Dell™ PowerConnect™ 5324 System

User Guide

Notes, Notices, and Cautions

NOTE: A NOTE indicates important information that helps you make better use of your computer.

NOTICE: A NOTICE indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

CAUTION: A CAUTION indicates a potential for property damage, personal injury, or death.

Information in this document is subject to change without notice.

May 2007

Contents

1 Introduction

2 Hardware Description

3 Installing the PowerConnect Device

4 Starting and Configuring the Device

5 Using Dell OpenManage Switch Administrator

6 Configuring System Information

7 Configuring Device Information

9 Configuring Quality of Service

10 Device Specifications

Glossary

Figures

Tables

1

Introduction

NOTICE: Before proceeding, read the release notes for this product. The release notes can be downloaded from support.dell.com.

This User Guide contains the information needed for installing, configuring and maintaining the PowerConnect device.

PowerConnect 5324

The PowerConnect 5324 has 24 Gigabit Ethernet ports. There are also four SFP fiber ports that are designated as combo port alternatives to Ethernet ports 21-24. The combo ports are single ports with two physical connections. When one is connected the other is disabled.

Figure 1-1 and Figure 1-2 illustrates the PowerConnect 5324 front and back panels.

Figure 1-1. PowerConnect 5324 Front Panel

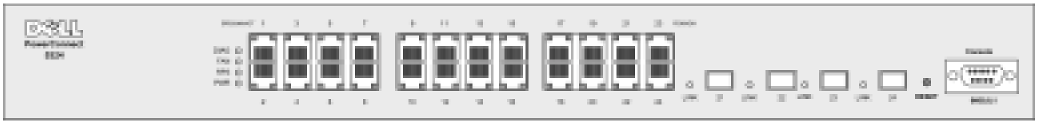
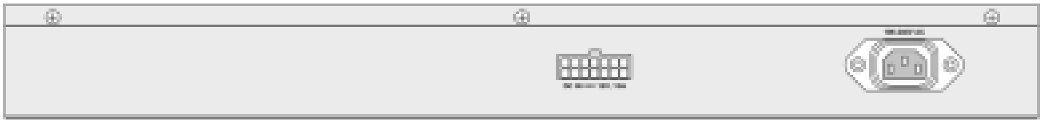


Figure 1-2. PowerConnect 5324 Back Panel



Features

This section describes the device user-configured features. For a complete list of all updated device features, refer to the latest software version Release Notes.

General Features

Head of Line Blocking

Head of Line (HOL) blocking results in traffic delays and frame loss caused by traffic competing for the same egress port resources. HOL blocking queues packets, and the packets at the head of the queue are forwarded before packets at the end of the queue.

Virtual Cable Testing (VCT)

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

Jumbo Frames Support

Jumbo frames enables transporting the identical data in fewer frames. Ensuring less overhead, lower processing time, and fewer interrupts.

For information on enabling Jumbo Frames, see "Defining General Device Information".

MDI/MDIX Support

The device supports auto-detection between crossed and straight-through cables.

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).

For information on configuring MDI/MDI for ports or Link Aggregate Groups (LAGs), see "Defining Port Parameters" or "Defining LAG Parameters".

Flow Control Support (IEEE 802.3X)

Flow control enables lower speed devices to communicate with higher speed devices, by requesting that the higher speed device refrains from sending packets. Transmissions are temporarily halted to prevent buffer overflows.

For information on configuring Flow Control for ports or LAGs, see "Defining Port Parameters" or "Defining LAG Parameters".

Back Pressure Support

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

For information on configuring Back Pressure for ports or LAGs, see "Defining Port Parameters" or "Defining LAG Parameters".

MAC Address Supported Features

MAC Address Capacity Support

The device supports up to eight thousand MAC addresses. The device reserves specific MAC addresses for system use.

Self-Learning MAC Addresses

The device enables automatic MAC address learning from incoming packets. The MAC addresses are stored in the Bridging Table.

Automatic Aging for MAC Addresses

MAC addresses from which no traffic is received for a given period are aged out. This prevents the Bridging Table from overflowing.

For more information on configuring the MAC Address Age Out Time, see "Configuring Address Tables".

Static MAC Entries

User defined static MAC entries are stored in the Bridging Table.

For more information, see "Configuring Address Tables".

VLAN-aware MAC-based Switching

Packets arriving from an unknown source address are sent to the microprocessor, where the source addresses are added to the Hardware Table. Packets addressed to or from this address are more efficiently forwarded using the Hardware Table.

MAC Multicast Support

Multicast service is a limited broadcast service, which allows one-to-many and many-to-many connections for information distribution. Layer 2 Multicast service is where a single frame is addressed to a specific Multicast address, from where copies of the frame are transmitted to the relevant ports.

For more information, see "Multicast Forwarding Support".

Layer 2 Features

IGMP Snooping

Internet Group Membership Protocol (IGMP) Snooping examines IGMP frame contents, when they are forwarded by the device from work stations to an upstream Multicast router. From the frame, the device identifies work stations configured for Multicast sessions, and which Multicast routers are sending Multicast frames.

For more information, see "IGMP Snooping".

Port Mirroring

Port mirroring monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from a monitored port to a monitoring port. Users specify which target port receives copies of all traffic passing through a specified source port.

For more information, see "Defining Port Mirroring Sessions".

Broadcast Storm Control

Storm Control enables limiting the amount of Multicast and Broadcast frames accepted and forwarded by the device.

When Layer 2 frames are forwarded, Broadcast and Multicast frames are flooded to all ports on the relevant VLAN. This occupies bandwidth, and loads all nodes connected on all ports.

For more information, see "Enabling Storm Control".

VLAN Supported Features

VLAN Support

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 based on a combination of the ingress port and packet contents. Packets sharing common attributes can be grouped in the same VLAN.

For more information, see "Configuring VLANs".

Port Based Virtual LANs (VLANs)

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

For more information, see "Defining VLAN Ports Settings".

IEEE802.1V Protocol Based Virtual LANs (VLANs)

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

For more information, see "Defining VLAN Protocol Groups".

Full 802.1Q VLAN Tagging Compliance

IEEE 802.1Q defines an architecture for virtual bridged LANs, the services provided in VLANs and the protocols and algorithms involved in the provision of these services. An important requirement included in this standard is the ability to mark frames with a desired Class of Service (CoS) tag value (0-7).

GVRP Support

GARP 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 device registers and propagates VLAN membership on all ports that are part of the active underlying "Spanning Tree Protocol Features" topology.

For more information, see "Configuring GVRP".

Spanning Tree Protocol Features

Spanning Tree Protocol (STP)

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

For more information, see "Configuring the Spanning Tree Protocol".

Fast Link

STP can take up to 30-60 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.

For more information enabling Fast Link for ports and LAGs, see "Defining STP Port Settings" or "Defining STP LAG Settings".

IEEE 802.1w Rapid Spanning Tree

Spanning Tree can take 30-60 seconds for each host to decide whether its ports are actively forwarding traffic. Rapid Spanning Tree (RSTP) detects uses of network topologies to enable faster convergence, without creating forwarding loops.

For more information, see "Configuring Rapid Spanning Tree".

Link Aggregation

For more information, see "Aggregating Ports".

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, set to full-duplex operation.

For more information, see "Defining LAG Membership".

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 to aggregators within the system.

For more information, see "Defining LACP Parameters".

Layer 3 Features

Address Resolution Protocol (ARP)

ARP is a TCP/IP protocol that converts IP addresses into physical addresses. ARP automatically determines Device Next-Hop MAC addresses of systems, including directly attached end systems. Users can override and supplement this by defining additional ARP Table entries.

For more information, see "Mapping Domain Host".

TCP

Transport Control Protocol (TCP) connections are defined between 2 ports by an initial synchronization exchange. TCP ports are identified by an IP address and a 16-bit port number. Octets streams are divided into TCP packets, each carrying a sequence number.

BootP and DHCP Clients

Dynamic Host Configuration Protocol (DHCP) enables additional 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.

For more information on DHCP, see "Defining DHCP IP Interface Parameters".

Quality of Service Features

Class Of Service 802.1p Support

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

For more information, see "Configuring Quality of Service".

Device Management Features

SNMP Alarms and Trap Logs

The system logs events with severity codes and timestamps. Events are sent as Simple Network Management Protocol (SNMP) traps to a Trap Recipient List.

For more information on SNMP Alarms and Traps, see "Defining SNMP Parameters".

SNMP Version 1 and Version 2

Simple Network Management Protocol (SNMP) over the UDP/IP protocol. To control 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.

Web Based Management

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.

Configuration File Download and Upload

PowerConnect 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.

For more information, see "Managing Files".

Trivial File Transfer Protocol (TFTP)

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

Remote Monitoring

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 current and historical MAC-layer statistics and control objects, allowing real-time information to be captured across the entire network.

For more information, see "Viewing RMON Statistics".

Command Line Interface

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

Syslog

Syslog is a protocol that allows event notifications to be sent to a set of remote servers, where they can be stored, examined and acted upon. Multiple mechanisms are implemented to send notification of significant events in real time, and keep a record of these events for after-the-fact usage.

For more information on Syslog, see "Managing Logs".

SNTP

The Simple Network Time Protocol (SNTP) assures accurate network device clock time synchronization up-to the millisecond. Time synchronization is performed by a network SNTP server. Time sources are established by Stratums. Stratums define the distance from the reference clock. The higher the stratum (where zero is the highest), the more accurate the clock.

For more information, see "Configuring SNTP Settings".

Traceroute

Traceroute enables discovering 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.

Security Features

SSL

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

Port Based Authentication (802.1x)

Port based authentication 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).

For more information, see "Configuring Port Based Authentication".

Locked Port Support

Locked Port 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.

For more information, see "Configuring Port Security".

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.

For more information, see "Configuring RADIUS Global Parameters".

SSH

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH version 1 is currently available. 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 Public Key cryptography for device connections and authentication.

TACACS+

TACACS+ provides centralized security for validation of users accessing the device. TACACS+ provides a centralized user management system, while still retaining consistency with RADIUS and other authentication processes.

For more information, see "Defining TACACS+ Settings".

Additional CLI Documentation

The CLI Reference Guide, which is available on the Documentation CD, provides information about the CLI commands used to configure the device. The document provides information including the CLI description, syntax, default values, guidelines, and examples.

Hardware Description

Device Port Configurations

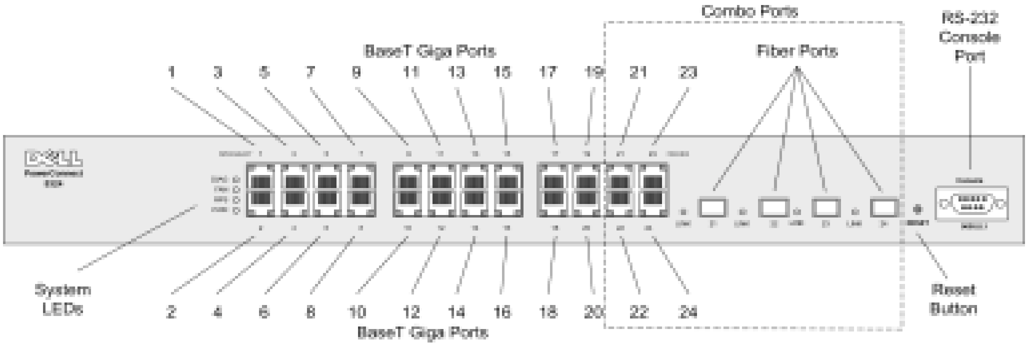
PowerConnect 5324 Front Panel Port Description

The PowerConnect 5324 device is configured with the following ports:

- **24 Copper ports** — RJ-45 ports designated as 10/100/1000 BaseT Gigabit Ethernet ports
- **4 Fiber ports** — Designated as Gigabit ports
- **Terminal port** — RS-232 console based port

The following figure illustrates the PowerConnect 5324 front panel.

Figure 2-3. PowerConnect 5324 Front Panel



The front panel contains ports1-24, which are copper based RJ-45 ports, designated as 10/100/1000 Mbps and support both Half and Full Duplex modes. There are four SFP fiber ports which are designated as Combo ports 21-24. A Combo port is a single logical port with two physical connections. Only one physical connection can be active at a time, so either the copper ports or the equivalent fiber ports 21-24 can be active, but they cannot both be active simultaneously. The upper row of ports are marked by odd numbers 1-23 and the lower row of ports are marked with even numbers 2-24.

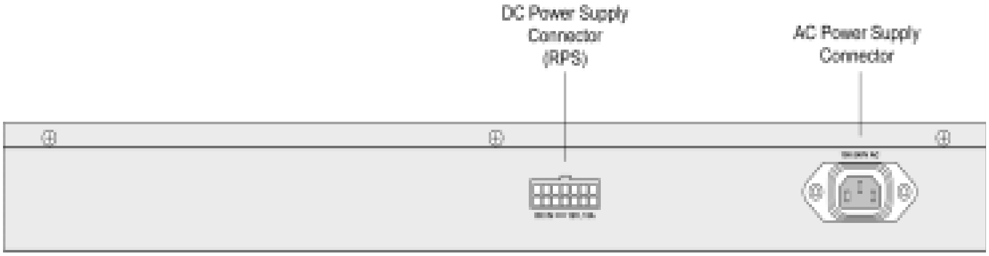
On the front panel is an RS-232 Console port, all the device LEDs and a Reset Button which is used to manually reset the device.

The device automatically detects whether the cable connected to an RJ-45 port is crossed or straight through, and functions either way.

PowerConnect Back Panel Port Description

The device back panel contains connectors for power, as illustrated in the Figure 2-4.

Figure 2-4. Device Back Panel



On the device back panel are two power supply connectors. For general use there is an AC Power Supply connector which is connectable to either 110V or 220V power supplies.

The DC Power Supply connector is to connect a Redundant Power Supply (RPS) to be activated automatically in the event of an AC power supply outage.

Device Ports

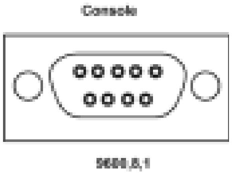
SFP Ports

The Small Form Factor Plugable (SFP) port is a hot swappable optical modular transceiver that offers high speed and compactness, which is designated as 1000Base-SX or LX.

RS-232 Console Port

One DB-9 connector for a serial terminal connection which is used for debugging, software download, etc. The default baud rate is 9600 bps. The baud rate can be configured from 2400 bps up to 38400 bps.

Figure 2-5. Console Port



Combo Ports

A combo port is a single logical port with two physical connections:

- A RJ-45 connection for Twisted Pair copper cabling
- A SFP connection for various fiber-based modules

Only one of the two physical connections of a combo port may be used at any one time. Port features and available port controls are determined by the physical connection used.

The system automatically detects the media used on a combo port, and utilizes this information in all operations and control interfaces.

If both RJ-45 and SFP are present, and a connector is inserted in the SFP port, the SFP port is active, unless the copper connector of the Base-T port of the same number is inserted and has a link.

