negotiation Advertised Capabilities	Communicates to other switch ports the auto-negotiation capabilities of the port
Duplex mode	A 10/100/1000BASE-T port can be set to work under auto-negotiation mode. The port can negotiate with the partner to determine the operating speed and mode. The port can also be set to a fixed speed and duplex mode (when operating in 10/100 Mbps, the full/half duplex mode is support. When operating in 1000Mbps, the full duplex mode is support only). The 1000BASE-X port always operates in 1Gbps full-duplex modes.
Broadcast Strom Control (BSC)	Broadcast storm control allows a switch to limit switching of broadcast traffic. Since high rates and continuous traffic can cause flooding on the network. The broadcast control mechanism is to prevent the packets from flooding into other parts of the network. The switch will drop any broadcast/multicast traffic received in excess of the threshold. Unicast must continue to be forwarded even as excessive broadcast traffic is being dropped. BSC allows management to control the rate of multi-destination packets, to prevent Denial of Service (DoS) attacks. Control Multicast/Broadcast traffic can still be trapped to the CPU when rate is exceeded. The threshold for the number of broadcast packets that are sent over a port can be set, to prevent broadcast storms. Storm control can be enabled per port, and limitation can be based on: • All frames·Unicast • Multicast • Broadcast only • Any combination
MAC Address Support Static and dynamic MAC entries: Supports the ability to dynamically learn MAC addresses on inbound packets; the user can also enter Static MAC addresses.	The devices support a total of 8K MAC addresses. Note that during the operation of some features (e.g. Trunking, defining routing interfaces) additional MAC addresses may be used internally as part of the normal operation of these features. Note that MAC addresses are stored in the hardware tables based on an internal hashing mechanism. When several different MAC addresses generate an identical Hash result, a hash-collision resolution operation is carried out. **VLAN-Aware MAC-based Switching** The System always performs VLAN-aware bridging. Therefore, the system does not perform pure "classic" bridging as defined in IEEE802.1D, where frames are forwarded based on their destination MAC address only. However, a similar functionality may be configured for untagged frames. Addresses are associated with ports by learning them from the SRC address of incoming frames. **Functional Description** MAC address-based bridging – the device always performs VLAN-aware bridging. When MAC address-based forwarding is desired, all ports should be placed in a single VLAN, and set to Untagged. In this case, untagged frames are accepted and classified to the PVID (port VLAN id). When forwarding has considered this PVID, it will have no effect, as all ports have the same PVID, providing the same functionality as MAC address-based switching. The Packet Processor performs this type of bridging by looking up the destination address and VLAN in an L2 lookup table on the device that receives the frame from the network. The L2 lookup table indicates the exit port(s) for the bridged packet. Note that Tagged frames arriving in this mode will be dropped, unless they are tagged with the PVID value.
IP addresses	Maximum number of IP addresses per system: 5 Maximum number of default gateway per system: 1
Environmental Monitoring	The system hardware contains several sensors that keep track of important Physical attributes of the system. The Software tracks these sensors and reports anomalies to the user so that appropriate action may be taken.
Fan Status	The system will monitor the status of the fans, if they are present. **Functional Description** For each one of the fans the following status will be available: Status OK, Status – Fail Any change is status will generate a user notification (SNMP Trap, log message, console message etc.). This will include any active Telnet sessions, including ones over SSH.
VLANs IEEE 802.1D, IEEE 802.3ac; Switch supports 4096 range (4,094 VLAN tags) VLANs; support for packet tagging following IEEE 802.1Q 256 active VLANs Maximum number of VLANs per system: 256.	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 groups in the same VLAN. A VLAN defines a broadcast domain that contains physical ports and can span across multiple switches. All switches contain a default VLAN#1. Physical switch ports are initially assigned to VLAN#1 until they are statically or dynamically assigned to other VLANs. The VLAN management commands comply with RFC 2674. VLANs support: • Per Port, 802.1Q, MAC, IP Subnet, and Protocol-based VLANs are supported. **4.1.11** • Per Service VLAN Stacking (Q in Q) • Multicast TV VLAN registration per port maximum bandwidth efficiency between edge and core • Full 4K (4,094 VLAN tags) range is supported • 256 active VLANs

	• Policy based (TCAM) VLANs • MAC VLAN: 128 rules • IP Subnet VLAN: 128 rules • Protocol VLAN: 16 rules • VLAN rule precedence 1. MAC 2. IP Subnet 3. Protocol
Port-Based VLANs	Port-based VLANs classify incoming packets to VLANs based on their ingress port.
VLAN Tagging IEEE 802.1Q defines architecture for virtual bridged LANs, the services provided in VLANs, and the protocols and algorithms involved in the provision of these services.	The OmniStack LS 6200 switch supports 802.1Q/p VLAN tagging. VLAN tagging is a method of identifying a packet as a member of a VLAN. VLAN tagging enables you to configure ports on multiple switches into a single VLAN. Using tagged VLANs can ease network management and ensures interoperability with other devices. When a switch sends a packet that is a member of a tagged VLAN, the switch "tags" the packet to indicate its VLAN membership. Other switches that support VLAN tagging recognize the tag and process the packet according to its VLAN membership. 802.1Q VLAN Tagging support allows a user to assign ports to one or more of the 255 VLANs either manually or automatically with GVRP.
GVRP support for VLANs IEEE 802.1D; system supports group VLAN registration protocol for dynamic propagation of VLANs throughout the network GVRP VLAN Registration Protocol (GVRP) provides IEEE 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports. When GVRP is enabled, the switch registers and propagates VLAN membership on all ports that are part of the active underlying Spanning Tree protocol topology.	The OmniStack LS 6200 switch supports GVRP Protocol for VLAN configuration. GVRP (GARP VLAN Registration Protocol), a registration protocol specifically for VLANs. GVRP may be used in end stations and in switches. Using this protocol, stations request admission to specific VLANs. A network management or policy system determines membership in a VLAN, and GVRP helps simplify the administration of VLANs in several ways. It handles registration of end stations with Ethernet switches and maintains current information about membership. The protocol may be used between end stations across a large network. GVRP enables the switch to dynamically create VLANs on links with other devices running GVRP. It enables the switch to automatically create VLAN links between GVRP-aware devices. This reduces configuration efforts and minimizes the chances for errors in VLAN configuration. When GVRP is enabled, the switch registers and propagates VLAN membership on all ports that are part of the active topology of the underlying spanning tree. Incoming VLAN registration and de-registration requests are used to update the dynamic VLAN database. Any changes in the registration state of a given VLAN on a given port are propagated on ports that are part of the active topology of the spanning tree, in order to ensure that other GVRP-aware devices on the LAN update their VLANs' databases. The dynamic VLANs database, in all GVRP-aware devices is thus automatically configured so that the port is registered if one or more members of the corresponding VLAN are reachable through the port. **Functional Description** The system supports GVRP VLAN registration on all ports. By default, GVRP is disabled on all ports. The user may enable GVRP per port. If a port is GVRP-enabled, it starts sending GVRP declarations about all registered VLANs on other GVRP-enabled ports in the switch. The port can also receive GVRP declarations from neighboring switches. When receiving GVRP declarations, the software does the following: 1. If the declared VLAN doesn't exist in the device, it creates it. 2. It registers the port to the declared VLAN. 3. It floods the GVRP declaration to all other GVRP-enabled ports in the device. In case users do not wish new VLANs to be created in the device, they may disable dynamic VLAN creation. A user may decide that a port will not be registered in some specific VLANs, or will not be registered in any dynamic VLAN, even though it will participate in GVRP. In order to add static ports to dynamic VLAN already created, the user must first "recreate" (define) the VLAN as static. The information that determines whether frames destined for each VLAN are transmitted tagged or untagged is carried in a static VLANs database. If no static information for the VLAN exists, the frames for that VLAN are transmitted tagged.
Private VLAN Edge Provide the ability for ports to be members of the same VLAN while still not being able to gain access to other ports within that same VLAN; requires the establishment of private vs. public ports within each VLAN (default is public)	A Private VLAN is a Layer 2 security feature providing port-based security and isolation between adjacent ports within a VLAN. It is an extension, of the common VLAN. Private VLAN Edge provides security and isolation between ports on a switch so that traffic from "protected" ports is only sent to the uplinks and cannot travel to another port within a switch, thereby keeping calls private. When private VLAN edge is enabled, there is no forwarding of unicast, broadcast, or multicast traffic between ports on a switch, and all traffic between ports on the switch must be forwarded through a designated (router) ports device. Private VLAN enables per port security, requiring only a VLAN on every switch, not every port. This feature greatly minimizes the number of VLANs required. Private VLANs and normal VLANs can exist simultaneously in the same switch. A port can be defined as a Private VLAN Edge port of an uplink port, so that it will be isolated from other ports. **Functional Description** • A port can be defined as a Private VLAN Edge (PVE) port of an uplink port. • If the destination address isn't MAC-to-Me, the FDB decision for a packet entering a PVE port would always be the uplink port. • Trap-to-CPU and Mirror-to-CPU rules still apply. • All ingress and egress rules would still be applied on packets entering PVE port.

	• All L2 protocols can be enabled on PVE ports. • All port modes can be enabled on PVE port. • IP address can’t be defined on PVE port. • Uplink port can be a null port. This is required if the routing is done by the switch router.
Protocol Based VLANs 802.1v; VLANs can be established based upon the protocol information within the packet header of the traffic flow	The switch associates a frame with a VLAN based on a combination of the station’s MAC source address and the protocol stack in use. Separate VLANs can be created for each set of protocol-specific application. Protocol-based VLAN allows a station to be a member of multiple VLANs, depending on the number of protocols it supports. **Functional Description** Untagged frames received on a VLAN-aware switch can be classified by methods others than source port. Specifically, classification rules may be based on data-link layer protocol identification. Such classification is referred to as protocol-based VLANs. Protocol-based VLANs are useful for isolating Layer 2 traffic of different Layer 3 protocols. If, for example, a switch serves IP stations and IPX stations that communicate with a single VLAN-unaware server, without using protocol-based VLANs, all the Layer 2 broadcast traffic would reach all the stations. With protocol-based VLANs, the switch can forward incoming traffic from the server to stations in a specific VLAN only. Support of Protocol-based VLANs uses the PCL mechanism.
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.
IP Subnet-based VLANs and MAC-based VLANs	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 single port (e.g. on a router uplink) and for the untagged packets to be assigned to their proper VLAN. MAC-based VLAN classification allows packets to be classified according to the packet’s source MAC address.
Port-based VLANs	By default, all ports in a device belong to a common Layer 2 broadcast domain. When the device sends a broadcast packet, the packet goes out all active ports. A port-based VLAN (Virtual LAN) is a subset of ports on a device that constitutes a Layer 2 broadcast domain. Port-based VLANs can reduce the likelihood and severity of broadcast storms by reducing the number of ports affected by a storm. In addition, for devices such as servers that can cause broadcast storms, you can add static MAC entries for the devices and assign the static entries to a VLAN.
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 802.1Q enables service providers to use a single VLAN to support customers who have multiple VLANs. The IEEE 802.1Q-in-Q VLAN Tag Termination feature on the sub-interface level preserves VLAN IDs and segregates between traffic in different customer VLANs.
COS/QoS	
Quality of Service Features --- L2/L3/L4 QoS **CoS/QoS** To overcome unpredictable network traffic and optimize performance, you can apply Quality of Service (QoS) throughout the network to ensure that network traffic is prioritized according to specific criteria. The switch supports two modes of QoS: basic and advanced. QoS in brief: 802.1p, TOS, DSCP marking • QoS mapping: 802.1p to TOS/DSCP, TOS to 802.1p/DSCP, DSCP to 802.1p/TOS • Classification per port, 802.1p(COS) value, MAC SA/DA, Ethertype, TOS precedence, DSCP value, ICMP code and type, IP SA/DA, IP protocol, TCP/UDP port • Four egress queues per port that support strict and WRR queuing algorithms • Ingress bandwidth rate limiting per port/flow • Egress bandwidth rate limiting per port/queue	Network traffic is usually unpredictable, and the only basic assurance that can be offered is Best Effort traffic delivery. To overcome this challenge, Quality of Service (QoS) is applied throughout the network. This ensures that network traffic is prioritized according to specified criteria, and that specific traffic receives preferential treatment. The system enables the user to define various services for specific traffic flows. This is achieved by two mechanisms: • Classification – the user specifies certain fields within the packet, which are matched to some values. All packets matching those fields are related to the same flow/class. • Actions – user can set various actions such as manipulating fields within the packet (e.g., VPT, DSCP), policing at the ingress, scheduling at the egress, and shaping at the egress. Same actions are applied to all packets within a specific flow. The underlying mechanism for supporting most of the actions related to bandwidth management and control is the concept of queues. After a packet has been classified it is assigned to one of the output queues. The system supports 4 queues per port. The system services the queues (takes frames out of a queue for transmission) according to the current queue scheduling settings, as defined by the user. These settings determine which queue is handled and how many frames from that queue will be handled before any other queue is taken care of.
Queuing Algorithms	Up to four priority queues are supported system wide. The QoS application will use the devices enhanced tail drop algorithms. (When IEEE 802.3x Flow Control is not activated).
Number of queues per port	4 egress queues per port that support Strict Priority (SP) and Weighted Round Robin (WRR)
Scheduling	Scheduling profiles may be defined as Strict Priority (SP) and Weighted Round Robin (WRR). To ensure minimal latency, scheduling of transmitted packets is implemented using a Strict Priority algorithm. The system egress queues can work either in Strict Priority or Weighted Round Robin.
User Priority	Support for IETF DiffServ and IEEE 802.1p User Priority. Support for management and prioritization of packets forwarded to the CPU with built in mechanisms that allow controlled traffic to be forwarded to the CPU without forcing the CPU to be a member of the specific VLAN
Egress Rate Shaping	For maximal bandwidth limitation, each of the ports incorporates an egress rate shaper. Each port incorporates four egress rate shapers. One for shaping the port’s aggregate egress traffic and the

	remaining for shaping the traffic from each of the port traffic class queues. The egress rate shapers are implemented using the Token bucket algorithm. Traffic shaping can be set only per port of the LAG (Link Aggregated) members. Regarding the rate-limit and traffic-shape commands under the interface command mode, here are the valid value ranges: 1) rate-limit command is used to limits the rate of the incoming traffic and need to be configured on an interface; range: 62K – 1000M on GE and 62K – 100M on FE 2) traffic-shape command is used to configure the shaper of the egress queue on a port; CIR range: 64K – 1000M on GE and 64K – 100M on FE; CBS range: 4096 – 16769020 bytes on GE.
QoS Marking	802.1p, TOS, DSCP marking
QoS Mapping	QoS mapping: 802.1p to TOS/DSCP, TOS to 802.1p/DSCP, DSCP to 802.1p/TOS
Classification	Classification per port, 802.1p (COS) value, MAC SA/DA, Ethertype, TOS precedence, DSCP value, ICMP code and type, IP SA/DA, IP protocol, TCP/UDP port
Basic and Advanced QoS mode overview 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.	While the system facilities providing Access Control and CoS/QoS are given, there are several ways to configure the system to provide the desired effect. These modes present different levels of functionality and complexity to the user. Note These Modes are different ways to control and configure the system CoS/QoS facilities, and not different operational modes of the actual system CoS/QoS facilities. There are three CoS/QoS control modes • None • Basic Mode In Basic CoS mode the user can classify frames into broad classes, by the ingress interface or by the value of a single frame header field. Each class can be directed to a desired egress queue, and the user can also configure the queue servicing parameters. This is enough to provide relative class-by-class differential services. This mode does NOT include the facility to classify traffic into fine-grained flows (e.g. define a flow as a specific value in a frame-header fields, or a combination of values in several header fields) and does not include traffic measurement facilities. • Advanced Mode In Advanced mode CoS/QoS the user has access, and must explicitly configure all aspects of all CoS/QoS facilities in use. Traffic may be classified into broad classes or fine-grained flows.
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.
QoS Basic Mode In basic QoS mode, it is possible to activate a trust mode (to trust VPT, DSCP or none). In addition, a single access control list can be attached to one or more interfaces.	In the basic mode the user is actually “trusting” a specific domain in the network. Within that domain, packets are marked on predefined fields (from L2 or L3) to signal the type of service they should get. Nodes within the domain use these fields to assign the packet to a specific output queue. The initial packet classification and marking of those fields was done in the ingress of the trusted domain. **Classification for basic mode** The user can select the trust behavior, i.e., identify the fields upon which the output service assignment is done. The following selections are available: • VLAN tag (802.1p tag) / 802.1p port based • DSCP Only one selection can be applied at a time. The selection is done on a system basis, i.e., the selection is applicable to all ports. User can also choose to trust none of the above, by that classifying all the traffic to Best Effort service. **802.1p Tag-based** In this mode the IEEE802.1p tag is used to classify the packet. Packets with an IEEE802.1p tag are mapped according to their VPT to one of the output queues. There is a default mapping of the VPT to output queue as defined in the 802.1p standard. **802.1p Port-based** The IEEE 802.1p specifies a method for indicating frame priority based on the new fields defined in the 802.1Q (VLAN) standard. The capabilities defined in 802.1Q include the definition of a VLAN frame format, which allows carrying of VLAN identification and priority information over LAN technologies. The IEEE 802.1p specifies a mechanism for indicating frame priority based on existing priority fields - in the 802.1Q VLAN standard. 802.1p supports up to 8 traffic classes (priorities), with multiple priority queues established on a per port basis. **L3 predefined fields** In this mode, the user configures the system to use the IP DSCP of the incoming packet to map the packet to the output priority queues. The original VPT of the packet will be kept. The mapping of the IP DSCP to priority queue is set on a per system basis. It can be enabled or disabled per port. If this mode is active then a non-IP packet will always be classified to the best effort queue.
Services for basic mode	**Scheduling: Strict Priority (SP), and Weighted Round Robin (WRR)** The OmniStack LS 6200 supports Weighted Round Robin (WRR) scheduling: The WRR scheduling

	algorithm ensures that the lower priority packets are not entirely starved for bandwidth and are serviced without compromising the priority settings administered by the network manager. Strict priority queuing ensures that the highest priority packets will always get serviced first, ahead of all other traffic, and allows the other three queuing to be serviced using WRR scheduling. After the packet has been assigned to a specific queue, using the chosen classification method, various services can be applied. The user can configure the output queues for scheduling scheme: all in strict priority or all in Weighted Round Robin (WRR). This selection is done per system, i.e., set on all ports. When assigning queues to strict priority policy, they are automatically assigned from the highest priority queues. In case of WRR policy, the user is free to assign the weights to the queues in any order. The weights setting are available on a per port basis. The system always assigns best effort traffic to q1. It is user responsibility to assign weights to output queues correctly so that q1 will be kept as the best effort queue. System will have defaults to reflect strict priority on all queues. The user can also configure the output shaping (burst size, CIR, CBS per queue or port) By using combinations of the mentioned settings the user can set the following services: • Minimum delay – queue assigned to strict priority policy, traffic assigned to highest priority queue • Best effort – traffic assigned to the lowest priority queue • Bandwidth assignments – by configuring WRR scheduling scheme and choosing the right weights The user is not configuring the services (BE, min delay, etc.) but rather setting traffic classes (queues), scheduling scheme and weights for the queues. Below are some guidelines for setting the specific services: Best effort – some portion of the bandwidth must always be kept free for BE traffic. The system always maps best effort traffic to the lowest priority queue. So the user must assign some bandwidth also for this queue. Minimum delay: traffic should be assigned to output queues that are scheduled with strict priority (SP). For minimum delay, traffic should be assigned to the highest priority queue among the SP queues.
QoS 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.	In this mode the user is able to define rules specifying classification of flows and assigning actions to them that relate to bandwidth management, bandwidth control and more. The ACL mechanism described above is used to classify traffic in Advanced Quality of Service mode. Advanced mode services: After the packet has been assigned to a specific queue, using the chosen classification method, various services can be applied. The user can configure the output queues for scheduling scheme: all in strict priority or all in Weighted Round Robin (WRR). This selection is done per system, i.e., set on all ports. When assigning queues to strict priority policy, they are automatically assigned from the highest priority queues. WRR Weights per queue are preconfigured globally to 1, 2, 4, and 8. System will have defaults to reflect strict priority on all queues. The user can also configure the output shaping (burst size, CIR, CBS per queue or port) In addition to all these settings, which are available also in the basic mode, the advanced mode allows the setting of the metering for enabling ingress policing. By using combinations of the mentioned settings the user can set the following services: • Assign egress priority queue • Best effort – traffic assigned to the lowest priority queue • Mark 802.1p Priority (set VPT value according to the classification) • Mark IP DSCP (set value according to the classification) • Min. delay – queue assigned to strict priority policy, traffic assigned to highest priority queue • Maximum bandwidth of a flow (by setting the metering at the ingress) - User specifies a maximum bandwidth value above which all traffic is dropped. This is done by setting a meter at the input for the max bandwidth and setting the excess policy to drop. It is up to the user to verify that the total bandwidth he is setting on a specific egress port does not exceed the port rate. The user can apply all the Packet Processor available meters to a specific ingress port. • Guarantee/reserve minimum bandwidth of a flow (by setting the scheduling at the output queues) User specifies a minimum bandwidth value above which all traffic is marked for discard. As such, it will be discarded at the egress queue when exceeding the Tail Drop threshold. It will be transmitted if the queue has extra bandwidth. This configuration is done by setting a meter at the input for the min bandwidth and setting the excess policy (exceed action) to remark the DSCP of the packet • Set the Tail Drop thresholds: User can set thresholds for the non-conforming/excess/out of profile traffic (different names for the same thing). The egress queue will drop all packets that are marked for discard when exceeding the threshold. The user can configure the threshold per each queue of a port. This is a system setting (same setting applies to all ports). User can enable/disable tail drop per port. The default state is tail drop disabled. User can also activate any of the trust modes, one per CCL. The services above can be combined in the following manner: Queue assignment operations AND Metering (max bandwidth or min bandwidth) AND Scheduling (min delay) AND Traffic shaping