The system can switch from the RJ-45 to the SFP (or vice-versa) without a system reboot or reset.

Physical Dimensions

The device has the following physical dimensions:

- Height — 44 mm (1.73 inch)
- Width — 440 mm (17.32 inch)
- Depth — 255 mm (10.03 inch)

LED Definitions

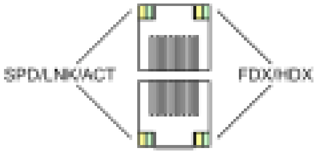
The front panel contains light emitting diodes (LED) that indicate the status of links, power supplies, fans, and system diagnostics.

Port LEDs

10/100/1000 Base-T Port LEDs

Each 10/100/1000 Base-T port has two LEDs. Speed/link/activity is indicated on the left LED and the duplex mode is indicated on the right LED.

Figure 2-6. RJ-45 Copper based 10/100/1000 BaseT LEDs



The RJ-45 LED indications are described in the following table:

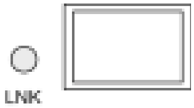
Table 2-1. RJ-45 Copper based 10/100/1000BaseT LED Indications

LED	Color	Description
Left LED	Green Static	The port is linked at 1000 Mbps.
	Green Flashing	The port is transmitting or receiving data at 1000 Mbps.
	Orange Static	The port is linked at either 10 or 100 Mbps.
	Orange Flashing	The port is transmitting or receiving data at either 10 or 100 Mbps.
Right LED	Green	The port is currently transmitting in Full Duplex mode.
	OFF	The port is operating in Half Duplex mode.

SFP LEDs

The SFP ports each have one LED marked as LNK.

Figure 2-7. SFP Port LED



The SFP port LED indications are described in the following table:

Table 2-2. SFP Port LED Indications

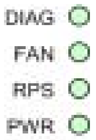
LED	Color	Description
SFP	Green Static	The port is currently up.
	Green Flashing	The port is currently transmitting or receiving data.
	OFF	The port is currently down.

When the SFP port is connected, the Duplex LED on the corresponding copper Combo port is Green.

System LEDs

The system LEDs, located on the left side of the front panel, provide information about the power supplies, fans, thermal conditions, and diagnostics. Figure 2-8 illustrates the system LEDs.

Figure 2-8. System LEDs



The following table describes the system LED indications.

Table 2-3. System LED Indications

LED	Color	Description
Diagnostics (DIAG)	Green Flashing	The system is currently running a diagnostic test.
	Green Static	The system passed the diagnostic test.
	Red Static	The system failed the diagnostic test.
Fan (FAN)	Green Static	The device fans are operating normally.
	Red Static	One or more fans are not operating.
Redundant Power Supply (RPS)	Green Static	The redundant power supply is currently operating.
	Red Static	The redundant power supply is not operating.
	OFF	The redundant power supply is not currently operating.
Main Power Supply (PWR)	Green Static	The main power supply is currently operating normally.
	OFF	The main power supply is not currently operating.
	Red	The main power supply has failed

Hardware Components

Power Supplies

The device has an internal power supply unit (AC unit) and a connector to connect the device to an external power supply unit (DC unit). The external unit provides redundancy and is called an RPS unit. To power up the device, only one power supply is required. Operation with both power supply units is regulated through load sharing.

Load sharing is where the device power requirements are devided between the two power supplies. If one power supply has an outage, the second power supply automatically continues providing power to the whole device.

Power supply LEDs indicate the power supply status. For more information on LEDs, see "LED Definitions".

AC Power Supply Unit

The AC power supply unit converts standard 220/110V AC 50/60 Hz to 5V DC at 5A, 12V DC at 3A. The unit automatically senses the available voltage rating (110 or 220V) and no setting is required.

The AC power supply unit uses a standard AC220/110V connector. LED indicator is on the front panel and indicates whether the AC unit is connected.

DC Power Supply Unit

An external DC power supply unit is used as a redundant power supply unit. Operation is possible with power supplied from this unit only. RPS600 connector type is used. No configuration is required. LED indicator is on the front panel and indicates whether DC unit is connected.

When the device is connected to a different power source, the probability of failure in the event of a power outage decreases.

Reset Button

The reset button, located on the front panel, manually resets the device.

Ventilation System

The device uses a fan system for cooling. Fan operational status can be verified by observing the LEDs that indicate if there is a faulty fan. For information, see "LED Definitions".

3

Installing the PowerConnect Device

This section contains information about device unpacking, location, installation, and cable connections.

Installation Precautions

⚠ **CAUTION Before performing any of the following procedures, read and follow the safety instructions located in the *System Information Guide* included in the Dell Documentation.**

⚠ **CAUTION Observe the following points before performing the procedures in this section:**

- Ensure that the rack or cabinet housing the device is adequately secured to prevent it from becoming unstable and/or falling over.
- Ensure that the power source circuits are properly grounded.
- Observe and follow the service markings. Do not service any device except as explained in the system documentation. Opening or removing covers marked with a triangular symbol with a lighting bolt may cause electrical shock. These components are to be serviced by trained service technicians only.
- Ensure that the power cable, extension cable, and/or plug is not damaged.
- Ensure that the device is not exposed to water.
- Ensure that the device is not exposed to radiators and/or heat sources.
- Ensure that the cooling vents are not blocked.
- Do not push foreign objects into the device, as it may cause a fire or electric shock.
- Use the device only with approved equipment.
- Allow the device to cool before removing covers or touching internal equipment.
- Ensure that the device does not overload the power circuits, wiring, and over-current protection. To determine the possibility of overloading the supply circuits, add together the ampere ratings of all switches installed on the same circuit as the device. Compare this total with the rating limit for the circuit.
- Do not install the device in an environment where the operating ambient temperature might exceed 40ºC (122ºF).
- Ensure that the airflow around the front, sides, and back of the device is not restricted.

Site Requirements

The device can be mounted in a standard 19-inch rack or placed on a tabletop. Before installing the device, verify that the location chosen for installation meets the site requirements.

- **General** — Ensure that the power supply is correctly installed.
- **Power** — The device is installed within 1.5 m (5 feet) of a grounded, easily accessible outlet 220/110 VAC, 50/60 Hz.
- **Clearance** — There is adequate frontal clearance for operator access. Allow clearance for cabling, power connections and ventilation.
- **Cabling** — Cabling is routed to avoid sources of electrical noise such as radio transmitters, broadcast amplifiers, power lines and fluorescent lighting fixtures.
- **Ambient Requirements** — The ambient unit operating temperature range is 0 to 40ºC (32 to 104ºF) at a relative humidity of 10% to 90%, non-condensing. Verify that water or moisture cannot enter the unit casing.

Unpacking

Package Contents

While unpacking the device, ensure that the following items are included:

- The device
- An AC power cable
- RS-232 crossover cable
- Self-adhesive rubber pads
- Rack mount kits for rack installation
- Documentation CD

Unpacking the Device

To unpack the device:

NOTE: Before unpacking the device, inspect the package and report any evidence of damage immediately.

NOTE: An ESD strap is not provided, however it is recommended to wear one for the following procedure.

1. Place the container on a clean, flat surface and cut all straps securing the container.
2. Open the container or remove the container top.
3. Carefully remove the device from the container and place it on a secure and clean surface.
4. Remove all packing material.

5 Inspect the device for damage. Report any damage immediately.

Mounting the Device

Overview

The power connectors for the device are positioned on the back panel. Connecting a DC Redundant Power Supply (UPS) is optional, but is recommended. The UPS DC connector is located on the back panel of the device.

Mounting the System

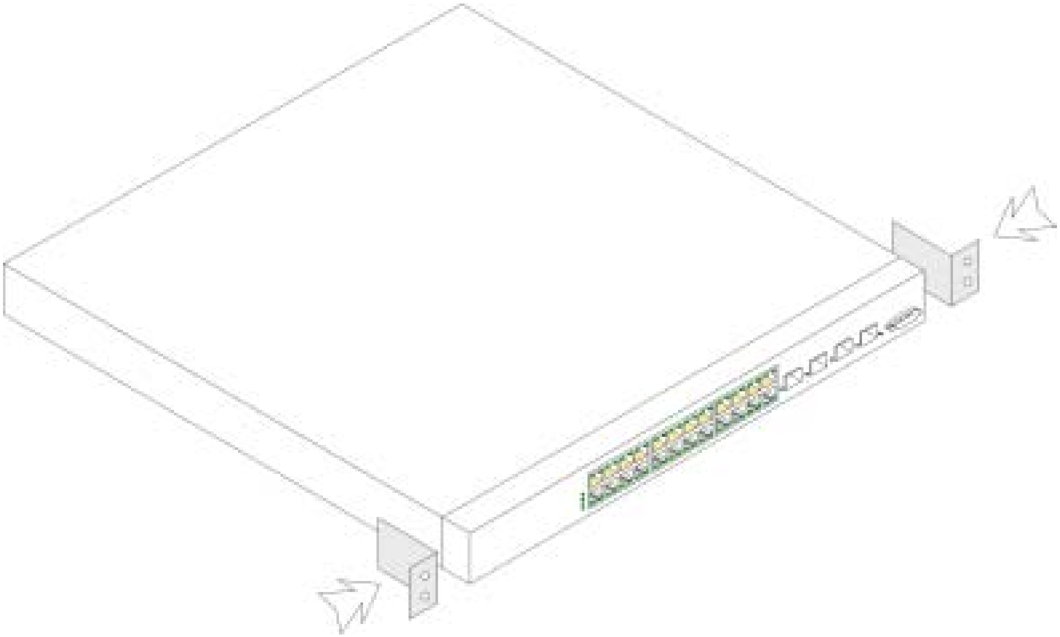
Device Rack Installation

⚠ **CAUTION: Disconnect all cables from the unit before mounting the device in a rack or cabinet.**

⚠ **CAUTION: When mounting multiple devices into a rack, mount the devices from the bottom up.**

1 Place the supplied rack-mounting bracket on one side of the device ensuring the mounting holes on the device line up to the mounting holes on the rack mounting bracket. Figure 3-9 illustrates where to mount the brackets.

Figure 3-9. Connection Rack Mounting Brackets



2 Insert the supplied screws into the rack mounting holes and tighten with a screwdriver.

3 Repeat the process for the rack-mounting bracket on the other side of the device.

4 Insert the unit into the 19-inch rack ensuring the rack-mounting holes on the device line up to the mounting hole on the rack.

5 Secure the unit to the rack with the rack screws (not provided). Fasten the lower pair of screws before the upper pair of screws. This ensures that the weight of the unit is evenly distributed during installation. Ensure that the ventilation holes are not obstructed.

Installing the Device without a Rack

The device must be installed on a flat surface if it is not installed on a rack. The surface must be able to support the weight of the device and the device cables.

1 Install rubber feet provided with the device.

2 Set the device on a flat surface, while leaving 2 inches (5.08cm) on each side and 5 inches (12.7cm) at the back.

3 Ensure that the device has proper ventilation.

Connecting the Device

To configure the device, the device must be connected to a terminal.

Connecting a Device to a Terminal

The device provides a Console port, that enables a connection to a terminal desktop system running terminal emulation software for monitoring and configuring the device. The Console port connector is a male DB-9 connector, implemented as a data terminal equipment (DTE) connector.

To use the Console port, the following is required:

- VT100 compatible terminal or a desktop or portable system with a serial port and running VT100 terminal emulation software.
- A RS-232 crossover cable with a female DB-9 connector for the Console port and the appropriate connector for the terminal.

To connect a terminal to the device Console port, perform the following:

1 Connect an RS-232 crossover cable to the terminal running VT100 terminal emulation software.

2 Ensure that the terminal emulation software is set as follows:

  a Select the appropriate serial port (serial port 1 or serial port 2) to connect to the console.

  b Set the data rate to 9600 baud.

  c Set the data format to 8 data bits, 1 stop bit, and no parity.

  d Set flow control to *non*e.

e Under **Properties**, select **VT100 for Emulation** mode.

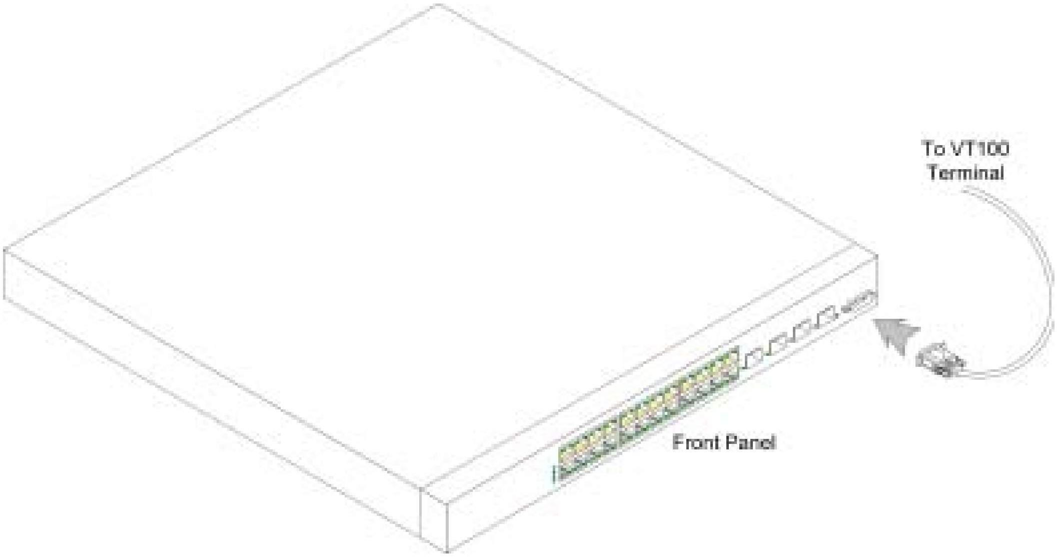
f Select **Terminal keys** for **Function, Arrow, and Ctrl keys**. Ensure that the setting is for **Terminal keys** *(not* **Windows keys**).

NOTICE: When using HyperTerminal with Microsoft® Windows 2000,ensure that Windows® 2000 Service Pack 2 or later is installed. With Windows 2000 Service Pack 2, the arrow keys function properly in HyperTerminal's VT100 emulation. Go to www.microsoft.com for information on Windows 2000 service packs.

3 Connect the female connector of the RS-232 crossover cable directly to the device Console port, and tighten the captive retaining screws.

The device Console port is located on the front panel.

Figure 3-10. Connecting to PowerConnect 5324 Console Port

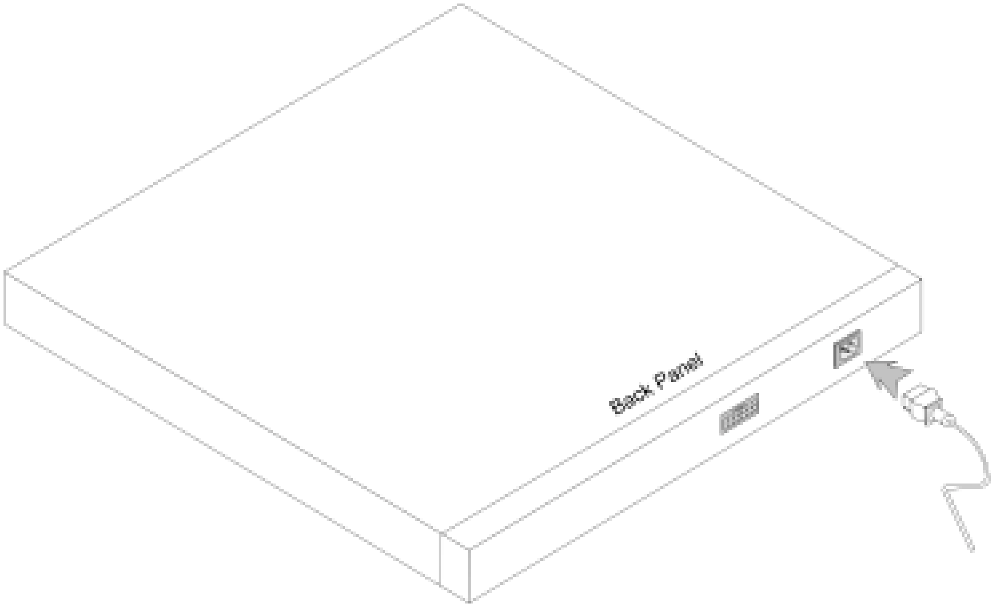


Connecting a Device to a Power Supply

1 Using a 5-foot (1.5 m) standard power cable with safety ground connected, connect the power cable to the AC connector located on the back panel.

2 Connect the power cable to a grounded AC outlet.

Figure 3-11. Connecting to Device Power Connector



Confirm that the device is connected and operating correctly by examining the LEDs on the front panel.

Port Connections, Cables, and Pinout Information

This section explains the device's physical interfaces, and provides information about port connections. Connector types, ports and cables are summarized in Ports, Connectors, and Cables. Copper Cable and Optical Transceiver Diagnostics are supported.

RJ-45 Connections for 10/100/1000BaseT Ports

The 10/100/1000BaseT ports are copper twisted-pair ports.

To establish a link for the twisted-pair ports, Tx pair on one cable end must be connected to the Rx pair on the other cable end, and vice versa. If the cabling is done such that Tx on one end is wired to Tx on the other end, and Rx is wired to Rx, a link is not established.

When selecting cables to connect the device ports to their networking peers, straight through cables must be used to connect the device to a station, and crossover cables must be used to connect one transmission device (switch or hub) to another. Both the straight through and crossover cables are category 5.

After a port is connected, its LINK indication LED is lit.

Table 3-4. Ports, Connectors and Cables

Connector	Port/Interface	Cable
RJ-45	10/100/1000BaseT Port	Cat.5

The RJ-45pin number allocation for the 10/100/1000BaseT ports is listed in the table following.

Table 3-5. RJ-45 Pin Number Allocation for 10/100/1000BaseT Ethernet Port

Pin No	Function
1	TxRx 1+
2	TxRx 1-
3	TxRx 2+
4	TxRx 2-
5	TxRx 3+
6	TxRx 3-
7	TxRx 4+
8	TxRx 4-

Port Default Settings

The general information for configuring the device ports includes the short description of the auto-negotiation mechanism and the default settings for switching ports.

Auto-Negotiation

Auto-negotiation enables automatic detection of speed, duplex mode and flow control on switching 10/100/1000BaseT ports. Auto-negotiation is enabled per port by default.

Auto-negotiation is a mechanism established between two link partners to enable a port to advertise its transmission rate, duplex mode and flow control (the flow control by default is disabled) abilities to its partner. The ports then both operate at the highest common denominator between them.

If connecting a NIC that does not support auto-negotiation or is not set to auto-negotiation, both the device switching port and the NIC must be manually set to the same speed and duplex mode.

If the station on the other side of the link attempts to auto-negotiate with a device 10/100/1000BaseT port that is configured to full duplex, the auto-negotiation results in the station attempting to operate in half duplex.

MDI/MDIX

The device supports auto-detection of straight through and crossed cables on all switching 10/100/1000BaseT ports. The feature is part of the Auto-negotiation and is enabled when Auto-negotiation is enabled.

When the MDI/MDIX (Media Dependent Interface with Crossover) is enabled, the automatic correction of errors in cable selection is possible, making the distinction between a straight through cable and a crossover cable irrelevant. (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.)

Flow Control

The device supports 802.3x Flow Control for ports configured with the Full Duplex mode. By default, this feature is disabled. It can be enabled per port. The flow control mechanism allows the receiving side to signal to the transmitting side that transmission must temporarily be halted to prevent buffer overflow.

Back Pressure

The device supports back pressure for ports configured to half duplex mode. By default, this feature is disabled. It can be enabled per port. The back pressure mechanism prevents the transmitting side from transmitting additional traffic temporarily. The receiving side may occupy a link so it becomes unavailable for additional traffic.

Switching Port Default Settings

The following table gives the port default settings.

Table 3-6. Port Default Settings

Function	Default Setting
Port speed and mode	10/100/1000BaseT copper: auto-negotiation 100 full duplex
Port forwarding state	Enabled
Port tagging	No tagging
Flow Control	Off (disabled on ingress)
Back Pressure	Off (disabled on ingress)

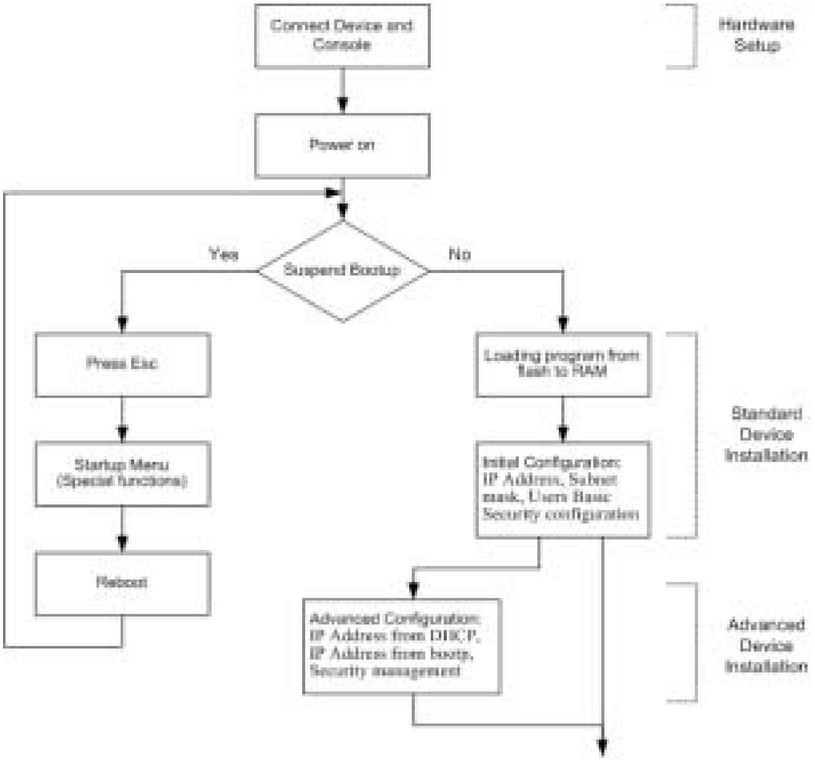
4

Starting and Configuring the Device

After completing all external connections, connect a terminal to the device to configure the device and for other procedures. For initial configuration, the standard device configuration is performed.

NOTE: Before proceeding, read the release notes for this product. The release notes can be downloaded from **www.support.dell.com**.

Figure 4-12. Installation and Configuration Flow


Connect Device and Console
Hardware Setup
Power on
Yes
Suspend Bootup
No
Press Esc
Startup Menu (Special functions)
Reboot
Loading program from flash to RAM
Standard Device Installation
Initial Configuration: IP Address, Subnet mask, Users Basic Security configuration
Advanced Configuration: IP Address from DHCP, IP Address from bootp, Security management
Advanced Device Installation

Configure the Terminal

To configure the device, the terminal must be running terminal emulation software.

Ensure that the terminal emulation software is set as follows:

1. Select the appropriate serial port (serial port 1 or serial port 2) to connect to the console.
2. Set the data rate to 9600 baud.
3. Set the data format to 8 data bits, 1 stop bit, and no parity.
4. Set flow control to **none**.
5. Under **Properties**, select **VT100 for Emulation** mode.
6. Select **Terminal keys** for **Function, Arrow, and Ctrl keys**. Ensure that the setting is for **Terminal keys** *(*not **Windows keys**).

NOTICE: When using HyperTerminal with Microsoft® Windows 2000,ensure that Windows® 2000 Service Pack 2 or later is installed.With Windows 2000 Service Pack 2, the arrow keys function properly in HyperTerminal's VT100 emulation. Go to www.microsoft.com for information on Windows 2000 service packs.

Booting the Device

NOTE: The assumed bootup information is as follows:

- The device is delivered with a default configuration.
- The device is not configured with a default user name and password.

To boot the device, perform the following:

1. Ensure that the device Serial port is connected to an ASCII terminal, or the serial connector of a desktop system running terminal emulation software.
2. Locate an AC power receptacle.
3. Switch off the AC power receptacle.
4. Connect the device to the AC receptacle. See "Connecting a Device to a Power Supply" .
5. Switch on the AC power receptacle.

When the power is turned on with the local terminal already connected, the device goes through Power On Self Test (POST). POST runs every time the device is initialized and checks hardware components to determine if the device is fully operational before completely booting. If a critical problem is detected, the program flow stops. If POST completes successfully, a valid executable image is loaded into RAM. POST messages are displayed on the terminal and indicate test success or failure.

1. Ensure that the ASCII cable is connected to the terminal, and that parameters on SW emulation are configured correctly.
2. Connect the power supply to the device.
3. Power on the device.
4. As the device boots, the bootup test first counts the device memory availability and then continues to boot. The following screen is an example of the displayed POST:

```
------ Performing the Power-On Self Test (POST) ------
UART Channel Loopback Test........................PASS
Testing the System SDRAM..........................PASS
Boot1 Checksum Test...............................PASS
Boot2 Checksum Test...............................PASS
Flash Image Validation Test.......................PASS

BOOT Software Version 1.0.0.20 Built  22-Jan-2004  15:09:28
Processor: FireFox 88E6218 ARM946E-S , 64 MByte SDRAM.
I-Cache 8 KB. D-Cache 8 KB. Cache Enabled.

Autoboot in 2 seconds - press RETURN or Esc. to abort and enter
prom.
Preparing to decompress...
```

The boot process runs approximately 90 seconds.

The auto-boot message displayed at the end of POST (see the last lines) indicates that no problems were encountered during boot.

During boot the **Startup** menu can be used to run special procedures. To enter the **Startup** menu, press <Esc> or <Enter> within the first two seconds after the auto-boot message is displayed.

If the system boot process is not interrupted by pressing <Esc> or <Enter>, the process continues decompressing and loading the code into RAM. The code starts running from RAM and the list of numbered system ports and their states (up or down) are displayed.

The following screen is an example configuration. Items such as addresses, versions, and dates may differ for each device.

```
Decompressing SW from image-2
78c000
OK
Running from RAM...

*********************************************************************
*** Running  SW  Ver. 1.0.0.15  Date  03-Mar-2004  Time  10:41:14 ***
*********************************************************************
```

```
HW version is 00.01.07
Base Mac address is: 00:00:07:77:77:77
Dram size is  : 64M bytes
Dram first block size is  : 40960K bytes
Dram first PTR is  : 0x1800000
Flash size is: 16M
Device configuration:
Prestera based system
Slot 1 - Neyland24 HW Rev. 0.1
Tapi Version: v1.2.9
Core Version: v1.2.9
01-Jan-2000 01:01:32 %INIT-I-InitCompleted: Initialization task is
completed


console> 01-Jan-2000 01:01:35 %LINK-W-Down:  g1
01-Jan-2000 01:01:35 %LINK-W-Down:  g2
01-Jan-2000 01:01:35 %LINK-W-Down:  g3
01-Jan-2000 01:01:35 %LINK-W-Down:  g4
01-Jan-2000 01:01:35 %LINK-W-Down:  g5
01-Jan-2000 01:01:35 %LINK-W-Down:  g6
01-Jan-2000 01:01:35 %LINK-W-Down:  g7
01-Jan-2000 01:01:35 %LINK-W-Down:  g8
01-Jan-2000 01:01:35 %LINK-W-Down:  g9
01-Jan-2000 01:01:35 %LINK-W-Down:  g10
01-Jan-2000 01:01:35 %LINK-W-Down:  g11
01-Jan-2000 01:01:35 %LINK-W-Down:  g12
01-Jan-2000 01:01:35 %LINK-W-Down:  g13
01-Jan-2000 01:01:36 %LINK-W-Down:  g14
01-Jan-2000 01:01:36 %LINK-W-Down:  g15
01-Jan-2000 01:01:36 %LINK-W-Down:  g16
01-Jan-2000 01:01:36 %LINK-W-Down:  g17
```

```
01-Jan-2000 01:01:36 %LINK-W-Down:  g18
01-Jan-2000 01:01:36 %LINK-W-Down:  g19
01-Jan-2000 01:01:36 %LINK-W-Down:  g20
01-Jan-2000 01:01:36 %LINK-W-Down:  g21
01-Jan-2000 01:01:36 %LINK-W-Down:  g22
01-Jan-2000 01:01:36 %LINK-I-Up:  Vlan 3000
01-Jan-2000 01:01:36 %LINK-I-Up:  Vlan 1
01-Jan-2000 01:01:36 %LINK-I-Up:  g1
01-Jan-2000 01:01:36 %LINK-I-Up:  g13
01-Jan-2000 01:01:36 %LINK-I-Up:  g14
01-Jan-2000 01:01:36 %LINK-I-Up:  g19
01-Jan-2000 01:01:36 %LINK-I-Up:  g20
01-Jan-2000 01:01:36 %LINK-I-Up:  g21
01-Jan-2000 01:01:36 %LINK-W-Down:  g23
01-Jan-2000 01:01:36 %LINK-W-Down:  g24
01-Jan-2000 01:01:36 %LINK-W-Down:  ch1
01-Jan-2000 01:01:36 %LINK-I-Up:  Vlan 1000
01-Jan-2000 01:01:36 %TRUNK-I-PORTADDED: Port g24 added to ch1
01-Jan-2000 01:01:36 %LINK-I-Up:  g22
01-Jan-2000 01:01:36 %LINK-I-Up:  g23
01-Jan-2000 01:01:36 %LINK-I-Up:  g24
01-Jan-2000 01:01:36 %LINK-I-Up:  ch1
01-Jan-2000 01:01:36 %LINK-W-Down:  g1
01-Jan-2000 01:03:42 %INIT-I-Startup: Cold Startup

console>
```

After the device boots successfully, a system prompt is displayed (`console>`) which is used to configure the device. However, before configuring the device, ensure that the latest software version is installed on the device. If it is not the latest version, download and install the latest version. For more information on downloading the latest version, see the "Software Download" .