Inner VLAN Classification MAC ACL – Inner VLAN Classification	**What it is** Inner VLAN Classification is a new feature added to MAC ACL classification in addition to outer VLAN tag classification. It allows setting priority and rate limiting (ACL) based on the customer tag value. In order to allow the user to configure Inner VLAN Classification, a new field is added to the Access Control Rules, called “inner-vlan” **How to use it** The inner-vlan field is followed by the vlan-id which is the inner VLAN ID of a double tagged packet The inner-vlan field can be assigned only on: ▪ FE customer interfaces (the port mode is customer) ▪ Service provider interfaces when the traffic is double tagged **Functional Description** For traffic ingressing from the Provider to the Customer, the forwarding priority of the packet is based on priority bits of the Outer VLAN tag. This is achieved by using Basic Quality of Service Mode prioritization. For traffic egressing from the Customer to the Provider, the priority of the outer VLAN tag should be assigned: • Configured mapping of outer tag priority based on customer tag bits. This is achieved by configuring an ACL to classify traffic that arrives with a given VPT. A policy is then used to override the priority bits, and set them to a new value. This can be done in Advanced Quality of Service Mode. • Exact mapping of outer tag priority bits as the customer tag bits. This is achieved by using Basic Quality of Service Mode prioritization, or as described above. • Per configuration per service (port and customer VLAN) – This is achieved by using the user-defined bytes of the ACL, and is also called “Inner VLAN Classification”. **User Controls** The ACL configuration is updated to include configuration of user defined bytes, where the user specifies the offset and the classification rule. Web interface includes examples of use of user-defined bytes / offsets. **References, Notes and Limitations** It is the user’s responsibility to ensure that there are no contradictions between the classification rules. The inner-vlan field can be assigned only on: • Fast Ethernet customer interfaces (the port mode is customer). • Service provider interfaces when ALL the traffic is double tagged.
Rate Limiting (Ingress/Egress) Ingress rate limiting and egress shaping: • Ingress bandwidth rate limiting per port • Egress bandwidth rate limiting per port	**Egress Rate Limiting (Shaping):** The device is capable of limiting the transmission rate of selected egressing frames but still keep QoS. The device supports this on a per-port basis. Shaping the output load performs egress rate limiting. **Functional Description** The device can limit the transmission rate of selected egressing frames and supports this on a per-port basis. Shaping the output load performs the egress rate limiting. The device can determined the types of frames to limit, or shape it can: • Limit all frames except for management frames Management frames are excluded. Any frame that is not limited is ignored in the rate calculations (i.e., their size is not counted toward the limit total). The device can select the required maximum rate, it supports 4095 different rate speeds or shapes from 62 Kbps to 256 Mbps in a 4k non-linear steps (Egress rate shaping can be disabled). Required rates are: 64kb, 128kb, 256kb, 384kb, 512kb, 640kb, 768kb, 896kb, 1M, 1.5M, 2M, 2.5M, 3M, 3.5M, 4M-100M in single for both. Device determines the bytes to count for shaping needs to be. **User Controls** • User can set shaping to an Ethernet port • User can set committed-rate, the average traffic rate (CIR) in kbps to a specific port. • User can disable the shaper on the interface. **References, Notes and Limitations** • Rate limiting steps are in 4k and are non-linear • Shaping is done only on "network frames" and not on management frames (this is not a user defined parameter) • Shaping is done on packet itself (not including preamble or IFG) • The committed rates are in Kbps and not bps. Traffic shaping is on per port base and not per queue base **Ingress Rate Limiting:** Similar to storm control, the user can define the overall rate limit for all packets. For Giga Ethernet port it is recommended to use the metering mechanism in the QoS advanced mode. Metering mechanism enables the combinations of port; port and VLAN; port and Inner VLAN. Basic mode can be used effectively only for Fast Ethernet ports limiting entire port only. **Inner VLAN in Ingress Rate Limiting:** **What it is** Ingress Rate Limiting ▪ Now supported to limit the rate of the incoming traffic by: o port o port and VLAN o port and Inner VLAN o port, VLAN and Inner VLAN ▪ With the added support of Inner VLAN, user can configure MAC ACL with VLAN and/or Inner VLAN, which will be used by a class and policy-map.

	▪ Eventually user can police the ingress rate in the policy-map and then apply the map to an Ethernet interface or a port-channel interface
Multicast Support	
Layer-2 Multicast Support	**Functional Description** The system supports forwarding incoming multicast traffic according to their Multicast Group (as defined by their destination MAC address). By default, such traffic is flooded to all relevant ports, but the user may limit forwarding to a smaller subset. The system has two separate related functions: Forwarding and Filtering of L2 Multicast frames. Forwarding of L2 multicast frames is always on, filtering is user controlled. If Filtering is OFF, multicast frames are flooded to all ports in the relevant VLAN. If Filtering is ON, L2 multicast frames will be forwarded to a SUBSET of the ports in the relevant VLAN. This subset is defined by the entries currently in the Multicast Filtering Database. The Multicast Filtering Database is filled by the results of the IGMP Snooping facility (if enabled) or by adding Static entries. Entries are defined per VLAN. If traffic addressed to an unregistered multicast group is seen it is handled by a special entry in the Multicast Filtering Database. The default setting of this is to flood all such traffic (traffic in unregistered multicast groups). The system supports Multicast Filtering for 256 Multicast Groups; additional Multicast groups will be treated as Unregistered. For each multicast group, the user may define a list of Forbidden ports. These ports will not be included in the multicast group even if IGMP snooping suggests they should. This list is static, and will be preserved across resets. The user may define ports as “forward all” which will cause them to receive a copy of any incoming frame with a MAC multicast destination address. Multicast filtering is enforced on all traffic. The default handling of all unregistered multicast frames is for them to be flooded, so that the user will not be required to add an excessive number of rules. Starting with Release 1.5 S/W version, there is support for IGMPv3 as well as IGMPv1/v2. The router closest to each potential client, upon discovering that there are no intervening routers, turns each L3 multicast frame into an L2 multicast frame carrying the same data (by attaching appropriate L2 headers, and sending a copy on each relevant interface). If there are any L2 switches attached to such a router port enroute to the possible clients, they make sufficient copies to send to each relevant port. (Note: if there is an L2 switch attached to a single router interface, the router will see all clients attached to different ports of that L2 switch as if they are directly attached to its interface, and so will only generate a single copy of the L2 multicast frame on that interface). Also introduced in this S/W version is IGMP Snooping Querier. The querier function is used to support network topologies where layer3 multicast protocols are not activated (traffic does not need to be routed). **1. The system supports Multicast Filtering for 256 Multicast Groups;** **2. Additional Multicast groups are treated as Unregistered. By default, such traffic is flooded.** **3. All multicast packets are forwarded.** **4. IGMP throughput – data packets: wire rate, control packets: could not reach wire speed.** **User Controls** User may enable/disable MAC Multicast Filtering System-wide. By default, MAC Multicast Filtering is OFF. User may set treatment of Multicast traffic in Unregistered Multicast groups to either flood to all ports of the incoming VLAN or silently ignore it. By default, such traffic is flooded, to allow routing protocols (which use multicast traffic internally) to function. The user may set forbidden ports in multicast groups, per VLAN. The user may define “forward all” ports, Per VLAN.
Static Multicast Groups Supports static multicast groups; with up to 256 multicast groups. The user may define by explicit action multicast groups to be supported, per port. Each such group is defined in the context of a specific single VLAN. In general, this feature allows the user to manually achieve what IGMP snooping can do automatically, as a replacement (when it is undesirable to use IGMP snooping) or as a supplement (e.g. to handle hosts that do not generate IGMP reports correctly).	When the user explicitly configures a multicast group, it is considered static – that is, Each such multicast group is defined in the context of a single VLAN, and will affect only incoming multicast frames classified into that VLAN. The user has to explicitly designate which ports (in this VLAN) will be registered as members of the multicast group defined. Static assignments are kept even if no multicast traffic is seen for that group. The assignments will be preserved across resets and reboots. A port may be made a member of as many multicast groups as desired (up to the maximum of 256 multicast groups supported by the system). Note that any static entries will only take effect if/when Multicast Filtering is enabled. If Multicast Filtering is OFF, Multicast traffic will be flooded to all ports of the relevant VLAN.
IGMP Snooping (versions 1& 2 &3 are supported). Starting with Software Release 1.5, IGMPv3 snooping is supported as well. (RFC 3376) The system can recognize and handle IGMPv3 messages as well as IGMPv1 and v2.	IGMP snooping (IGMP snooping on IGMPv1/v2/v3) is supported. The IGMP protocol is used between devices and their neighboring multicast routers to communicate devices’ willingness to start or stop reception of multicast traffic addressed to a specific multicast group. The IGMPv2 is widely used (backward compatibility with IGMPv1) and it introduces Leave-Group messages & querier election mechanism. The IPMS or the IGMP snooping/gleaning mechanism optimizes multicast delivery in a switched environment. The IPMS is a Layer-2 multicast switching with a wire-speed performance. The maximum number of IGMP Multicast Group supported is 256. **Functional Description** The switching Packet Processor is programmed to forward all IGMP frames to the CPU. The CPU analyzes the incoming frames and concludes which ports have stations wishing to join (or stay connected) to which multicast groups, and which ports have multicast routers generating IGMP