Configuration Overview

Before assigning a static IP address to the device, obtain the following information:

- A specific IP address that has been allocated to the device in order for it to be configured.
- Default route.
- Network mask for the network.

There are two configuration types:

- **Initial Configuration** — Consists of configuration functions with basic security considerations.
- **Advanced Configuration** — Consists of dynamic IP configuration and more advanced security considerations.

NOTE: After making any configuration changes, the new configuration must be saved before rebooting. To save the configuration, enter:

```
console# copy running-config startup-config
```

Initial Configuration

NOTE: Before proceeding, read the release notes for this product. The release notes can be downloaded from Dell support website at **support.dell.com**.

NOTE: The initial simple configuration uses the following assumptions:

- The PowerConnect device was never configured before, and is in the same state as when it was received.
- The PowerConnect device booted successfully.
- The Serial connection is established and the console prompt is displayed on the screen of a VT100 terminal device. (Press the <Enter> key several times to verify that the prompt displays correctly.)
- The device is not configured with a default user name and password.

The initial device configuration is through the Serial port. After the initial configuration, the device can then be managed either from the already connected Serial port or remotely through an interface defined during the initial configuration.

The initial configuration consists of the following:

- Setting the user name 'admin', password as 'dell' with the highest privilege level of 15.
- Configuring the static IP address and the default gateway.
- Configuring the SNMP read/write community string.
- Assigning the IP address allocated by the DHCP server.

Before applying the initial configuration procedure to the PowerConnect device, the following information must be obtained from the network administrator:

- The IP address to be assigned to a VLAN through which the device is managed.

- The IP subnet mask for the network.
- The default gateway IP address.
- The SNMP community.

Static IP Address and Subnet Mask

An IP address can be configured on any interface, including a VLAN, a LAG, and a physical port. After entering the configuration command, it is recommended to check if a port was configured with the IP address by entering the **show ip interface** command.

Important: If an IP address is configured on a LAG or physical port (ex. g10), that interface is removed from VLAN 1.

Static Route Configuration

To manage the device from a remote network a static route must be configured, which is an IP address to where packets are sent when no entries are found in the device tables. The configured IP address must belong to the same subnet as one of the device IP interfaces.

To configure a static route, enter the command at the system prompt as shown in the following configuration example where 100.1.1.1 (mask 24) is the specific management station, and 100.1.1.10 is the static route which acts as the default gateway.

Assigning Static IP Addresses on an Inband Interface

NOTE: This example uses the following assumptions:

- The IP address to be assigned to the PowerConnect VLAN interface is 192.168.1.123
- The IP subnet mask for the network is 255.255.255.0
- The IP address of the default route is 192.168.1.1
- The read/write SNMP community string is "private"

```
console> enable

console# configure

console(config)# username admin password dell level 15

console(config)# interface VLAN 1

console (config-if) # ip address 192.168.1.123 /24

console (config-if) # exit

console (config) # ip default-gateway 192.168.1.1

console (config) # snmp-server community private rw

console(config)# exit

console#
```

Verifying the IP and Default Gateway Addresses

Ensure that the IP address and the default gateway are properly assigned by executing the following command and examining its output:

Command

```
console# show ip interface vlan 1
```

Output

```
Gateway IP Address       Activity status
---------------------    ------------------
192.168.1.1              Active

IP address               Interface           Type
-------------------      ------------        ------------
192.168.1.123 /24         VLAN 1              Static
```

NOTE: It is recommended that the most recent revision of the user documentation is downloaded from the Dell support website at **support.dell.com**.

User Name

To manage the device remotely, for example through SSH, Telnet, or the Web interface, a user name must be configured. To gain complete administrative control over the device the highest priviledge (15) must be specified.

NOTE: Only the administrator (super-user) with the highest priviledge level (15) is allowed to manage the device through the Web browser interface.

For more information about the privilege level, see the "CLI Reference Guide".

The configured user name is entered as a login name for remote management sessions. To configure user name and privilege level, enter the command at the system prompt as shown in the configuration example:

```
console> enable
console# configure
console(config)# username admin password abc level 15
```

SNMP Community Strings

Simple Network Management Protocol (SNMP) provides a method for managing network devices. Devices supporting SNMP run a local software (agent). The SNMP agents maintain a list of variables, used to manage the device. The variables are defined in the Management Information Base (MIB). The MIB presents the variables controlled by the agent. The SNMP agent defines the MIB specification format, as well as the format used to access the information over the network. Access rights to the SNMP agents are controlled by access strings and SNMP community strings.

The device is SNMP-compliant and contains an SNMP agent that supports a set of standard and private MIB variables. Developers of management stations require the exact MIB tree structure and receive the complete private MIBs information before being able to manage the MIBs.

All parameters are manageable from any SNMP management platform, except the SNMP management station IP address, community name, and access rights. The SNMP management access to the device is disabled if no community strings exist.

NOTE: The device is delivered with no community strings configured. SNMPv1 and SNMPv2 are supported on the device. This section describes SNMPv1/v2 configuration parameters.

The following screen displays the default device configuration:

```
Console# show snmp


Community-       Community-Access  IP address
String
--------------   ---------------   ----------------------------


Traps are enabled.
Authentication trap is enabled.


Trap-Rec-        Trap-Rec-         Version
Address          Community


System Contact:
System Location:
```

During the initial configuration procedure the community-string, community-access, and IP address can be set through the local terminal.

The SNMP configuration options are:

- Community string.

- **Read Only** — Indicates that the community members can view configuration information, but cannot change any information.
- **Read/Write** — Indicates that the community members can view and modify configuration information.
- **Super** — Indicates that the community members have administration access.

- Configurable IP address. If IP address is not configured, all community members with the same community name are granted the same access rights.

Common practice is to use two community strings for the device — one (public community) with read-only access and the other (private community) with read-write access. The public string allows authorized management stations to retrieve MIB objects, while the private string allows authorized management stations to retrieve and modify MIB objects.

During initial configuration, it is recommended to configure the device according to the network administration requirements, in accordance with using an SNMP-based management station.

Configuring SNMP

To configure SNMP station IP address and community string(s) for the general device router tables, perform the following steps.

1. At the console prompt, enter the command `Enable`. The prompt is displayed as `#`.
2. Enter the command `configure` and press <Enter>.
3. In the configuration mode, enter the SNMP configuration command with the parameters including community name (private), community access right (read and write) and IP address, as shown in the example below:

```
console# configure
config(config)# snmp-server community private rw 11.1.1.2
```

Viewing SNMP Community Tables

To view SNMP station IP address and community tables:

1. At the console prompt, enter the command `exit`. The prompt is displayed as `#`.
2. In the Privileged Exec mode, enter the show command as shown in the example below:

The configured parameters enable further device configuration from any remote location.

```
Console# show snmp

Community-       Community-Access  IP address
String
---------------  ----------------  -----------------------------
private          read write        11.1.1.2

Traps are enabled.
Authentication trap is enabled.

Trap-Rec-        Trap-Rec-         Version
Address          Community

System Contact:
System Location:
```

Advanced Configuration

This section provides information about dynamic allocation of IP addresses and security management based on the authentication, authorization, and accounting (AAA) mechanism, and includes the following topics:

- Configuring IP Addresses through DHCP
- Configuring IP Addresses through BOOTP
- Security Management and Password Configuration

When configuring/receiving IP addresses through DHCP and BOOTP, the configuration received from these servers includes the IP address, and may include subnet mask and default gateway.

Retrieving an IP Address From a DHCP Server

When using the DHCP protocol to retrieve an IP address, the device acts as a DHCP client. When the device is reset, the DHCP command is saved in the configuration file, but not the IP address. To retrieve an IP address from a DHCP server, perform the following steps:

1 Select and connect any port to a DHCP server or to a subnet that has a DHCP server on it, in order to retrieve the IP address.

2 Enter the following commands to use the selected port for receiving the IP address. In the following example, the commands are based on the port type used for configuration.

- Assigning Dynamic IP Addresses:

```
console# configure
console(config)# interface ethernet g1
console(config-if)# ip address dhcp hostname device
console(config-if)# exit
console(config)#
```

- Assigning Dynamic IP Addresses (on a VLAN):

```
console# configure
console(config)# interface ethernet vlan 1
console(config-if)# ip address dhcp hostname device
console(config-if)# exit
console(config)#
```

3 To verify the IP address, enter the **show ip interface** command at the system prompt as shown in the following example.

```
Console# show ip interface

Gateway IP Address      Activity status
---------------------   ------------------
10.7.1.1                Active



IP address              Interface           Type
-------------------     ------------        ------------
10.7.1.192/24           VLAN 1              Static
10.7.2.192/24           VLAN 2              DHCP
```

NOTE: It is not necessary to delete the device configuration to retrieve an IP address from the DHCP server.

NOTE: When copying configuration files, avoid using a configuration file that contains an instruction to enable DHCP on an interface that connects to the same DHCP server, or to one with an identical configuration. In this instance, the device retrieves the new configuration file and boots from it. The device then enables DHCP as instructed in the new configuration file, and the DHCP instructs it to reload the same file again.

Receiving an IP Address From a BOOTP Server

The standard BOOTP protocol is supported and enables the device to automatically download its IP host configuration from any standard BOOTP server in the network. In this case, the device acts as a BOOTP client.

To retrieve an IP address from a BOOTP server:

1. Select and connect any port to a BOOTP server or subnet containing such a server, to retrieve the IP address.

2. At the system prompt, enter the **delete startup configuration** command to delete the Startup Configuration from flash.

   The device reboots with no configuration and in 60 seconds starts sending BOOTP requests. The device receives the IP address automatically.

NOTE: When the device reboot begins, any input at the ASCII terminal or keyboard automatically cancels the BOOTP process before completion and the device does not recieve an IP address from the BOOTP server.

The following example illustrates the process:

```
console> enable
```

```
console# delete startup-config

Startup file was deleted

console# reload

You haven’t saved your changes. Are you sure you want to continue (y/n)
[n]?

This command will reset the whole system and disconnect your current
session. Do you want to continue (y/n) [n]?

******************************************************

/* the switch reboots */
```

To verify the IP address, enter the **show ip interface** command.

The device is now configured with an IP address.

Security Management and Password Configuration

System security is handled through the Authentication, Authorization, and Accounting (AAA) mechanism that manages user access rights, privileges, and management methods. AAA uses both local and remote user databases. Data encryption is handled through the SSH mechanism.

The system is delivered with no default password configured. All passwords are user-defined. If a user-defined password is lost, a password recovery procedure can be invoked from the **Startup** menu. The procedure is applicable for the local terminal only and allows a one-time access to the device from the local terminal with no password entered.

Configuring Security Passwords

The security passwords can be configured for the following services:

- Terminal
- Telnet
- SSH
- HTTP
- HTTPS

NOTE: Passwords are user-defined.

NOTE: When creating a user name, the default priority is 1, which allows access but not configuration rights. A priority of 15 must be set to enable access and configuration rights to the device. Although user names can be assigned privilege level 15 without a password, it is recommended to always assign a password. If there is no specified password, privileged users can access the Web interface with any password.

Configuring an Initial Terminal Password

To configure an initial terminal password, enter the following commands:

```
console(config)# aaa authentication login default line
console(config)# aaa authentication enable default line
console(config)# line console
console(config-line)# login authentication default
console(config-line)# enable authentication default
console(config-line)# password george
```

- When initially logging on to a device through a terminal session, enter **george** at the password prompt.
- When changing a device's mode to enable, enter **george** at the password prompt.

Configuring an Initial Telnet Password

To configure an initial Telnet password, enter the following commands:

```
console(config)# aaa authentication login default line
console(config)# aaa authentication enable default line
console(config)# line telnet
console(config-line)# login authentication default
console(config-line)# enable authentication default
console(config-line)# password bob
```

- When initially logging onto a device through a Telnet session, enter **bob** at the password prompt.
- When changing a device mode to enable, enter **bob**.

Configuring an Initial SSH Password

To configure an initial SSH password, enter the following commands:

```
console(config)# aaa authentication login default line
console(config)# aaa authentication enable default line
console(config)# line ssh
console(config-line)# login authentication default
console(config-line)# enable authentication default
console(config-line)# password jones.
```

- When initially logging onto a device through a SSH session, enter `jones` at the password prompt.
- When changing a device's mode to enable, enter `jones`.

Configuring an Initial HTTP Password

To configure an initial HTTP password, enter the following commands:

```
console(config)# ip http authentication local
console(config)# username admin password user1 level 15
```

Configuring an Initial HTTPS Password

To configure an initial HTTPS password, enter the following commands:

```
console(config)# ip https authentication local
console(config)# username admin password user1 level 15
```

Enter the following commands once when configuring to use a terminal, a Telnet, or an SSH session in order to use an HTTPS session.

NOTE: In the Web browser enable SSL 2.0 or greater for the page content to be displayed.

```
console(config)# crypto certificate generate key_generate
console(config)# ip https server
```

When initially enabling an http or https session, enter `admin` for user name and `user1` for password.

NOTE: Http and Https services require level 15 access and connect directly to the configuration level access.

Startup Procedures

Startup Menu Procedures

The procedures called from the Startup menu cover software download, flash handling and password recovery. The diagnostics procedures are for use by technical support personnel *only* and are not disclosed in the document.

The Startup menu can be entered when booting the device – a user input must be entered immediately after the POST test.

To enter the Startup menu:

1 Turn the power on and watch for the auto-boot message.

```
**************************************************
*****************  SYSTEM RESET  *****************
```

```
**************************************************



------ Performing the Power-On Self Test (POST) ------

UART Channel Loopback Test........................PASS
Testing the System SDRAM..........................PASS
Boot1 Checksum Test...............................PASS
Boot2 Checksum Test...............................PASS
Flash Image Validation Test.......................PASS



BOOT Software Version 1.0.0.20 Built  22-Jan-2004  15:09:28
Processor: FireFox 88E6218 ARM946E-S , 64 MByte SDRAM.
I-Cache 8 KB. D-Cache 8 KB. Cache Enabled.

Autoboot in 2 seconds - press RETURN or Esc. to abort and enter
prom.
Preparing to decompress...
```

2 When the auto-boot message appears, press <Enter> to get the Startup menu. The Startup menu procedures can be done using the ASCII terminal or Windows HyperTerminal.

```
[1]  Download Software
[2]  Erase Flash File
[3]  Password Recovery Procedure
[4]  Enter Diagnostic Mode
[5]  Set Terminal Baud-Rate
[6]  Back
Enter your choice or press 'ESC' to exit
```

The following sections describe the available Startup menu options.

NOTE: When selecting an option form the Startup menu, time out must be taken into account: if no selection is made within 35 seconds (default), the device times out. This default value can be changed through CLI.

Software Download

The software download procedure is performed when a new version must be downloaded to replace the corrupted files, update or upgrade the system software. To download software from the Startup menu:

1 From the Startup menu, `press [1]`. The following prompt appears:

```
Downloading code using XMODEM
```

2 When using the HyperTerminal, click **Transfer** on the HyperTerminal Menu Bar.

3 In the **Filename** field, enter the file path for the file to be downloaded.

4 Ensure that the **Xmodem** protocol is selected in the **Protocol** field.

5 Press **Send**. The software is downloaded.

NOTE: After software download, the device reboots automatically.

NOTE: The length of time taken by the download varies according to the tool used.

Erase FLASH File

In some cases, the device configuration must be erased. If the configuration is erased, all parameters configured via CLI, EWS or SNMP must be reconfigured.

Erasing the Device Configuration

1 From the Startup menu, `press [2]` within two seconds to erase flash file. The following message is displayed:

```
Warning! About to erase a Flash file.

Are you sure (Y/N)? y
```

2 Press **Y**. The following message is displayed.

```
Write Flash file name (Up to 8 characters, Enter for none.):config

File config (if present) will be erased after system
initialization

======== Press Enter To Continue ========
```

3 Enter `config` as the name of the flash file. The configuration is erased and the device reboots.

4 Repeat the device initial configuration.

Password Recovery

If a password is lost, the Password Recovery procedure can be called from the Startup menu. The procedure enables entry to the device once without password.

To recover a lost password for the local terminal only:

1 From the Startup menu, type **3** and press <Enter>.

The password is deleted.

NOTE: To ensure device security, reconfigure passwords for applicable management methods.

Software Download Through TFTP Server

This section contains instructions for downloading device software (system and boot images) through a TFTP server. The TFTP server must be configured before beginning to download the software.

System Image Download

The device boots and runs when decompressing the system image from the flash memory area where a copy of the system image is stored. When a new image is downloaded, it is saved in the other area allocated for the other system image copy.

On the next boot, the device will decompress and run the currently active system image unless chosen otherwise.

To download a system image through the TFTP server:

1 Ensure that an IP address is configured on one of the device ports and pings can be sent to a TFTP server.

2 Make sure that the file to be downloaded is saved on the TFTP server (the `ros` file).

3 Enter `show version` to verify which software version is currently running on the device. The following is an example of the information that appears:

```
console# show version

SW version   1.0.0.42 (date 22-Jul-2004 time 13:42:41)

Boot version 1.0.0.18 (date 01-Jun-2004 time 15:12:20)

HW version
```

4 Enter `show bootvar` to verify which system image is currently active. The following is an example of the information that appears:

```
console# sh bootvar

Images currently available on the Flash

Image-1 active (selected for next boot)

Image-2 not active

console#
```

5 Enter `copy tftp://{tftp address}/{file name} image` to copy a new system image to the device. When the new image is downloaded, it is saved in the area allocated for the other copy of system image (image-2, as given in the example). The following is an example of the information that appears:

```
console# copy tftp://176.215.31.3/file1.ros image

Accessing file ‘file1’ on 176.215.31.3Ö

Loading file1 from 176.215.31.3:

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Copy took 00:01:11 [hh:mm:ss]
```

Exclamation symbols indicate that a copying process is in progress. Each symbol (!) corresponds to 512 bytes transferred successfully. A period indicates that the copying process is timed out. Many periods in a row indicate that the copying process failed.

6 Select the image for the next boot by entering the `boot system` command. After this, enter `show bootvar` to verify that the copy indicated as a parameter in the `boot system` command is selected for the next boot.

The following is an example of the information that appears on the screen.

```
console# boot system image-2

console# sh boot

Images currently available on the Flash

Image-1 active

Image-2 not active (selected for next boot)
```

If the image for the next boot is not selected by entering the **`boot system`** command, the system boots from the currently active image.

7 Enter the `reload` command. The following message is displayed:

```
console# reload

This command will reset the whole system and disconnect your current

session. Do you want to continue (y/n) [n]?
```

8 Enter `y`. The device reboots.

Boot Image Download

Loading a new boot image from the TFTP server and programming it into the flash updates the boot image. The boot image is loaded when the device is powered on. A user has *no* control over the boot image copies. To download a boot image through the TFTP server:

1 Ensure that an IP address is configured on one of the device ports and pings can be sent to a TFTP server.

2 Ensure that the file to be downloaded is saved on the TFTP server (the `rfb` file).

3 Enter `show version` to verify which software version is currently running on the device. The following is an example of the information that appears:

```
console# sh ver

SW version   1.0.0.42 (date 22-Jul-2004 time 13:42:41)

Boot version 1.0.0.18 (date 01-Jun-2004 time 15:12:20)

HW version 00.00.01 (date 01-May-2004 time 12:12:20)
```

4 Enter `copy tftp://{tftp address}/{file name} boot` to copy the boot image to the device. The following is an example of the information that appears:

```
  console# copy tftp://176.215.31.3/332448-10018.rfb boot

  Erasing file..done.

  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Copy: 2739187 bytes copied in 00:01:13 [hh:mm:ss]
```

5 Enter the `reload` command. The following message is displayed:

```
console# reload

This command will reset the whole system and disconnect your
current

session. Do you want to continue (y/n) [n]?
```

6 Enter `y`.

The device reboots.

5

Using Dell OpenManage Switch Administrator

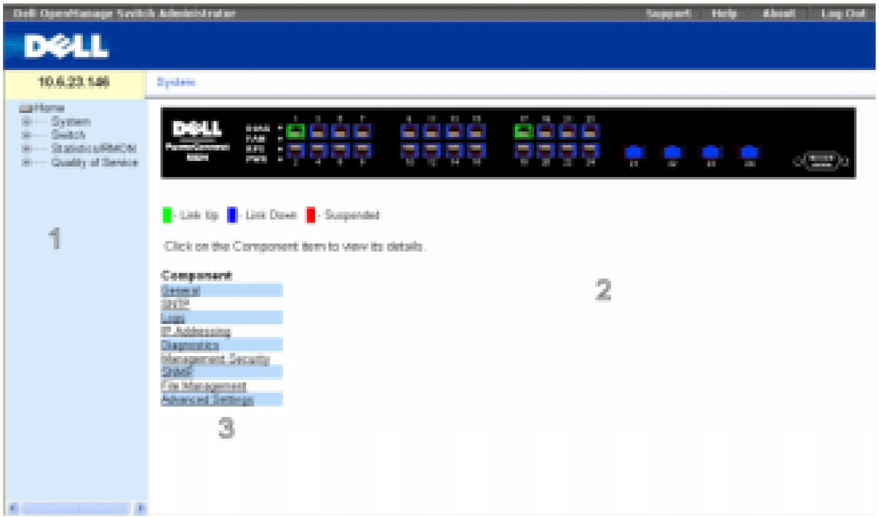
This section provides an introduction to the user interface.

Understanding the Interface

The home page contains the following views:

- Tree View — Located on the left side of the home page, the tree view provides an expandable view of the features and their components.
- Device View — Located on the right side of the home page, the device view provides a view of the device, an information or table area, and configuration instructions.

Figure 5-13. Switch Administrator Components



Click on the Component item to view its details.

Table 5-7 lists the interface components with their corresponding numbers.

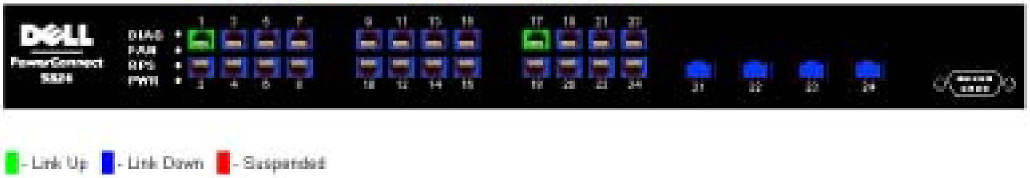
Table 5-7. Interface Components

Component	Name
1	The tree view contains a list of the different device features. The branches in the tree view can be expanded to view all the components under a specific feature, or retracted to hide the feature's components. By dragging the vertical bar to the right, the tree area can be expanded to display the full name of a component.
2	The device view provides information about device ports, current configuration and status, table information, and feature components. Depending on the option selected, the area at the bottom of the device view displays other device information and/or dialogs for configuring parameters.
3	The components list contains a list of the feature components. Components can also be viewed by expanding a feature in the tree view.
4	The information buttons provide access to information about the device and access to Dell Support. For more information, see "Information Buttons."

Device Representation

The PowerConnect home page contains a graphical device representation of the front panel.

Figure 5-14. Port LED Indicators



The port coloring indicates if a specific port is currently active. Ports can be the following colors:

Table 5-8. Led Indicators

Component	Name
Port Indicators	
Green	The port is currently enabled.
Red	An error has occurred on the port.
Blue	The port is currently disabled.

NOTE: The Port LEDs are not reflected in PowerConnect front panel in the PowerConnect OpenManage Switch Administrator. LED status can only be determined by viewing the actual device. For more information about LEDs, see "LED Definitions".

Using the Switch Administrator Buttons

This section describes the buttons found on the OpenManage Switch Administrator interface.

Information Buttons

Information buttons provide access to on-line support and online help, as well as information about the OpenManage Switch Administrator interfaces.

Table 5-9. Information Buttons

Button	Description
Support	Opens the Dell Support page at **support.dell.com.**
Help	Online help containing information to assist in configuring and managing the device. The online help pages are linked directly to the page currently open. For example, if the **IP Addressing** page is open, the help topic for that page opens when **Help** is clicked.
About	Contains the version and build number and Dell copyright information.
Log Out	Logs out of the application and closes the browser window.

Device Management Buttons

Device Management buttons provide an easy method of configuring device information, and includes the following:

Table 5-10. Device Management Buttons

Button	Description
Apply Changes	Applies changes to the device.
Add	Adds information to tables or dialogs.
Telnet	Starts a Telnet session.
Query	Queries tables.
Show All	Displays the device tables.
Left arrow/Right arrow	Moves information between lists.
Refresh	Refreshes device information.
Reset All Counters	Clears statistic counters.
Print	Prints the **Network Management System** page and/or table information.
Show Neighbors Info	Displays the **Neighbors List** from the **Neighbors Table** page.
Draw	Creates statistics charts on-the-fly.

Starting the Application

1 Open a web browser.

2 Enter the device's IP address (as defined in the CLI) in the address bar and press <Enter>.

For information about assigning an IP address to a device, see "Static IP Address and Subnet Mask."

3 When the **Enter Network Password** window opens, enter a user name and password.

NOTE: The device is not configured with a default password, and can be configured without entering a password. For information about recovering a lost password, see “Password Recovery."

NOTE: Passwords are both case sensitive and alpha-numeric.

4 Click **OK**.

The **Dell PowerConnect OpenManage™ Switch Administrator** home page opens.

Accessing the Device Through the CLI

The device can be managed over a direct connection to the console port or via a Telnet connection. Using the CLI is similar to entering commands on a Linux system. If access is via a Telnet connection, ensure the device has an IP address defined and that the workstation used to access the device is connected to the device prior to beginning using CLI commands.

For information about configuring an initial IP Address, see "Static IP Address and Subnet Mask."

NOTE: Ensure the client is loaded, before using the CLI.

Console Connection

1. Power on the device and wait until the startup is complete.
2. When the `Console>` prompt displays, type `enable` and press <Enter>.
3. Configure the device and enter the necessary commands to complete the required tasks.
4. When finished, exit the session with the `quit` or `exit` command.

NOTE: If a different user logs into the system in the Privilege EXEC command mode, the current user is logged off and the new user is logged in.

Telnet Connection

Telnet is a terminal emulation TCP/IP protocol. ASCII terminals can be virtually connected to the local device through a TCP/IP protocol network. Telnet is an alternative to a local login terminal where a remote login is required.

The device supports up to four simultaneous Telnet sessions. All CLI commands can be used over a telnet session.

To start a Telnet session:

1. Select **Start** > **Run**.

   The **Run** window opens.

2. In the **Run** window, type `Telnet` *`<IP address>`* in the **Open** field.
3. Click **OK** to begin the Telnet session.

Using the CLI

This section provides information for using the CLI.

Command Mode Overview

The CLI is divided into command modes. Each command mode has a specific command set. Entering a question mark at the console prompt displays a list of commands available for that particular command mode.

In each mode, a specific command is used to navigate from one command mode to another.

During the CLI session initialization, the CLI mode is the User EXEC mode. Only a limited subset of commands are available in the User EXEC mode. This level is reserved for tasks that do not change the console configuration and is used to access configuration sub-systems such as the CLI. To enter the next level, the Privileged EXEC mode, a password is required (if configured).

The Privileged EXEC mode provides access to the device global configuration. For specific global configurations within the device, enter the next level, Global Configuration mode. A password is not required.

The Global Configuration mode manages the device configuration on a global level.

The Interface Configuration mode configures the device at the physical interface level. Interface commands which require subcommands have another level called the Subinterface Configuration mode. A password is not required.

User EXEC Mode

After logging into the device, the EXEC command mode is enabled. The user-level prompt consists of the host name followed by the angle bracket (>). For example:

```
console>
```

NOTE: The default host name is `console` unless it has been modified during initial configuration.

The user EXEC commands permit connecting to remote devices, changing terminal settings on a temporary basis, performing basic tests, and listing system information.

To list the user EXEC commands, enter a question mark at the command prompt.

Privileged EXEC Mode

Privileged access can be protected to prevent unauthorized access and ensure operating parameters. Passwords are displayed in the ***** format on the screen, and are case sensitive.

To access and list the Privileged EXEC Mode commands:

1. At the prompt type `enable` and press <Enter>.
2. When a password prompt displays, enter the password and press <Enter>.

   The Privileged EXEC mode prompt displays as the device host name followed by #. For example:

```
console#
```

To list the Privileged EXEC commands, type a question mark at the command prompt and press <Enter>.

To return from Privileged EXEC Mode to User EXEC Mode use any of the following commands: `disable`, `exit/end`, or <Ctrl><Z>.

The following example illustrates accessing privileged EXEC mode and then returning to the User EXEC mode:

```
console>enable

Enter Password: ******

console#

console#disable

console>
```

Use the **exit** command to move back to a previous mode. For example, from Interface Configuration mode to Global Configuration mode, and from Global Configuration mode to Privileged EXEC mode.

Global Configuration Mode

Global Configuration commands apply to system features, rather than a specific protocol or interface.

To access Global Configuration mode, at the Privileged EXEC Mode prompt, type `configure` and press <Enter>. The Global Configuration Mode displays as the device host name followed by (config) and the pound sign #.

```
console(config)#
```

To list the Global Configuration commands, enter a question mark at the command prompt.

To return from Global Configuration mode to Privileged EXEC mode, type the `exit` command or use the <Ctrl><Z> command.

The following example illustrates how to access Global Configuration Mode and return back to the Privileged EXEC Mode:

```
console#

console#configure

console(config)#exit

console#
```

Interface Configuration Mode

Interface configuration commands modify specific IP interface settings, including bridge-group, description, etc.