	queries, Routing protocols packets, and multicast traffic. The switch CPU forwards a representative IGMP report as a Join request (or as a “still interested” response to a query) to the relevant multicast router ports, making sure that IGMP reports are not forwarded to other ports, for fear of squelching stations on that port from generating Join requests. IGMP queries arriving from the multicast router are forwarded normally to all relevant ports (all ports currently registered in that multicast group). Ports connecting to Multicast routers will be defined as “forward all” ports in the relevant VLAN(s) on that port. This means that these ports will receive a copy of each MAC multicast frame received, including a copy of all IGMP reports from stations. Immediately after receiving a join message from a host, the switch would join the ingress port to the multicast group that was requested by the host. A port would be removed from a multicast group if: • IGMP reports for the multicast group were not received for a “Host timeout”. • IGMP leave message for that group was received and no IGMP reports for the multicast group were received for a “leave timeout”. The “Leave timeout” can be set to 0 for immediate leave. **User Controls** The user may enable or disable the feature System-wide and per VLAN. User may statically define which ports connect to a Multicast router The user may enable/disable dynamic learning of “multicast router ports” from multicast routing protocols (DVMRP and PIM) by default dynamic learning is enabled. The user may set the following parameters of the IGMP snooping facility per VLAN: • Host time-out: how long before giving up on getting an IGMP report/response (Default: 260 seconds) • Multicast router time-out: How long before deciding a multicast router is no longer active on that interface. Note that statically configured Multicast router ports do not age. (Default: 300 seconds) Leave time-out: How long after the last host asks to “leave” a multicast group (IGMPv2) to wait for another possible station on the same broadcast domain trying to join the same group (or asking for the group to not be pruned). If this time expires, the system will stop forwarding the relevant multicast group to this interface. The user may specify “immediate leave”, which will cause this value to be effectively set to 0. (Default: 10 seconds) The user may examine and see which ports are members of each multicast group, and where multicast routers are located. **References, Notes and Limitations** IGMP snooping configuration is defined per-VLAN. Therefore, the relevant VLANs must already exist in the system. When a VLAN is removed from the system, any IGMP snooping configuration for this VLAN will be lost. IGMP snooping is not available on dynamically created (via GVRP) VLANs. According to the standard, packets with a destination IP address in the 224.0.0.X range, which are not IGMP, must be forwarded on all ports. Therefore, IGMP reports in the 224-239.128|0.0.X (all 32 addresses are mapped to the same MAC multicast address) range will be ignored and will not be snooped (unless a static entry exists and 224.0.0.X IGMP reports had been allowed by the user). Traffic to 224.0.0.X should have been broadcast through the VLAN, but will not be, because there is already an entry for 225.0.0.X. So, to meet standard, all packets within the aforementioned range will not be marked to Packet Processor. Thus, when traffic arrives, it will not be broadcast per port, but throughout the whole VLAN (just like 224.0.0.X). This is common industry practice.
IGMP Querier	**What it is** IGMP Querier is used to support IGMP snooping where the multicast traffic doesn’t need to (or cannot) be routed Example A local network where the multicast content is provided from a local server, and the router of the network does not support multicast IGMP Snooping can only work when there is a IGMP Querier in the network **How to use it** To configure an IGMP snooping switch to be an IGMP snooping querier of a VLAN (default is disabled) Configuration is per VLAN (under vlan interface) Must enable IGMP snooping for the VLAN Must configure igmp snooping querier address before enabling IGMP snooping querier IGMP snooping querier starts after 60 seconds if no IGMP traffic is detected from a multicast router IGMP Snooping Querier will disable itself if it detects IGMP traffic from multicast router **IP Address** IGMP snooping querier requires an IP address to be configured on the VLAN interface to define the source IP address that the IGMP snooping querier will use If an IP address is configured for the VLAN, it would be used as the source address of the IGMP snooping querier Use the command “ip igmp snooping querier address” to configure the address for the querier If no IP address is configured for querier, the IGMP snooping querier cannot be enabled **Version** Default IGMP snooping querier version is set to IGMPv2 User can set the IGMP snooping querier version to IGMPv2 or IGMPv3

	When working in querier version IGMPv3, the switch will automatically downgrade the version to IGMPv2 if it detects an IGMPv2 message from the hosts (in the case the hosts do not support IGMPv3) Similarly, configured IGMPv2 querier can be downgraded to IGMPv1, however, it cannot be automatically upgraded to IGMPv3 **Guidelines** Only one switch can be configured as the IGMP Querier of a VLAN, even if there are more than one IGMP snooping switches in a local network When the IGMP Snooping Querier is enabled, it disables itself if it detects IGMP traffic from multicast router When receiving "Fast Leave" message, the switch will not issue a special query messages **Functional Description** The IGMP Snooping Querier is used to support IGMP snooping where the multicast traffic does not have to be routed. 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. The network administrator can configure an IGMP snooping switch to be an IGMP Snooping Querier of a VLAN. If a VLAN is shared by more than one IGMP snooping switch, the user should verify that only one switch is configured as the IGMP Querier of a VLAN. When the IGMP Snooping Querier is enabled, it starts after 60 seconds with no IGMP traffic detected from a multicast router. IGMP Snooping Querier requires an IP address per VLAN. The user can either use the VLAN's IP Interface address or define a unique IP address. If there is no IP address configured on the VLAN interface, the IGMP Snooping Querier can not be enabled. The user can set the IGMP Querier mode to either V2 or V3. (Default is V2). When working in IGMPv3 mode and detecting an IGMPv2 message, the switch will automatically change its mode to IGMPv2. (Same goes when working in mode v2 and detecting v1 messages). **User Controls** The user can: •Configure an IGMP Snooping Switch to be an IGMP snooping querier of a VLAN (default = disabled) •Configure IP Address of the Querier interface •Set the IGMP Querier version **References, Notes and Limitations** •If a VLAN is shared by more than one IGMP snooping switch, the user should verify that only one switch is configured as the IGMP Querier of a VLAN. •When the IGMP Snooping Querier is enabled, it disables itself if it detects IGMP traffic from multicast router. •When receiving "Fast leave" message the switch will not issue a special query messages.
IGMPv3 Snooping Enhancement	**What it is** ▪ Starting with Software Release 1.5, IGMPv3 (RFC 3376) is supported as well as IGMPv1 and IGMPv2. ▪ The system can recognize and handle IGMPv3 messages o IGMPv3 adds support for "source filtering" for a system to report its interest in receiving multicast traffic ONLY from specific source addresses sent to a particular multicast address o This feature is intended to avoid delivering multicast packets from specific sources to networks where there are no interested receivers o IGMPv3 snooping listens to IGMPv3 query and membership report messages to maintain host-to-multicast group associations. It enables a switch to propagate multicast data only to the member ports.
IGMP timers	1) A port will be removed from a multicast group if: a. The OS6200 doesn't see the IGMP reports (sent from a receiver) for a "Host timeout" (configurable; default is 260 seconds) b. The OS6200 receive a IGMP leave message (sent from a receiver) and no IGMP reports for the multicast group were received for a "Leave timeout" (configurable; default is 10 seconds; can be set to 0 for immediate leave) 2) If a multicast router is no longer active on that interface, the multicast group will be removed for a "Mrouter timeout" (configurable; default is 300 seconds) Please note that there are Mrouter timer and host timer to timeout host port and Mrouter port. How would a port be aged out without receiving any "leave" message: Answer: on the "Host timeout".
Packet Storm Control	**Functional Description** The system can measure the rate of incoming broadcast/multicast frames on each port separately, and discard frames when the rate exceeds a user-set desired rate.The system measures the rate of incoming "unknown" frames (addressed to an unknown destination MAC address) separately. This means that the value specified is the maximum rate any single port will be allowed to pass, but if several ports of the same Packet Processor will operate together, this value is the aggregate allowed for all. **User Controls** The threshold for the number of broadcast packets that are sent over a port can be set, to prevent

	broadcast storms. The range is defined from 70 kbps to 285 mbps. Storm control can be enabled per port, and limitation can be based on: • Unknown unicast, multicast & broadcast • Multicast & broadcast • Broadcast only
The triple play feature (Please refer to the Triple Play Section for configuration example)	The triple play feature enables to supply Internet, IP TV and IP phone services, to service provider subscribers in an efficient way, while keeping Layer 2 isolation between the subscribers. **Principals** Each subscriber has a CPE MUX box. The MUX has multiple access ports that are connected to subscri devices, and one uplink port that is connected to the provider network. The box directs packets from the uplink port to a MUX access port based on the VLAN tag of the packet: Each VLAN is mapped to one MUX access ports. The VLAN tag is used to identify: 1) The service type: Internet, TV, or Phone. 2) Service provider. Packets from the subscriber to the service provider network are encapsulated by the OS LS 6200 switch with the subscriber's VLAN, except for IGMP snooping messages from the TV receivers that are associated with the multicast TV VLANs (VOD information that is sent also From the TV receivers would be sent like any other type of traffic). Packets from the service provider network to the subscriber can come from two types of VLANs: Subscriber's VLAN (Includes Internet, VOD and IP Phones) and Multicast TV VLANs. In all cases the packet on the provider network is doubled tagged: The external tag is the Subscriber's VLAN or one of the Multicast TV VLANs, while the inner tag is the tag that determined the destination the subscriber's network (by the CPE MUX). **Note:** A provider VLAN (outer tag) can be assigned per port **User Controls** • The user can configure multiple multicast TV VLANs for a customer port. • The user can define a CPE VLAN to multicast VLAN mapping for IGMP snooping **References, Notes and Limitations** Note: This is in addition to the Customer VLAN configuration of the customer port. The administrator cannot classify packets based on the inner tag. The user can't transmit multicast transmissions on multicast TV VLANs. A provider VLAN cannot be assigned per port/VLAN. If an IGMP message is received on a customer port tagged with a CPE VLAN, and there is a mapping from that CPE VLAN to a multicast-TV VLAN, the IGMP message would be associated with the multicast-TV VLAN.
Multicast TV VLAN	**Functional Description** The Multicast TV VLAN feature provides the ability to supply multicast transmissions to L2-isolated subscribers, without replicating the multicast transmissions for each subscriber VLAN. The subscribers are receivers only for the multicast transmissions. IGMP snooping is supported for those transmissions. The user can define a multicast-TV VLAN for an Access port. The multicast-TV VLAN can be any VLAN. The configuration is per port. If a multicast-TV VLAN is defined for an Access port, then: 1.The Access port joins the multicast-TV VLAN. 2.The egress rule for the multicast-TV VLAN on the Access port is untagged. 3.The Acceptable frame type of the port is set to Admit Untagged Only. The port's configuration is as follows: 1.Port's VLAN membership= Access VLAN, Multicast-TV VLAN. 2.Egress rules= Untagged for both VLANs. 3.PVID= Access VLAN. 4.Acceptable Frame Type= Untagged only. 5.Ingress Filtering= Enabled. If a multicast-TV VLAN is defined for an Access port, then all IGMP messages that are received from that port should be associated to the multicast-TV VLAN (Seeing the IGMP messages as was transmitted on the multicast-TV VLAN). If the MSTP state for the multicast-TV VLAN is Discard then the IGMP messages should be discard. If the STP state is Discard or the MSTP state for the Access VLAN is Discard then the IGMP messages should be discard. Note: Access ports are not supposed to be in Discard mode.
Spanning Tree	
Spanning Tree • IEEE 802.1d • IEEE 802.1w • IEEE 802.1s • Fast Port • BPDU Filtering when STP is disabled • Spanning Tree Protocol (STP) Root Guard • Spanning Tree Protocol (STP) BPDU	Spanning tree protocol (IEEE802.1D) protects an L2 broadcast domain from packet storms by selectively setting links to a 'standby" mode, in which they do not transfer user data, but are automatically re-activated when topology changes make it desirable. All L2 switches must comply with this standard. **Per-device Spanning Tree (802.1d)** Spanning tree is a standard requirement from L2 switches (performing transparent bridging) and allows bridges to automatically prevent and resolve L2 forwarding loops. The switches exchange configuration messages using specially formatted frames called BPDUs, and

Guard	selectively enable and disable forwarding on ports. The net result of this is that a tree of active forwarding links is created, ensuring there is an active path (series of L2 forwarding links) between any two devices in the network, with no loops. On a LAN interconnected by multiple bridges, Spanning Tree selects a controlling Root Bridge and Port for the entire bridged LAN, and a Designated Bridge and Port for each individual LAN segment. When traffic passes from one end station to another across the LAN, it is forwarded through the designated Bridge/Port for the LAN segment, to the Root Bridge, which in turn forwards the traffic to the designated Bridges/Ports on the opposite side. Bridges use Bridge Protocol Data Units (BPDUs) to communicate Spanning Tree information. **Functional Description** The system fully implements spanning tree, as defined in IEEE802.1D. By default, this feature is enabled at system startup, and is active on each port. BPDUs can be filtered or flooded per port for which STP is disabled.
Spanning Tree Fast Link option	While “classic” spanning tree, as defined in IEEE802.1D, is guaranteed to prevent L2 forwarding loops in a general network topology, it can take 30-60 seconds for it to “converge” (i.e. for each bridge/switch in the network to separately decide for each of its ports if it should actively forward traffic or not). This period is considered too long for many applications. The delay is needed to allow enough time to detect possible loops, allowing time for status changes to propagate and be acted upon by all relevant devices. In some cases, when network topology allows, faster convergence may be possible. For example, if a switch is known to be a “leaf” of the network topology (i.e. no bridges/switches at all are connected to its ports, except for a single one), it is known in advance that no loops will be created, and all ports may be set to the active, forwarding state with no delay at all. The Fast Link option allows a user to set a port to go immediately into forwarding state (skipping the blocking and listening states). The user assumes responsibility to sue this option only in appropriate cases. **Functional Description** This feature is switched off by default (i.e. at startup, only classical IEEE802.1D spanning tree will be enabled).
Rapid Spanning Tree (IEEE802.1w)	While “classic” spanning tree, as defined in IEEE802.1D, is guaranteed to prevent L2 forwarding loops in a general network topology, it can take 30-60 seconds for it to “converge” (i.e. for each bridge/switch in the network to separately decide for each of its ports if it should actively forward traffic or not). This period is considered too long for many applications. The delay is needed to allow enough time to detect possible loops, allowing time for status changes to propagate and be acted upon by all relevant devices. In some cases, when network topology allows, faster convergence may be possible. The “rapid spanning tree” protocol is designed to detect and make use of network topologies that allow a faster convergence of the spanning tree, without creating forwarding loops. **Functional Description** IEEE802.1W is implemented as an add-on to IEEE802.1D.
Multiple Spanning Tree- MSTP (IEEE802.1s)	Multiple Spanning Tree (MST) allows the user to group and associate VLANs to spanning tree instances. Each Spanning Tree Instance has an independent topology of other Spanning Tree Instances. The architecture provides multiple forwarding paths for data traffic, thus enabling load balancing in the network and fault tolerance provision. **Functional Description** IEEE802.1 is implemented as an add-on to IEEE802.1D. This feature is switched off by default (i.e. at startup, only classical IEEE802.1D spanning tree will be enabled). Up to sixteen (16) instances are supported. Effectively one spanning tree instance per VLAN.
Spanning Tree Protocol (STP) Root Guard If root guard is enabled on a port, it is never selected as the STP root port. The roles it can be assigned are: Designated, Alternate, Backup or Blocked. Root guard functionality enables detection and resolution of misconfiguration, while preventing loops or loss of connectivity.	**What it is** ▪ Used to prevent an unauthorized device from being the root of a spanning tree ▪ Configure root guard on an interface to prevent it from becoming the role of “root” ▪ Possible roles of a root-guard port: o ~~Root~~, Designated, Alternate, Backup, Disabled ▪ In the case of Multiple Spanning Tree, enabling root guard on an interface affects all the spanning tree instances ▪ If MSTP is enabled on the device, then configuring root guard on an interface forces the port to be “designated” **How to use it** ▪ Root Guard is disabled on a port by default ▪ Root Guard can be enabled on Ethernet or port-channel ▪ Root Guard can be enabled in STP, RSTP or MSTP ▪ When root guard is enabled, if spanning-tree calculations cause a port to be selected as the root port, the port transitions to the alternate (blocked) state 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. If root guard is enabled on a port, it is never selected as the STP root port; the roles it can be assigned are: Designated, Alternate, Backup or Disabled. Root guard functionality enables detection and resolution of mis-configurations, while preventing loops or loss of connectivity. **Functional Description** The Spanning Tree Protocols (STP, RSTP, and MSTP) prevent loops by allowing a single path to exist between any two endpoints on a network.

	Note: In the case of Multiple Spanning Tree, each MST instance has a root. Every port in the network is assigned a port role, which describes its functionality in the ST network: • Root – a forwarding port in the ST topology that provides the lowest cost path to the root bridge. • Designated – a forwarding port on a LAN segment in the network that provides the lowest cost path from that LAN to the root bridge. • Alternate – port that can provide connectivity to the root bridge, in the direction of the network bridge, if other network components fail. An alternate port offers an alternate path in the direction of the root bridge • Backup – port that can provide connectivity to the root bridge, in the direction of the leaves of the spanning tree, if other network components fail • Disabled – the port is not operational or is excluded from the active topology by management. • The Spanning Tree role is determined by calculations defined in the STP algorithm. By configuring root guard on an interface, the network administrator effectively prevents that interface (and the device to which it is attached) from assuming the role of “root”. If MSTP has been enabled on the device, then configuring root guard on an interface on the device forces the port to assume a role of “designated”.
STP BPDU Guard	**What it is** ▪ Used to protect the network from invalid configurations ▪ Recommend to use it when spanning-tree PortFast is enabled on a port or when STP is disabled ▪ Configuring BPDU guard on an interface (port or trunk) will cause the interface to be shut down when it receives a BPDU message **How to use it** ▪ BPDU Guard is disabled on a port by default ▪ BPDU Guard can be enabled on Ethernet or port-channel ▪ BPDU Guard can be enabled when spanning tree is enabled or disabled ▪ BPDU is useful when the port is in the PortFast mode **Functional Description** 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. **User Controls** The user can enable / disable STP BPDU guard on an interface (port/trunk). If enabled, the interface shuts down when a BPDU message is received. The user can view information about Spanning Tree, including BPDU guard status. **Reference notes and limitations** BPDU Guard is recommended to be used either when Fast Links ports is are enabled or when STP is disabled.
BPDU filtering (when STP is disabled) The user can: • Enable (when STP is disabled) / disable filtering • Flood BPDU packets when spanning tree is disabled on an interface • Filter BPDU packets when spanning tree is disabled on an interface	On a LAN interconnected by multiple bridges, Spanning Tree selects a controlling Root Bridge and Port for the entire bridged LAN, and a Designated Bridge and Port for each individual LAN segment. When traffic passes from one end station to another across the LAN, it is forwarded through the designated Bridge/Port for the LAN segment, to the Root Bridge, which in turn forwards the traffic to the designated Bridges/Ports on the opposite side. Bridges use Bridge Protocol Data Units (BPDUs) to communicate Spanning Tree information. **Filtering motivation** Filtering STP BPDUs may be useful when a bridge interconnects two regions and there is a need to have a separate spanning tree for each region. Filtering the BPDU in the bridge connecting the two regions will serve this purpose. **Functional Description** BPDU filtering functions only when the STP is globally disabled or on a single interface
System IP Address Management	IP interfaces are either configured by the user manually, or auto-configured on system start-up from a suitable remote configuration/startup server (BootP or DHCP server). A total of 5 IP interfaces can be defined. This total includes statically configured and dynamically defined (DHCP/BootP) addresses. Static Assignment of IP Address(s) **Functional Description** The user may set this system’s IP addresses manually These address(s) may be changed without requiring a system reset. **User Controls** The user may define the system IP address. **References, Notes and Limitations** A total of five IP addresses can be defined on the system (including static and dynamic addresses).
BootP and DHCP Clients for IP Address Assignments	The BootP protocol allows a device to solicit and receive configuration data and parameters from a suitable server. DHCP is an extension to BootP allowing additional setup parameters to be received from a network server upon system startup. Notably, while BootP stops operating once the system is up and running, DHCP service is an on-going process. For example, the IP address assigned to the system has a “lease time” that may expire, and can be renewed on the fly.