VLAN Database Mode

The VLAN mode contains commands to create and configure a VLAN as a whole, for example, to create a VLAN and apply an IP address to the VLAN. The following is an example of the VLAN mode prompt:

```
Console # vlan database

Console (config-vlan)#
```

Port Channel Mode

The Port Channel mode contains commands for configuring Link Aggregation Groups (LAG). The following is an example of the Port Channel mode prompt:

```
Console (config)# interface port-channel 1

Console (config-if)#
```

Interface Mode

The Interface mode contains commands that configure the interface. The Global Configuration mode command `interface ethernet` is used to enter the interface configuration mode. The following is an example of the Interface mode prompt:

```
console> enable

console# configure

console(config)# interface ethernet g18

console(config-if)#
```

Management Access List

The Management Access List mode contains commands to define management access-lists. The Global Configuration mode command `management access-list` is used to enter the Management Access List Configuration mode.

The following example shows how to create an access-list called "mlist", configure two management interfaces ethernet g1 and ethernet g9, and make the access-list the active list:

```
Console (config)# management access-list mlist

Console (config-macl)# permit ethernet g1

Console (config-macl)# permit ethernet g9
Console (config-macl)# exit
Console (config)# management access-class mlist
```

SSH Public Key

The SSH Public Key mode contains commands to manually specify other device SSH public keys.

The Global Configuration mode command `crypto key pubkey-chain ssh` is used to enter the SSH Public Key-chain Configuration mode.

The following example enters the SSH Public Key-chain configuration mode:

```
Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)#
```

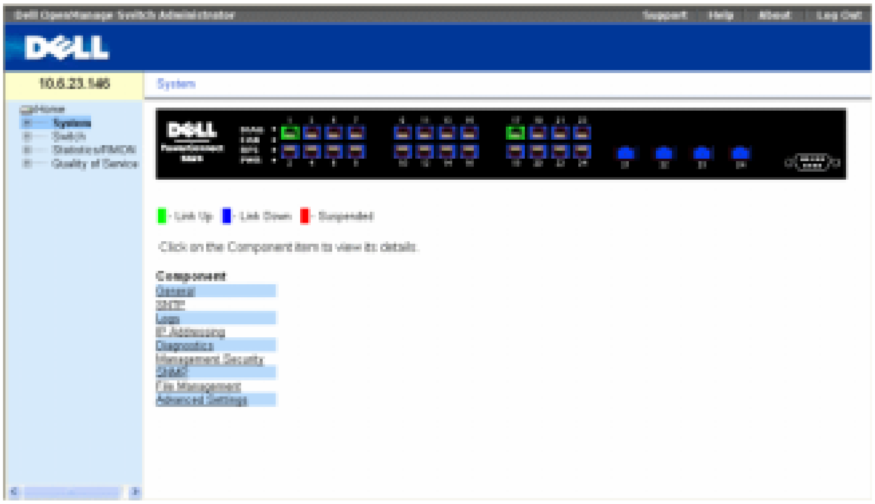
CLI Examples

CLI commands are provided as configuration examples. For a full description of the CLI commands, including examples, refer to the "CLI Reference Guide" included on the Documentation CD.

Configuring System Information

This section provides information for defining system parameters including security features, downloading device software, and resetting the device. To open the **System** page, click **System** in the tree view.

Figure 6-15. System



🟩 - Link Up 🟦 - Link Down 🟥 - Suspended

Click on the Component item to view its details.

Component

General
SNTP
Logs
IP Addressing
Diagnostics
Management Security
SNMP
File Management
Advanced Settings

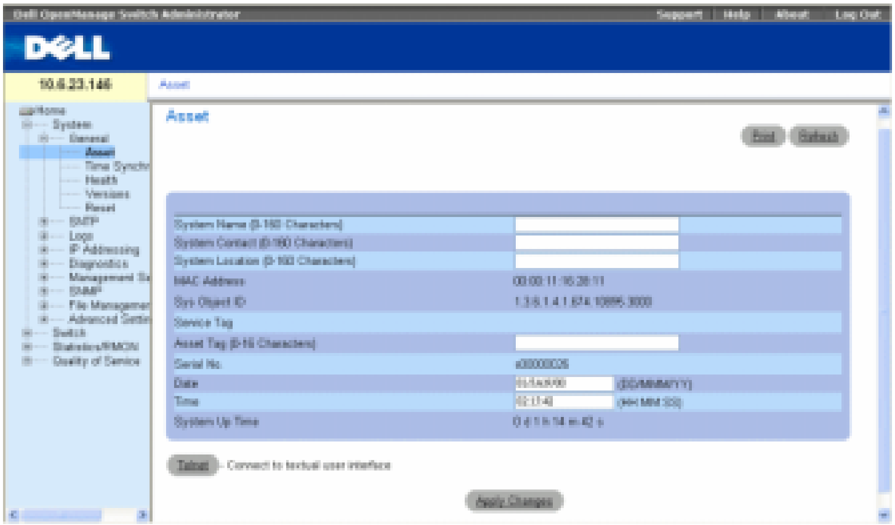
Defining General Device Information

The **General** page contains links to pages for configuring device parameters.

Viewing the Asset Page

The **Asset** page contains parameters for configuring general device information, including the system name, location, and contact, the system MAC Address, System Object ID, date, time, and System Up Time. To open the **Asset** page, click **System →General →Asset** in the tree view.

Figure 6-16. Asset



System Name (0-160 Characters)
System Contact (0-160 Characters)
System Location (0-160 Characters)
MAC Address 00:00:11:16:28:11
Sys Object ID 1.3.6.1.4.1.674.10895.3000
Service Tag
Asset Tag (0-16 Characters)
Serial No. a00000026
Date 01/14/00 (DD/MM/YY)
Time 02:17:40 (HH:MM:SS)
System Up Time 0 d 1 h 14 m 42 s

Telnet - Connect to textual user interface

System Name (0-160 Characters) — Defines the user-defined device name.

System Contact (0-160 Characters) — Specifies the name of the contact person.

System Location (0-160 Characters) — Specifies the location where the system is currently running.

MAC Address — Specifies the device MAC address.

Sys Object ID — Specifies the vendor's authoritative identification of the network management subsystem contained in the entity.

Service Tag — Specifies the service reference number used when servicing the device.

Asset Tag (0-16 Characters) — Specifies the user-defined device reference.

Serial No. — Specifies the device serial number.

Date (/YY) — Specifies the current date. The format is month, day, year, for example, 11/10/02 is November 10, 2002.

Time (HH:MM:SS) — Specifies the time. The format is hour, minute, second, for example, 20:12:03 is eight twelve and three seconds in the evening.

System Up Time — Specifies the amount of time since the last device reset. The system time is displayed in the following format: Days, Hours, Minutes and Seconds. For example, 41 days, 2 hours, 22 minutes and 15 seconds.

Defining System Information:

1. Open the **Asset** page.
2. Define the relevant fields.
3. Click **Apply Changes**.

   The system parameters are defined, and the device is updated.

Initiating a Telnet Session:

1. Open the **Asset** page.
2. Click **Telnet**.

   A Telnet session is initiated.

Configuring Device Information Using the CLI Commands

The following table summarizes the equivalent CLI commands for viewing and setting fields displayed in the **Asset** page.

Table 6-11. Asset CLI Commands

CLI Command	Description
hostname *name*	Specifies or modifies the device host name.
snmp-server contact *text*	Sets up a system contact.
snmp-server location *text*	Enters information on where the device is located.
clock set *hh***:***mm***:***ss day month year*	Manually sets the system clock and date.
show clock [**detail**]	Displays the time and date from the system clock.
show system id	Displays the service tag information.
show system	Displays system information.
asset-tag	Sets the device asset tag.

The following is an example of the CLI commands:

```
Console (config)# hostname dell

Console (config)# snmp-server contact Dell_Tech_Supp

Console (config)# snmp-server location New_York

Console (config)# exit

Console # exit

Console (config)# asset-tag 1qwepot

Console> clock set 13:32:00 7 Dec 2004

Console> show clock

13:32:00 (UTC+0) Dec 7 2004

No time source
```

```
DELL Switch# show system
System Description:                     Ethernet Routing Switch
System Up Time (days,hour:min:sec):     0,00:04:17
System Contact:                         spk
System Name:                            DELL Switch
System Location:                        R&D
System MAC Address:                     00:10:b5:f4:00:01
Sys Object ID:                          1.3.6.1.4.1.674.10895.3000
Type: PowerConnect 5324

Power Supply         Status
-------------        --------
Main                 OK
Redundant            OK

FAN                  Status
-------------        --------
1                    OK
2                    OK

DELL Switch#
```

Defining System Time Settings

The **Time Synchronization** page contains fields for defining system time parameters for both the local hardware clock, and the external SNTP clock. If the system time is kept using an external SNTP clock, and the external SNTP clock fails, the system time reverts to the local hardware clock. Daylight Savings Time can be enabled on the device. The following is a list of Daylight Time start and end times in specific countries:

- **Albania** — Last weekend of March until the last weekend of October.
- **Australia** — From the end of October until the end of March.
- **Australia - Tasmania** — From beginning of October the end of March.
- **Armenia** — Last weekend of March until the last weekend of October.
- **Austria** — Last weekend of March until the last weekend of October.
- **Bahamas** — From April to October, in conjunction with U.S. summer hours.

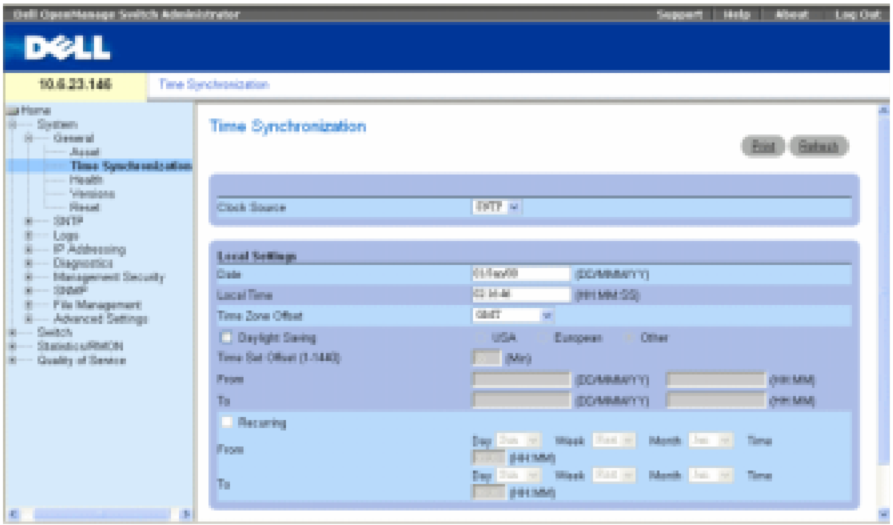
- **Belarus** — Last weekend of March until the last weekend of October.
- **Belgium** — Last weekend of March until the last weekend of October.
- **Brazil** — From the 3rd Sunday in October until the 3rd Saturday in March. During the period of Daylight Saving Time, Brazilian clocks go forward one hour in most of the Brazilian southeast.
- **Chile** — Easter Island 9th March 12th October. The first Sunday in March or after 9th March.
- **China** — China does not operate Daylight Saving Time.
- **Canada** — From the first Sunday in April until the last Sunday of October. Daylight Saving Time is usually regulated by provincial and territorial governments. Exceptions may exist in certain municipalities.
- **Cuba** — From the last Sunday of March to the last Sunday of October.
- **Cyprus** — Last weekend of March until the last weekend of October.
- **Denmark** — Last weekend of March until the last weekend of October.
- **Egypt** — Last Friday in April until the last Thursday in September.
- **Estonia** — Last weekend of March until the last weekend of October.
- **Finland** — Last weekend of March until the last weekend of October.
- **France** — Last weekend of March until the last weekend of October.
- **Germany** — Last weekend of March until the last weekend of October.
- **Greece** — Last weekend of March until the last weekend of October.
- **Hungary** — Last weekend of March until the last weekend of October.
- **India** — India does not operate Daylight Saving Time.
- **Iran** — From 1st Farvardin the 1st Mehr.
- **Iraq** — From 1st April until 1st October.
- **Ireland** — Last weekend of March until the last weekend of October.
- **Israel** — Varies year-to-year.
- **Italy** — Last weekend of March until the last weekend of October.
- **Japan** — Japan does not operate Daylight Saving Time.
- **Jordan** — Last weekend of March until the last weekend of October.
- **Latvia** — Last weekend of March until the last weekend of October.
- **Lebanon** — Last weekend of March the last weekend of October.
- **Lithuania** — Last weekend of March until the last weekend of October.
- **Luxembourg** — Last weekend of March until the last weekend of October.
- **Macedonia** — Last weekend of March until the last weekend of October.
- **Mexico** — From the first Sunday in April at 02:00 to the last Sunday in October at 02:00.
- **Moldova** — Last weekend of March until the last weekend of October.
- **Montenegro** — Last weekend of March until the last weekend of October.
- **Netherlands** — Last weekend of March until the last weekend of October.
- **New Zealand** — From the first Sunday in October until the first Sunday on or after 15th March.

- **Norway** — Last weekend of March until the last weekend of October.
- **Paraguay** — From 6th April until 7th September.
- **Poland** — Last weekend of March until the last weekend of October.
- **Portugal** — Last weekend of March until the last weekend of October.
- **Romania** — Last weekend of March until the last weekend of October.
- **Russia** — From the 29th March until the 25th October.
- **Serbia** — Last weekend of March until the last weekend of October.
- **Slovak Republic** — Last weekend of March until the last weekend of October.
- **South Africa** — South Africa does not operate Daylight Saving Time.
- **Spain** — Last weekend of March until the last weekend of October.
- **Sweden** — Last weekend of March until the last weekend of October.
- **Switzerland** — Last weekend of March until the last weekend of October.
- **Syria** — From 31st March until 30th October.
- **Taiwan** — Taiwan does not operate Daylight Saving Time.
- **Turkey** — Last weekend of March until the last weekend of October.
- **United Kingdom** — Last weekend of March until the last weekend of October.
- **United States of America** — From the first Sunday in April at 02:00 to the last Sunday in October at 02:00.

For more information on SNTP, see "Configuring SNTP Settings" .

To open the **Time Synchronization** page, click **System →General →Time Synchronization** in the tree view.

Figure 6-17. Time Synchronization



Clock Source: SNTP

Local Settings

Date (DD/MMM/YY)

Local Time (HH:MM:SS)

Time Zone Offset: GMT

□ Daylight Saving ○ USA ○ European ○ Other

Time Set Offset (1-1440) (Min)

From (DD/MMM/YY) (HH:MM)

To (DD/MMM/YY) (HH:MM)

□ Recurring

From Day Week Month Time (HH:MM)

To Day Week Month Time (HH:MM)

Clock Source

Clock Source — The source used to set the system clock. The possible field values:

SNTP — Specifies that the system time is set via an SNTP server. For more information, see "Configuring SNTP Settings" .

None — Specifies that the system time is not set by an external source.

Local Settings

Date — Defines the system date. The field format is Day:Month:Year, for example, 04 May 2050.

Local Time — Defines the system time. The field format is HH:MM:SS, for example, 21:15:03.

Time Zone Offset — The difference between Greenwich Mean Time (GMT) and local time. For example, the Time Zone Offset for Paris is GMT +1, while the local time in New York is GMT –5.

There are two types of daylight settings, either by a specific date in a particular year or a recurring setting irrespective of the year. For a specific setting in a particular year complete the **Daylight Savings** area, and for a recurring setting, complete the **Recurring** area.

Daylight Savings — Enables the Daylight Savings Time (DST) on the device based on the devices location. The possible field values are:

USA — The device switches to DST at 2 a.m. on the first Sunday of April, and reverts to standard time at 2 a.m. on the last Sunday of October.

European — The device switches to DST at 1:00 am on the last Sunday in March and reverts to standard time at 1:00 am on the last Sunday in October. The *European* option applies to EU members, and other European countries using the EU standard.

Other — The DST definitions are user-defined based on the device locality. If Other is selected, the **From** and **To** fields must be defined.

From — Defines the time that DST begins in countries other than USA or Europe, in the format DayMonthYear in one field and time in another. For example, DST begins on the 25th October 2007 5:00 am, the two fields will be 25Oct07 and 5:00. The possible field values are:

Date — The date at which DST begins. The possible field range is 1-31.

Month — The month of the year in which DST begins. The possible field range is Jan-Dec.

Year— The year in which the configured DST begins.

Time — The time at which DST begins. The field format is Hour:Minute, for example, 05:30.

To — Defines the time that DST ends in countries other than USA or Europe in the format DayMonthYear in one field and time in another. For example, DST ends on the 23rd March 2008 12:00 am, the two fields will be 23Mar08 and 12:00. The possible field values are:

Date — The date at which DST ends. The possible field range is 1-31.

Month — The month of the year in which DST ends. The possible field range is Jan-Dec.

Year— The year in which the configured DST ends.

Time — The time at which DST starts. The field format is Hour:Minute, for example, 05:30.

Recurring — Defines the time that DST starts in countries other than USA or European where the DST is constant year to year. The possible field values are:

From — Defines the time that DST begins each year. For example, DST begins locally every second Sunday in April at 5:00 am. The possible field values are:

Day — The day of the week from which DST begins every year. The possible field range is Sunday-Saturday.

Week — The week within the month from which DST begins every year. The possible field range is 1-5.

Month — The month of the year in which DST begins every year. The possible field range is Jan.-Dec.

Time — The time at which DST begins every year. The field format is Hour:Minute, for example, 02:10.

To — Defines the recurring time that DST ends each year. For example, DST ends locally every fourth Friday in October at 5:00 am. The possible field values are:

Day — The day of the week at which DST ends every year. The possible field range is Sunday-Saturday.

Week — The week within the month at which DST ends every year. The possible field range is 1-5.

Month — The month of the year in which DST ends every year. The possible field range is Jan.-Dec.

Time — The time at which DST ends every year. The field format is Hour:Minute, for example, 05:30.

Selecting a Clock Source

1. Open the **Time Synchronization** page.
2. Define the **Clock Source** field.
3. Click **Apply Changes**.

   The Clock source is selected, and the device is updated.

Defining Local Clock Settings

1. Open the **Time Synchronization** page.
2. Define the **Recurring** fields.
3. Click **Apply Changes**.

   The local clock settings are applied.

Defining the External SNTP Clock Settings

1. Open the **Time Synchronization** page.
2. Define the fields.
3. Click **Apply Changes**.

   The external clock settings are applied.

Defining Clock Settings Using CLI Commands

The following table summarizes the equivalent CLI commands for setting fields displayed in the **Time Synchronization** page.

Table 6-12. Clock Setting CLI Commands

CLI	Description
clock source {**sntp**}	Configures an external time source for the system clock.
clock timezone *hours-offset* [**minutes** *minutes-offset*] [**zone** *acronym*]	Sets the time zone for display purposes.
clock summer-time	Configures the system to automatically switch to summer time (Daylight Savings Time).
clock summer-time recurring {**usa** | **eu** | {*week day month hh:mm week day month hh:mm*}} [**offset** *offset*] [**zone** *acronym*]	Configures the system to automatically switch to summer time (according to the USA and European standards.)
clock summer-time date *date month year hh:mm date month year hh:mm* [**offset** *offset*] [**zone** *acronym*]	Configures the system to automatically switch to summer time (Daylight Savings Time) for a specific period - date/month/year format.

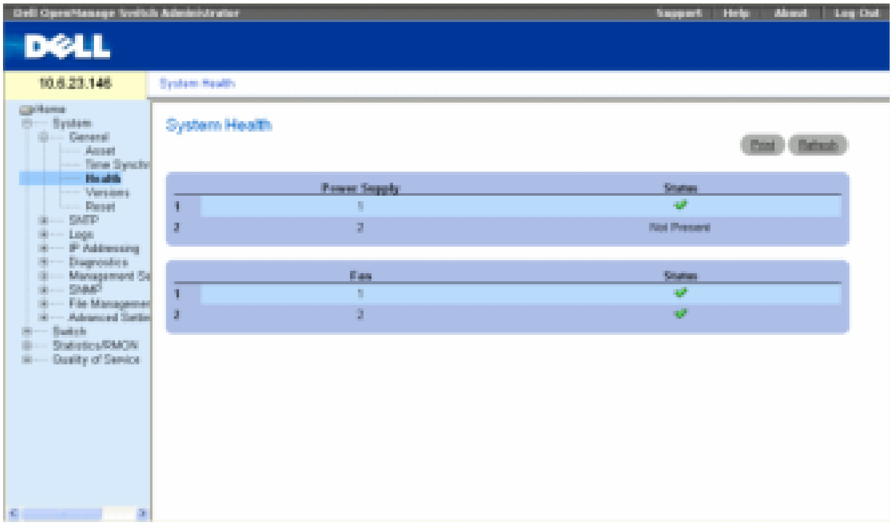
The following is an example of the CLI commands:

```
Console(config)# clock timezone -6 zone CST

Console(config)# clock summer-time recurring first sun apr 2:00
last sun oct 2:00
```

Viewing System Health Information

The **System Health** page shows physical device hardware information. To open the **System Health** page, click **System→General→Health** in the tree view.

Figure 6-18. System Health



System Health

	Power Supply	Status
1	1	✓
2	2	Not Present

	Fan	Status
1	1	✓
2	2	✓

Power Supply Status — The main power supply state. The possible field values are:

✓ — The main power supply is operating normally for the specified unit.

✗ — The main power supply is not operating normally for the specified unit.

Not Present — The power supply is not present for the specified unit.

Fan — The device fan status. The possible field values are:

✓ — The fans are operating normally for the specified unit.

✗ — The fans are not operating normally for the specified unit.

Not Present — The fans are not present for the specified unit.

Viewing System Health Information Using the CLI Commands

The following table summarizes the equivalent CLI command for viewing fields displayed in the **System Health** page.

Table 6-13. System Health CLI Commands

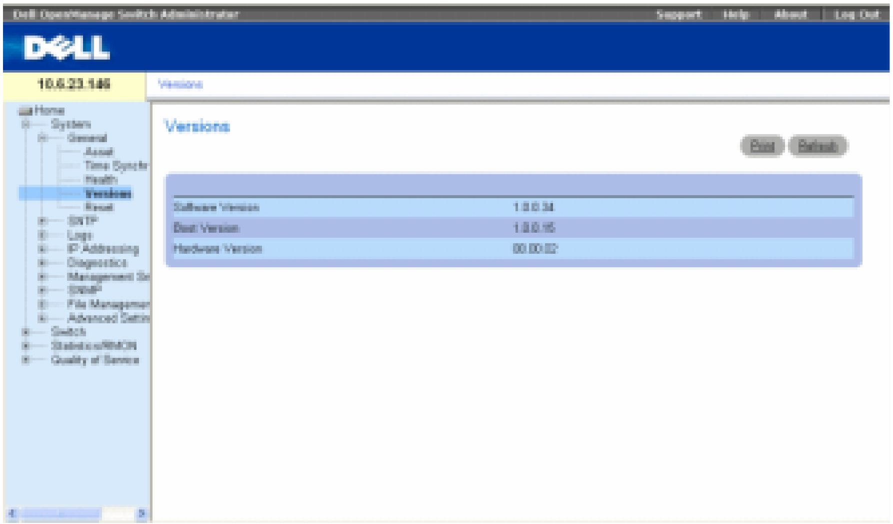
CLI Command	Description
show system	Displays system information.

```
DELL Switch# show system
System Description:                    Ethernet Routing Switch
System Up Time (days,hour:min:sec):    0,00:04:17
System Contact:                        spk
System Name:                           DELL Switch
System Location:                       R&D
System MAC Address:                    00:10:b5:f4:00:01
Sys Object ID:                         1.3.6.1.4.1.674.10895.3000
Type: PowerConnect 5324

Power Supply        Status
-------------       --------
Main                OK
Redundant           OK

FAN                 Status
-------------       --------
1                   OK
2                   OK

DELL Switch#
```

Viewing the Versions Page

The **Versions** page contains information about the hardware and software versions currently running. To open the **Versions** page, click **System→General→Versions** in the tree view.

Figure 6-19. Versions



Versions

Software Version	1.0.0.34
Boot Version	1.0.0.16
Hardware Version	00.00.02

Software Version — The current software version running on the device.

Boot Version — The current Boot version running on the device.

Hardware Version — The current hardware versions running on the device.

Displaying Device Versions Using the CLI

The following table summarizes the equivalent CLI commands for viewing fields displayed in the **Versions** page.

Table 6-14. Versions CLI Commands

CLI Command	Description
show version	Displays system version information.

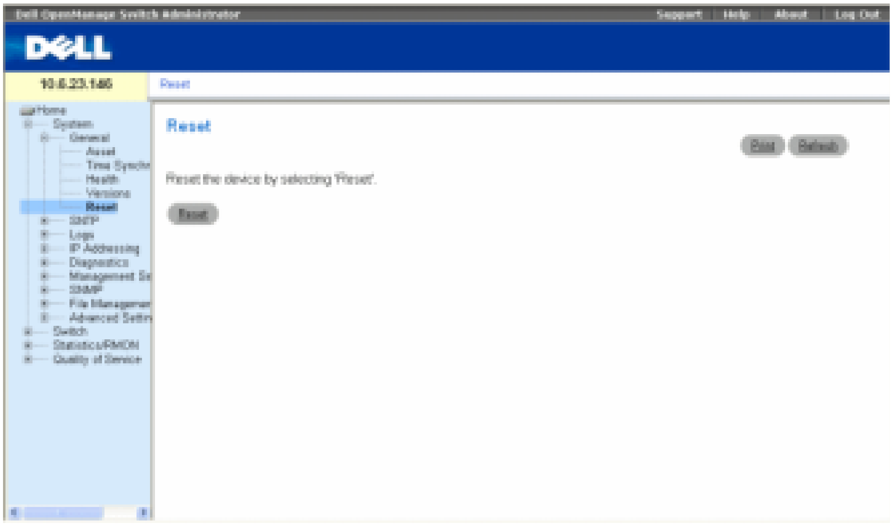
The following is an example of the CLI commands:

```
Console> show version
SW version x.xxx  (date 23-Jul-xxxx time 17:34:19)
Boot version x.xxx  (date 17-Jan-xxxx time 11:48:21)
HW version  x.x.x
```

Resetting the Device

The **Reset** page enables the device to be reset from a remote location. To open the **Reset** page, click **System→General→Reset** in the tree view.

Figure 6-20. Reset



Reset the device by selecting 'Reset'.

NOTE: Save all changes to the Running Configuration file before resetting the device. This prevents the current device configuration from being lost. For more information about saving Configuration files, see "Managing Files" .

Resetting the Device

1. Open the **Reset** page
2. Click **reset**.

   A confirmation message displays.
3. Click **OK**.

   The device is reset. After the device is reset, a prompt for a user name and password displays.
4. Enter a user name and password to reconnect to the Web Interface.

Resetting the Device Using the CLI

The following table summarizes the equivalent CLI commands for performing a reset of the device via the CLI:.

Table 6-15. Reset CLI Command

CLI Command	Description
reload	Reloads the operating system.

The following is an example of the CLI command:

```
Console >reload

This command will reset the whole system and disconnect your
current

session. Do you want to continue (y/n) [n] ?
```

Configuring SNTP Settings

The device supports the Simple Network Time Protocol (SNTP). SNTP assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. The device operates only as an SNTP client, and cannot provide time services to other systems.

The device can poll the following server types for the server time:

- Unicast
- Anycast
- Broadcast

Time sources are established by Stratums. Stratums define the accuracy of the reference clock. The higher the stratum (where zero is the highest), the more accurate the clock. The receives time from stratum 1 and above.

The following is an example of stratums:

- **Stratum 0** — A real time clock is used as the time source, for example, a GPS system.
- **Stratum 1** — A server that is directly linked to a Stratum 0 time source is used. Stratum 1 time servers provide primary network time standards.
- **Stratum 2** — The time source is distanced from the Stratum 1 server over a network path. For example, a Stratum 2 server receives the time over a network link, via NTP, from a Stratum 1 server.

Information received from SNTP servers is evaluated based on the Time level and server type.

SNTP time definitions are assessed and determined by the following time levels:

- **T1** — The time at which the original request was sent by the client.
- **T2** — The time at which the original request was received by the server.
- **T3** — The time at which the server sent the client a reply.
- **T4** — The time at which the client received the server's reply.

Polling for Unicast Time Information

Polling for Unicast information is used for polling a server for which the IP address is known. T1 - T4 are used to determine the server time. This is the preferred method for synchronizing switch time.

Polling for Anycast Time Information

Polling for Anycast information is used when the server IP address is unknown. The first anycast server to return a response is used to set the time value. Time levels T3 and T4 are used to determine the server time. Using Anycast time information for synchronizing switch time is preferred to using Broadcast time information.

Broadcast Time Information

Broadcast information is used when the server IP address is unknown. When a broadcast message is sent from an SNTP server, the SNTP client listens for the response. The SNTP client neither sends time information requests nor receives responses from the Broadcast server.