	This is useful, as it allows settings and parameters to be stored and managed centrally, as opposed to having to manage and manipulate them separately on each device. **Functional Description** The system incorporates BootP and DHCP clients that will solicit an IP address to use as the system IP address on each interface. The BootP client is operational on system startup if and only if no IP interface is defined, and if the startup configuration file is empty, and DHCP client is not configured to work. The BootP client will become operational sixty seconds after the device starts up. The BootP client will continuously try to find a BootP server by sending BootP requests to all VLANs and ports, until either of the following occurs: • A BootP server replies, in which case the replies are used to provide the system with an IP address on the interface on which the reply is received. (All other interfaces have to be assigned IP addresses using other means – DHCP or statically assigned) • The user starts to manually configure the system (command-line activity of any kind is detected on the serial console port) The user may then configure the system to use DHCP on any desired interface, to have an IP address assigned to it from a DHCP server. Once configured to use DHCP on any interface, the switch will continue to use DHCP even after resets, until either the configuration is erased (i.e. the switch is returned to the factory-default configuration) or the user explicitly disables DHCP on all interfaces and the device is reset, in which case the system will revert to BootP usage. A particular case of this involves failover to a backup master. If an IP address had been assigned dynamically, this command is preserved in the configuration file, which is always synchronized with the configuration file (running and startup) in the backup master. Therefore, in the event of a failover/switchover to the backup master, a DHCP request will be sent by the system. The result could be a different IP address, or failure to retrieve an IP address (in the event that communication with the DHCP server has been severed). **DHCP Client** When a DHCP client requires the use of TCP/IP network resources, it broadcasts a request for address information. The DHCP Server responds to this, assigns a new address and sends it to the client together with other required configuration for the network. This information is acknowledged by the client, and used to set up its configuration. This procedure is automatic, entirely transparent to the end user, and takes only an instant. Once a client has finished using the network, the configuration is made available for another client to make use of, thus conserving addresses.
Simplified Manageability	
Key Management Features Supported	• Access Control – Administration • Remote Authorization and Authentication (RADIUS) • TACACS+ • Management Security • The OS-LS-6200 is equipped with an RJ-45 console interface management port; this console interface is configured as DTE for operation, diagnostics, status, and configuration information. • In-Band Management: Telnet, Web-based HTTP or HTTPS, SNMP manager, or Secure Shell (SSH) o Remote Telnet Management or Secure Shell • Out-of-Band Management: RS-232 RJ-45 console port • TCP/IP Protocol • Traceroute • Software Loading: TFTP in-band or XModem out-of-band o Firmware Upgrade with XModem protocol • Dual image and multiple configuration file storage provides backup • Industry standard CLI with a familiar interface reduces training costs • Easy-to-use point-and-click Web-Based Element Manager with built-in help for easy configuration of new technology features • Remote Telnet management or secure shell • Port based, Port Mirroring for troubleshooting • Human readable ASCII-based config files for offline editing and bulk configuration • BootP/DHCP client allows auto-config of switch IP information to simplify deployment • DNS Client • SNMP: Management access via MIB database (SNMPv1/v2c/v3), Trap management to specified hosts o SNMPv1/v2/v3 **4.1.3** • Supports RFC 2819 RMON-I groups (1-Statistics, 2-History, 3-Alarm & 9-Events) **4.1.3** • Simple Network Time Protocol (SNTP) for network wide time synchronization • OmniVista NMS • Intuitive Web-based Management (WBM) Element Manager

	• Alcatel.Lucent Mapping Adjacency Protocol (AMAP) for building topology maps within OmniVista • 802.1ab – LLDP • 802.1ab –LLDP-MED • Virtual cable tester provides switch-based integrity testing on copper Ethernet cabling • Event logging and Remote SYSLOG support o Supports System logs: The switch allows you to control the logging of error messages, including the type of events that are recorded in switch memory, logging to a remote System Log (Syslog) server, and displays a list of recent event messages. • Power over Ethernet Support
Alcatel.Lucent's OmniVista Management Suite	The Alcatel.Lucent OmniVista Network Management System provides network management layer functions across all Alcatel.Lucent enterprise switching & Routing platforms. OmniVista is a multi-user environment that is able to discover all Alcatel.Lucent enterprise switches in the network. It also allows multiple users to monitor network-wide activities while providing access to each switch. The OmniVista Release 2.4.2 supports the launching of the OmniStack LS 6200 Web-Based Element Manager for switch configuration and management. Note: OmniVista Release 3.0 will support OS-LS-6200 for AMAP and Port Shutdown action for Quarantine. Note: for detailed information on the OmniVista Management please refer to the OmniVista Boilerplate/Users Manual documents. OmniVista, the Alcatel.Lucent enterprise network management solution, provides OS LS 6200 support with version 2.4.1. The level of functionalities includes: • Support all monitoring features applicable for a MIB-II compliant device • SNMP v1, v2, v3 support • MIB import with OID and icons installation out of the box without user intervention • MIB Browser • Discovery and topology support (including right click launch for element management launches such as web based interface and CLI/Telnet support) • OEM links between OS6200 and AOS devices within the Map application • Trap notification support from the notification application • Locator support with live, historical, browse searches • Statistics applications with MIB-II stats parameters OmniVista: version 3.0 provides configuration capabilities for OS6200 family for bulk operations and complex operations. Functionalities include: • Device adjacency support with automatic links association (AMAP support) • VLAN Manager • Resource Manager for backup and Restore device configuration, including new software image upload • OneTouch Quarantine with OmniVista Quarantine Manager • OneTouch QoS and Security through PolicyView for QoS and SecureView applications
The OmniStack LS 6200 Intuitive Web-based Management (WBM) Element Manager With web-based management, the system can be managed from any web browser. 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.	The OmniStack LS 6200 provides management with HTTP protocol, more commonly known as the World Wide Web. The system provides a series of Web pages written in HTML language, which displays the configuration and status of the system. The user can view and control the system with a standard Web Browser such as Netscape or Internet Explorer. The system contains an Embedded Web Server (EWS), which serves HTML pages through which the user can monitor and configure the system. This allows the system to be managed from the following browsers: • Wintel platform (2000, XP) - Microsoft IE V5.5 and above and Netscape V7.01 and above • Linux (Red Hat Linux 7.0 & greater) – Netscape 7.01 An attempt to log on to the system from any other platform will result in an error message to the user, indicating that only the above platforms are supported. The system internally converts web-based input (including menu selections, mouse clicks etc.) into configuration commands, MIB variable settings etc.
Multi-session Web Connections	Multiple (4 sessions) web connections supported; IEv6+ supported
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.
Alcatel.Lucent Adjacency Mapping Protocol (AMAP) Note: OmniVista 3.0 supports AMAP for the OS-LS-6200 Series	**AMAP** – A protocol used in conjunction with Alcatel.Lucent's enterprise SNMP based network management platform to automatically build topology maps. 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.
802.1ab - LLDP	**What it is** An IEEE standard for link layer discovery in Ethernet networks 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 Protocol (LLDP) allows a network management system to model the topology of the network by interrogating the MIB databases in the devices **Benefits**

	Simplifies and enhances the ability of a network management tools in multi-vendor environments Enables discovery of accurate physical network topologies Accurate topologies simplifies troubleshooting of enterprise networks Ensures proper aging so only valid network device data is presented Most implementations are expected to support optional system name, system description, system capabilities and management address **LLDP Protocol:** **What it is** ▪ LLDP is a Link-layer protocol that periodically transmits information to neighbors attached to the same network ▪ Advertisements contain o Device information, o Device capabilities o Media specific configuration ▪ The LLDP agent operates only in an advertising mode, and hence does not support any means for soliciting information, or keeping state between two LLDP entities ▪ The LLDP agent advertises information over Logical Link-Layer Control frames and records the information received from other agents in IEEE defined MIB modules. **Functional Description;** 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. All mandatory parts of the 802.1ab standard are supported. No optional parts of the 802.1ab standard are supported in this phase. **User Controls** Using SNMP, the user can configure the following: •Enable 802.1ab globally (LLDP) (enabled by default) •Enable 802.1ab per interface •Configure amount of time LLDP updates are sent •Configure the TTL field in the LLDP header, which is the time that receiving device is configured to hold an LLDP packet •Configure the time an LLDP port is configured to wait before reinitializing LLDP transmission o Configure the delay between successive LLDP frame transmissions initiated by value/status changes o Configure which IP address is advertised o The user can view LLDP information that was discovered from neighbors. **References, Notes and Limitations** LLDP support is a de facto subset of LLDP-MED, but cannot be supported when LLDP-MED is supported. For example, if LLDP-MED is supported, LLDP-MED advertisement from neighbor devices cannot be disabled.
SNMPv1/v2c/v3 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.	The SNMP model consists of a network management station and the devices that are managed. Managed devices include SNMP agents, which monitor network devices and store statistics in MIBs. The management application polls agents regularly to extract the contents of their MIBs. If data from the MIBs does not meet or exceeds a certain criterion, an alarm is generated. SNMP offers four basic functions: • Query the network device agent • Get a response from the network device agent • Change variables in the MIB of the network device • Recognize events (traps) from a network device such as startup, shut down, and errors A network management station uses query / get / change commands to inspect, configure, and monitor a network device through the MIB. It uses the fourth; recognize events, to detect traps from managed devices. The switch supports SNMPv1/v2c/v3.
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.
Files of Management Operation	Various Files of Management Operation: There are three types of files for the OmniStack LS 6200: • Configuration Files: The file stores system configuration information • Operation Code: Executed after system boot-up. Also known as Run Time Image • BootROM Image: The images brought up by loader when power up. Also known as POST (Power On Self-Test) Due to the size of flash memory, the OmniStack LS 6200 supports only two copies for Configuration files, two copies for Operation Code respectively, and two copies for BootROM Image.
RMON-I The RMON-I Groups that are supported includes: 1, 2, 3, 9 (Statistics, History, Alarm and Event) Remote Monitoring (RMON) is an extension to SNMP, which provides comprehensive network traffic monitoring capabilities (as opposed to SNMP, which allows network device management and monitoring). RMON is a standard MIB that defines	While SNMP gathers information from only one type of MIB, RMON extends SNMP to support a more comprehensive set of network statistics. The switch is an RMON-compliant device, which supports four types of MIBs as stated below. Remote Network Monitoring (RMON) probes can be used to monitor, manage and compile statistical data about network traffic from designated active ports in a LAN segment without negatively impacting network performance. This feature supports basic RMON 4 group implementation compliant with RFC 2819 (Remote Network Monitoring Management Information Base). 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. The RMON standard is an

current and historical MAC-layer statistics and control objects, allowing real-time information to be captured across the entire network.	SNMP MIB definition described in RFC 1757 (formerly 1271) for Ethernet. The product supports the following RMON-1 groups: The system supports in full the four following groups as defined by RFC2819 & 1757: • Ethernet statistics (Group 1) • History (Group 2) • Alarms (Group 3) • Events (Group 9) There is partial support with SMON MIB; it contains the port mirroring mib. There is no additional support for SMON counters.
Build-in web-server	An embedded http server running on the Management for Element Management purposes is supported
Unified Network Mgmt	The OmniStack LS 6200 can be configured and managed through: OmniVista 2.4.2 or greater, WBM (Web-based Management), SNMPv1/v2c/v3, and the Command Line Interface (CLI)
Port Mirroring Support for mirroring many-to-one; user controls include the ability to mirror RX, TX or both.	The Port Mirroring feature is used primarily as a diagnostic tool. The Port Mirroring feature allows you to have all the traffic (inbound and outbound) of an Ethernet port sent to another port on the switch. When you enable port mirroring, the active, or “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 session of traffic monitoring is supported system-wide, in which the user can have copies of all frames passing through a designated source port sent to a desired target port. The frames arriving at the target port are copies of the frames passing through the source port at ingress, prior to any in-switch action It is possible to specify up to 24 source ports to be monitored by a single target port. Port Mirroring is only relevant to Physical ports. Therefore, if it is desired to have an Aggregated Link as the source of a port mirroring session, the member ports have to be specified as sources in the port mirroring session individually. The system will allow selectively mirroring only RX or only TX frames (or both). Port mirroring is supported across the stack.
Virtual Cable Tester	The OmniStack LS 6200 switch feature allows for testing and troubleshooting of copper cabling and cabling faults. Provides the capability to perform Time Domain Reflectometry (TDR) of copper cabling per port: ability to measure copper cable length, integrity (opens, shorts), and stores history of previous measurements. Diagnostics of mini-GBIC transceivers is also supported.
Simple Network Time Protocol and Time-Zone (SNTP) Standards based time synchronization of logs and traps for optimum analysis Support for simple network time protocol; switch serves as SNTP client	SNTP is an Internet protocol used to synchronize the clocks of devices to a time reference synchronized via UTC. The OmniStack LS 6200, switch supports Simple Network Time Protocol (SNTP) used to synchronize the time of a computer client or server to another server or reference time source that is synchronized to Coordinated Universal Time (UTC). Time zone information is required for the translation of UTC time to local time. Alcatel.Lucent’s CLI Time-zone implementation provides the interface for establishing any time zone in the world. SNTP will not cause any performance degradation. SNTP is able to communicate with one or more NTP servers SNTP is part of the base software, and managed via CLI only The Simple Network Time Protocol (SNTP) assures accurate network Ethernet Switch clock time synchronization up to the millisecond. A network SNTP server performs time synchronization. Stratums establish time sources. Stratums define the distance from the reference clock. The higher the stratum (where zero is the highest), the more accurate the clock.
Support for multiple languages	Multilingual support per spec.
Access Control – Administration	It is desirable and useful to be able to limit who can view/change settings of the system. There are several facilities available for this purpose. In general, these are all ways to decide WHO can do WHAT on this system. **Privilege Levels** This feature provides network managers the ability to classify and prioritize user access to the device. This prevents users from either seeing or accessing the device configuration. **Functional Description** Privileges will be divided into two levels - 1 and 15. The higher level (15) will allow all access, while the lower level (1) will provide restricted access -mainly read-only access. Each of the CLI commands is associated with a privilege level, which is fixed and unchangeable. Users accessing the device are also associated with privilege levels. Users see only commands that are at a level less than or equal to their own. User privileges are maintained in the security database (RADIUS or local). *Note: Users are identified by user name and password.*
Remote Authorization and Authentication (RADIUS)	The device will support the Remote Authorization and Authentication (RADIUS) protocol. This 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 (for example: how long was the user connected). RADLAN supports the RADIUS client. RADIUS servers are standard, off-the-shelf products.
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.
TACACS+	In addition to RADIUS support, the device will also support the Terminal Access Controller Access

TACACS+ provides centralized security for validation of users accessing the device. TACACS+ provides a centralized user management system, while still retaining consistency with RADIUS and other authentication processes.	Control System (TACACS+). TACACS+ is a security application implemented in a Client/Server based protocol that provides centralized validation of users attempting to gain access to a router or network access server, in our case, it is only used to provide centralized validation for user wishing to manage the device only. TACACS+ was specified by Cisco and is released to the public as draft RFC available on the IETF. RADLAN support the TACACS+ client, TACACS+ servers are off the shelf product normally UNIX or Windows NT workstation.
Command Line Interface (CLI) The system may be wholly configured and managed by its Command Line Interface (CLI). Moreover, the system can display its current configuration to the user in the form of a collection of CLI commands, which may be stored and manipulated as text files. CLI commands can be used on the serial console connection, or over a Telnet connection.	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. Generally speaking, CLI syntax (and, when possible, semantics) is kept a close match to common industry practice. CLI is composed of mandatory and optional elements, and elements may have pre-defined formats and value ranges. The user can get on-line help to remind him of the format and value ranges allowed for the current commands. In addition, the CLI interpreter provides Command and Keyword completion to assist the user and shorten typing. Commands are grouped hierarchically into several modes: • User EXEC Mode • Privileged EXEC Mode • Global Configuration Mode • Interface Configuration Mode • Modes that are entered from Global Configuration Mode Each Command has an associated privilege level needed to run it.
Logging	The system implements multiple mechanisms to notify the user of significant events in real time, and keep a record of these events for after-the-fact usage. This section describes the various mechanisms implemented by the system for logging events
Event Logging	This feature provides the ability to log and manage events and report errors, and assists operators and network managers with monitoring and troubleshooting of large network malfunctions or local device errors. Network managers may use local (on device) event logging, and may monitor (and log events) in large network deployments on a standard remote SYSLOG server. The following events are logged for switch management: • Memory Alloc/Free error (resource exhausted) • Switch to default (selector-- if else, run to unexpected case) • Cold start/warm start (loader pass cold/warm start parameter via unclear memory) • All traps • Thermal, fan fail • Main power fail • Unexpected return
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. Logs and communicates events and traps via UDP messages as defined by the user; minimum of four Syslog servers are to be supported
Switch Auditing: Log auditing events locally, w/ time stamp: logins, configuration changes, etc	Switch logs the date, time, source address, destination address, and session oriented event into local memory (RAM and FLASH)
Traceroute (L3) for L3 nodes	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. This feature enables to discover the IP routes that packets will actually take when traveling to their destination. The trace command works by taking advantage of the error messages generated by devices when a datagram exceeds its time-to-live (TTL) value.
DNS Client Switch can serve as a DNS client	Domain Name System (DNS) converts user-defined domain names into IP addresses. Each time a domain name is assigned the DNS service translates the name 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 DNS protocol controls the Domain Name System (DNS), by which host names can be mapped to IP addresses. When DNS is configured on a switch, the host name can be substituted for the IP address with all IP commands. The DNS client retrieves this information from a nearby DNS server.
Power over Ethernet Support (PoE) **IEEE 802.3af Standard is supported.** 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	Power over Ethernet eliminates the need to run 110/220 V AC power to wireless network, IP telephony or other powered devices on a wired LAN. Use of a Power over Ethernet system eliminates the need to deploy double cabling systems in an enterprise, thus allowing greater flexibility in locations of network devices, and significantly decreasing installation costs. Power over LAN can be used in any enterprise network, which is deploying, or considering deployment of, IP telephony, wireless network, and other low-powered devices connected to the Ethernet LAN. DC voltage is inserted into the unused wires (data or spare) in a standard Ethernet cable. **PoE Features** The software supports all real time functions according to IEEE 802.3af-2003, including: • Detection • Port status monitoring (including thermal, current) • Power management algorithm

• Audio and video remote monitoring	• PD classification function • Fast power shutdown; in case of power supply failure (including thermal port protection) • Disable/enable power feeding • RFC 3621 MIB support • **IEEE 802.3af Standard is supported.**
Management Security Mgmt access control - privilege levels: User can define multiple user levels and user's access privilege capabilities (e.g., read-only/Level1 and read-write/Level 15)	For security reasons, it is useful to only a selected group of users to be allowed to perform system management. **Functional Description** The system allows limiting access to management functions only to users identified by their: • Ingress interface (Port, LAG or VLAN), including the out-of-band port • Source IP Address • Source IP Subnet Management access may be separately defined for each type of management access method: • Web (HTTP) • Secure Web (HTTPS, Using SSL) • Telnet (CLI over telnet sessions) • Secure Shell (CLI over SSH access) • SNMP (I.e. the set of allowed managers via Telnet may be different than that allowed as Web-based managers, which is different than that of secure-web based managers, etc.) A specific management access method may be completely disabled by denying all user access to that Management Traffic type (e.g. denying all users access to CLI/Telnet management effectively disables COI/Telnet as an available management interface to the system). By default all management access to the system is “Enabled” over all interfaces
Support for disabling each management interface	Switch is capable of disabling access to each manager interface, including SNMP, CLI and Web UI. Management access may be separately defined for each type of management access method: • Web (HTTP) • Secure Web (HTTPS, Using SSL) • Telnet (CLI over telnet sessions) • Secure Shell (CLI over SSH access) • SNMP (i.e., the set of allowed managers via Telnet may be different than that allowed as Web-based managers which is different than that of secure-web based managers, etc.)
Console Interface	The OS-LS-6200 is equipped with an RJ-45 console interface management port; this console interface is configured as DTE for operation, diagnostics, status, and configuration information.
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.
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.
Firmware Upgrade with XModem protocol	The system firmware of OmniStack LS 6200 is stored in Flash memory. They can be upgraded by loading the code into the system and update the Flash memory. Both systems can be upgraded with XModem protocol. The XModem works on the console interface. The user needs to run a terminal emulation program on a computer that It is initiated by starting a file transfer command in console interface, then starting a file transfer command.
TCP/IP Protocol	The OmniStack LS 6200 provides the TCP/IP and UDP/IP protocol stack for the use of network management applications such as SNMP, Telnet and Web management. The system defines an IP address, a subnet address mask and a default gateway. These parameters must be set up by the user and will be stored in the Flash memory for power-up configuration. Alternately the user can also choose to use BOOTP protocol to set up the IP address for the operation of the system. In order to support the TCP/IP, the system also supports ARP for address resolution function and ICMP protocol for Internet control message response. The main use of the ICMP protocol is to provide the reply of the PING application. The OmniStack LS 6200 also supports a PING function for probing remote devices.
SNMPv1&v2c&v3	The system is fully manageable using a combination of a database of MIB (Management Information Base) variables, whose combined values represent all facets of the system state, and the SNMP protocol to examine and possibly modify these values. SNMP is a very basic facility of the system and EVERY feature and configuration option is reflected in some MIB variable, and usually in many. There are extensive standards covering the various aspects related to MIB organization, functionality etc. and the related SNMP protocol. SNMPv1&v2&v3 are supported. Simple Network Management Protocol (SNMP) over the UDP/IP protocol controls access to the system, 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 read-only, read-write and super. Only a super user can access the community table.
SNMPv3	The SNMPv3 architecture supports three main features: security, access control and sending traps mechanism. It also describes how to apply the access control and the new sending traps mechanism on SNMPv1 and SNMPv2 PDUs.

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.
IP address filtering for SNMP	SNMP access is limited to select IP addresses that also match the community string
Multi-Session TELNET	The OmniStack LS 6200 supports Telnet capability. The management interface is the same interface as the console interface provided with the RS-232 port. The TELNET user interface supports four connections. A user will be disconnected immediately when there is already four session running TELNET. The TELNET session requires the same login procedure as the console interface session. The system supports up to 5 sessions, including separate Telnet sessions and a console connection. The user may use all CLI commands over a telnet session as would be possible over the console connection. User can connect to the system using any of the system's defined IP addresses. After logging in, the system displays the CLI prompt. Password recovery is not supported over telnet connections Timeout for telnet session is user configurable; default is 10 minutes.
BOOTP **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.	BOOTP is used to assign IP address dynamically on the network when the device powers up, instead of using permanently stored parameters. In order to use BOOTP, the user has to set up a BOOTP server, and define the IP address of the device in the table along with its MAC address. When the device powers up, it sends out BOOTP requests to get the IP address from the BOOTP server and starts its protocol stack. The OmniStack LS 6200 supports BOOTP operation. The BOOTP operation must be selected by management choice. When the BOOTP is activated, the configured IP address is ignored.
Dynamic assignment of IP addresses (DHCP/BootP)	Support for dynamic assignment of an IPv4 address to the switch. User can select IP address management method (Static / BootP / DHCP)
TFTP The device supports boot image, software and configuration upload/download via TFTP. **4.1.4**	The OmniStack LS 6200 supports the firmware code updating via the network with TFTP protocol. The TFTP file transfer can be started via the console command, or Web management. The system works normally while the file is transferred. When the code is updated successfully, the system restarts itself.
Configuration File Download and Upload	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.
Supported MIBs: Management Information Base – MIBs: A management information base (MIB) is a hierarchical database of objects that can be monitored and managed by a network management system. MIBs are used by network management protocols such as SNMP (Simple Network Management Protocol) and RMON (remote monitoring extensions to SNMP). The MIB format was standardized by the IETF as part of the SNMP specification, and all other types of MIBs are extensions to the original format. The switch supports MIB-I & MIB-II.	The OmniStack LS 6200 supports the following MIBs: MIB-II, Entity MIBs, and Radlan Private MIBs **Management Information Bases** • Bridge MIB (RFC 1493) o RFC1493 Bridge MIB ▪ Dot1dBase group ▪ Dot1dStp group ▪ Dot1dTp group (except dot1dTpHCPortTable, dot1dTpPortOverflowTable) ▪ Dot1dStatic group • Entity MIB (RFC 2737) o EntityPhysical group • Ether-like MIB (RFC 2665) o Dot3StatsTable group • Extensible SNMP Agents MIB (RFC 2742) • Forwarding Table MIB (RFC 2096) • IEEE 802.1w Rapid Reconfiguration Spanning Tree MIB • IEEE 802.3ad Link Aggregation MIB • IGMP MIB (RFC 2933) • Interface Group MIB (RFC 2233) • Interfaces Evolution MIB (RFC 2863) o IfXTable group o IfStackTable group • IP Multicasting related MIBs • MAU MIB (RFC 2668) • MIB II (RFC 1212, 1213) o RFC1213 standard MIB-II ▪ System group ▪ Interfaces group ▪ Ip group (except ipRouterTable (substitute by RFC 2096)) ▪ ICMPs group ▪ TCP group ▪ UDP group ▪ SNMP group • Port Access Entity MIB (IEEE 802.1x) • Private MIB • Quality of Service MIB • RADIUS Authentication Client MIB (RFC 2621) • RADIUS MIB (RFC 2618) o RadiusAuthClientMIB group • RMON MIB (RFC 2819)

	o RMON groups (e.g., 1, 2, 3 & 9) (RFC 2819) ▪ Statistics group ▪ History group ▪ Alarm group ▪ Event group • RMON II Probe Configuration Group (RFC 2021, partial implementation) • SNMP framework MIB (RFC 2571) • SNMP-MPD MIB (RFC 2572) • SNMP Target MIB, SNMP Notification MIB (RFC 2573) • SNMP User-Based SM MIB (RFC 2574) • SNMP View Based ACM MIB (RFC 2575) • SNMP Community MIB (RFC 2576) • TACACS+ Authentication Client MIB • TCP MIB (RFC 2013) • Trap (RFC 1215) • UDP MIB (RFC 2012) • Bridge MIB Extension (IEEE 802.1Q MIB RFC 2674) o P-bridge ▪ Dot1dExtBase group ▪ Dot1dPriority group (except dot1dUserPriorityRegenTable, dot1dPortOutBoundAccessPriority) ▪ Dot1dGarp group o Q-bridge ▪ Dot1qBase group ▪ Dot1qTp group (except dot1qTpGroupTable, dot1qForwardAllTable, dot1qForwardUnregisteredTable) ▪ Dot1qStatic group (except dot1qStaticMulticastTable) ▪ Dot1qVlane group (except dot1qqPortVlanStaticsTable, dot1qPortVlanHCStaticTable, dot1qLearningConstraintsTable)
Supported Traps	• Trap (RFC 1215) o ColdStart trap o WarmStart trap o LinkDown trap o LinkUp trap o AuthenticationFailure trap • Trap (RFC 1493) o NewRoot trap o TopologyChange trap • RMON groups (eg, 1, 2, 3 & 9) (RFC 2819) o RisingAlarm trap o FallingAlarm trap
Supported Standards	
The OmniStack LS 6200 complies with the following IEEE Standards	IEEE 802.1D STP/Bridging, 1993 IEEE 802.1Q Virtual LAN, 1998 IEEE 802.1Q/p Priority Tags IEEE 802.1s Multiple Spanning Tree Protocol IEEE 802.1x Port Authentication IEEE 802.1v; Protocol-based VLANs IEEE 802.1w Rapid Spanning Tree Protocol IEEE 802.3ac IEEE 802.3af IEEE 802.3 Ethernet IEEE 802.3ab 1000Base-T IEEE 802.3ad Link Aggregation Control Protocol IEEE 802.3x full duplex flow control support IEEE 802.3u Fast Ethernet / 100BASE-TX and 100BASE-FX IEEE 802.3z Gigabit Ethernet
The OmniStack LS 6200 complies with the following RFC Standards	RFC 792 (Future) RFC 1058 RFC 1212, RFC 1213, RFC 1215, RFC 1256 (Future) RFC 1305 RFC 1493 RFC 1517, RFC 1519 (Future) RFC 1724, RFC 1757 RFC 2012, RFC 2013, RFC 2021, RFC 2030, RFC 2096 RFC 2233 RFC 2328 (Future), RFC 2338 (Future)

	RFC 2453, RFC 2474, RFC 2475 RFC 2571, RFC 2572, RFC 2573, RFC 2574, RFC 2575, RFC 2576 RFC 2618, RFC 2621, RFC 2665, RFC 2668, RFC 2674 RFC 2737, RFC 2742, RFC 2787 (Future) RFC 2818, RFC 2819, RFC 2863, RFC 2865, RFC 2866, RFC 2867, RFC 2868, RFC 2869 RFC 2933 RFC 3164 RFC 3410, RFC 3411, RFC 3412, RFC 3413, RFC 3414, RFC 3415 RFC 3621