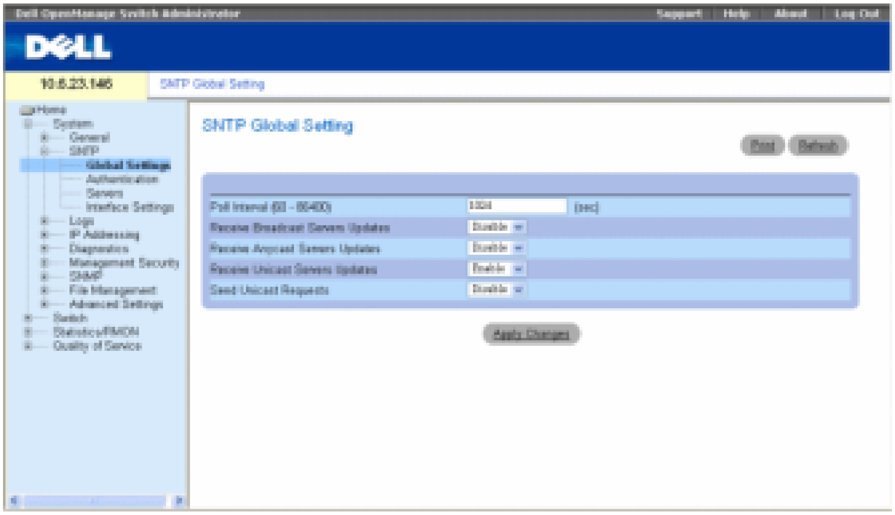
MD5 (Message Digest 5) Authentication safeguards switch synchronization paths to SNTP servers. MD5 is an algorithm that produces a 128-bit hash. MD5 is a variation of MD4, and increases MD4 security. MD5 verifies the integrity of the communication, authenticates the origin of the communication.

Click **System→SNTP** in the tree view to open the **SNTP** page.

Defining SNTP Global Parameters

The **SNTP Global Settings** page provides information for defining SNTP parameters globally. To open the **SNTP Global Settings** page, click **System →SNTP→SNTP Global Settings** in the tree view.

Figure 6-21. SNTP Global Settings



SNTP Global Setting

Poll Interval (60 - 86400) 1024 (sec)
Receive Broadcast Servers Updates Disable
Receive Anycast Servers Updates Disable
Receive Unicast Servers Updates Enable
Send Unicast Requests Disable

Poll Interval (60-86400) — Defines the interval (in seconds) at which the SNTP server is polled for Unicast information.

Receive Broadcast Servers Updates — Polls the SNTP servers for Broadcast server time information on the selected interfaces.

Receive Anycast Servers Updates — Polls the SNTP server for Anycast server time information, when enabled. If both the **Receive Anycast Servers Update**, and the **Receive Broadcast Servers Update** fields are enabled, the system time is set according the Anycast server time information.

Receive Unicast Servers Updates — Polls the SNTP server for Unicast server time information, when enabled. If the **Receive Broadcast Servers Updates**, **Receive Anycast Servers Updates**, and the **Receive Unicast Servers Updates** fields are all enabled, the system time is set according the Unicast server time information.

Poll Unicast Servers — Sends SNTP Unicast forwarding information to the SNTP server, when enabled.

Defining SNTP Global Parameters Using CLI Commands

The following table summarizes the equivalent CLI commands for setting fields displayed in the **SNTP Global Settings** page.

Table 6-16. SNTP Global Parameters CLI Commands

CLI Command	Description
sntp broadcast client enable	Enables SNTP broadcast clients
sntp anycast client enable	Enables SNTP anycast clients
sntp unicast client enable	Enables SNTP predefined unicast clients

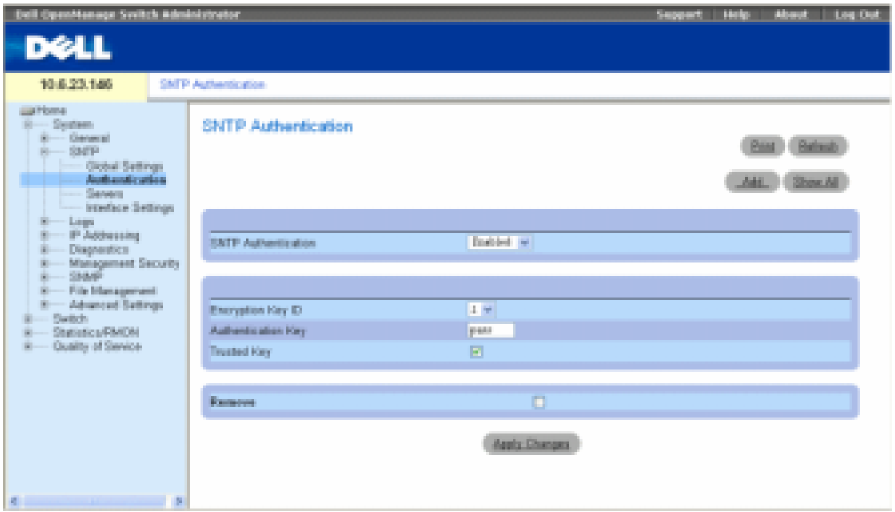
The following is an example of the CLI commands:

```
console> enable
console# configure
console(config)# sntp anycast client enable
```

Defining SNTP Authentication Methods

The **SNTP Authentication** page enables SNTP authentication between the and an SNTP server. The means by which the SNTP server is authenticated is also selected in the **SNTP Authentication** page. Click **System →SNTP→Authentication** in the tree view to open the **SNTP Authentication** page.

Figure 6-22. SNTP Authentication



SNTP Authentication

SNTP Authentication: Enabled

Encryption Key ID: 1

Authentication Key: pass

Trusted Key: ☑

Remove: ☐

SNTP Authentication — Enables authenticating an SNTP session between the device and an SNTP server, when enabled.

Encryption Key ID — Defines the Key Identification used to authenticate the SNTP server and device. The field value is upto 4294967295 characters.

Authentication Key (1-8 Characters) — Specifies the key used for authentication.

Trusted Key — Specifies the Encryption Key used to authenticate the SNTP server.

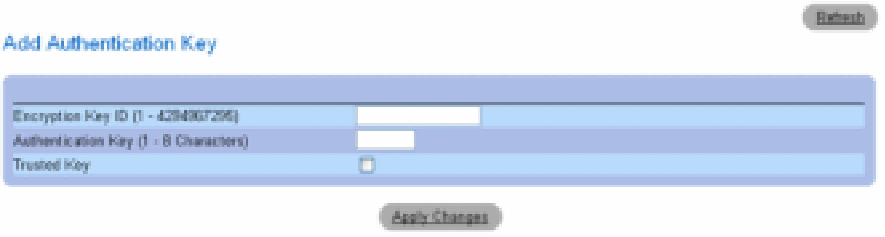
Remove — Removes when .

Adding an SNTP Authentication Key

1. Open the **SNTP Authentication** page.
2. Click **Add**.

   The **Add Authentication Key** page opens:

Figure 6-23. Add Authentication Key



Add Authentication Key

Encryption Key ID (1 - 4294967295)	
Authentication Key (1 - 8 Characters)	
Trusted Key	□

3. Define the fields.
4. Click **Apply Changes**.

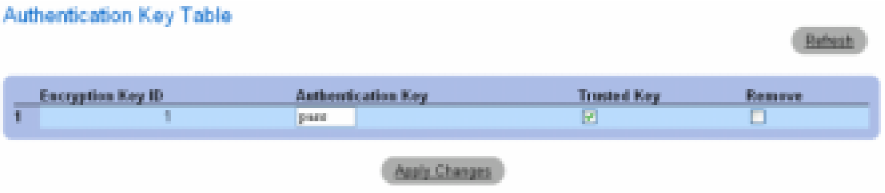
   The SNTP Authentication Key is added, and the device is updated.

Displaying the Authentication Key Table

1. Open the **SNTP Authentication** page.
2. Click **Show All**.

   The **Authentication Key Table** opens:

Figure 6-24. Authentication Key Table



Authentication Key Table

	Encryption Key ID	Authentication Key	Trusted Key	Remove
1	1	pass	☑	□

Deleting the Authentication Key

1. Open the **SNTP Authentication** page.
2. Click **Show All**.

   The **Authentication Key Table** opens.
3. Select an **Authentication Key Table** entry.
4. Select the **Remove** check box.

5 Click **Apply Changes**.

The entry is removed, and the device is updated.

Defining SNTP Authentication Settings Using CLI Commands

The following table summarizes the equivalent CLI commands for setting fields displayed in the **SNTP Authentication** page.

Table 6-17. SNTP Authentication CLI Commands

CLI Command	Description
sntp authenticate	Defines authentication for received Network Time Protocol traffic from servers.
sntp authentication-key *number* **md5** *value*	Defines an authentication key for SNTP.

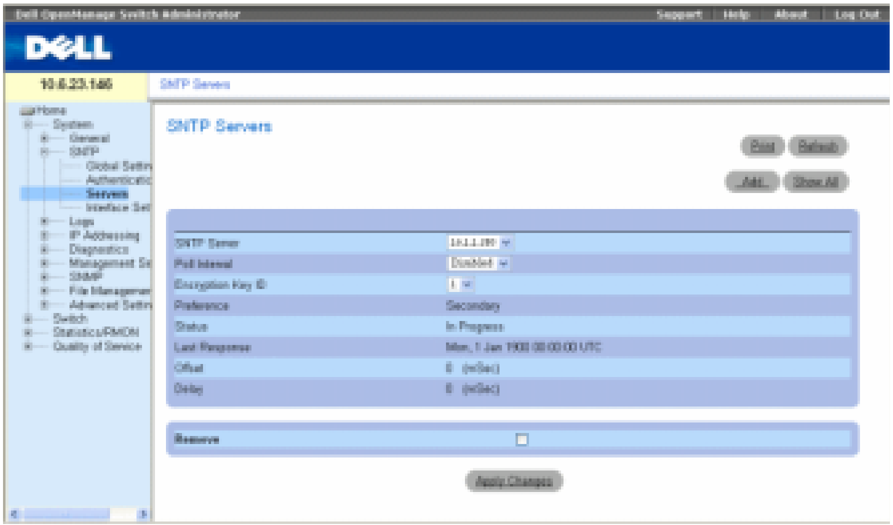
The following is an example of the CLI commands:

```
console> enable
console# configure
Console(config)# sntp authentication-key 8 md5 ClkKey
Console(config)# sntp trusted-key 8
Console(config)# sntp authenticate
```

Defining SNTP Servers

The **SNTP Servers** page contains information for enabling SNTP servers, as well as adding new SNTP servers. In addition, the **SNTP Servers** page enables the device to request and accept SNTP traffic from a server. To open the **SNTP Servers** page, click **System** →**SNTP** →**SNTP Servers** in the tree view.

Figure 6-25. SNTP Servers



SNTP Servers

SNTP Server	[illegible]
Poll Interval	Disabled
Encryption Key ID	1
Preference	Secondary
Status	In Progress
Last Response	Mon, 1 Jan 1900 00:00:00 UTC
Offset	0 (mSec)
Delay	0 (mSec)

Remove □

SNTP Server — Enter a user-defined SNTP server IP addresses or hostname. Up to eight SNTP servers can be defined. This field can contain 1 - 158 characters.

Poll Interval — Enables polling the selected SNTP Server for system time information, when enabled.

Encryption Key ID — Specifies the Key Identification used to communicate between the SNTP server and device. The range is 1 - 4294967295.

Preference — The SNTP server providing SNTP system time information. The possible field values are:

Primary — The primary server provides SNTP information.

Secondary — The backup server provides SNTP information.

Status Up — The operating SNTP server status The possible field values are:

Up — The SNTP server is currently operating normally.

Down — The SNTP server is currently not operating normally.

Unknown — The SNTP server status is currently unknown.

Last Response — The last time a response was received from the SNTP server.

Offset — Timestamp difference between the device local clock and the aquired time from the SNTP server.

Delay — The amount of time it takes to reach the SNTP server.

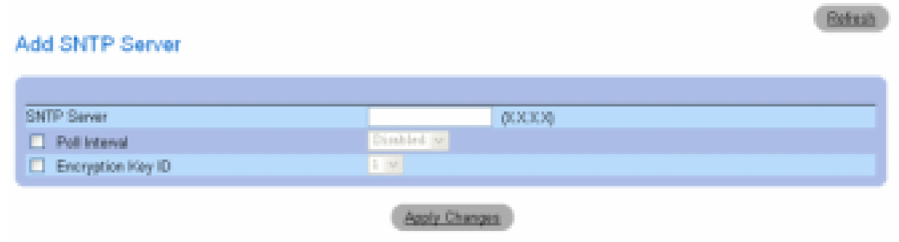
Remove — Removes a specific SNTP server from the **SNTP Server** list, when selected.

Adding an SNTP Server

1. Open the **SNTP Servers** page.
2. Click **Add.**

   The **Add SNTP Server** page opens:

Figure 6-26. Add SNTP Server



SNTP Server (X.X.X.X)

□ Poll Interval Disabled

□ Encryption Key ID 1

3. Define the fields.
4. Click **Apply Changes**.

   The SNTP Server is added, and the device is updated.

The following table summarizes the equivalent CLI commands for setting fields displayed in the **Add SNTP Server** page.

Table 6-18. SNTP Server CLI Commands

CLI Command	Description
sntp server *ip-address*|*hostname* [**poll**] [**key** *keyid*]	Configures the to use SNTP to request and accept NTP traffic from a server.

The following is an example of the CLI commands:

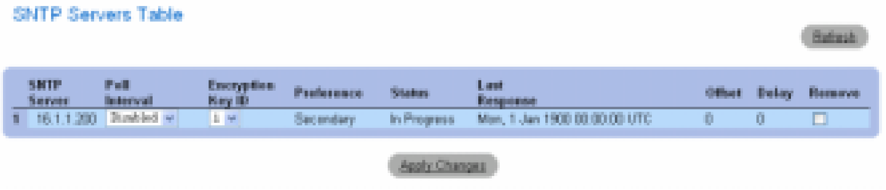
```
console> enable
console# configure
Console(config)# sntp server 100.1.1.1 poll key 10
```

Displaying the SNTP Server Table

1. Open the **SNTP Servers** page.
2. Click **Show All.**

   The **SNTP Servers Table** opens:

Figure 6-27. SNTP Servers Table



SNTP Servers Table

	SNTP Server	Poll Interval	Encryption Key ID	Preference	Status	Last Response	Offset	Delay	Remove
1	16.1.1.200	Disabled	1	Secondary	In Progress	Mon, 1 Jan 1900 00:00:00 UTC	0	0	□

Modifying an SNTP Server

1 Open the **SNTP Servers** page.

2 Click **Show All.**

The **SNTP Servers Table** opens.

3 Select an SNTP Server entry.

4 Modify the relevant fields.

5 Click **Apply Changes**.

The SNTP Server information is updated.

Deleting the SNTP Server

1 Open the **SNTP Servers** page.

2 Click **Show All.**

The **SNTP Servers Table** opens.

3 Select an **SNTP Server** entry.

4 Select the **Remove** check box.

5 Click **Apply Changes**.

The entry is removed, and the device is updated.

Defining SNTP Servers Settings Using CLI Commands

The following table summarizes the equivalent CLI commands for setting fields displayed in the **SNTP Servers** page.

Table 6-19. SNTP Server CLI Commands

CLI Command	Description
sntp server *ip-address*|*hostname* [**poll**] [*key keyid*]	Configures the device to use SNTP to request and accept NTP traffic from as server.

The following is an example of the CLI commands:

```
console> enable
console# configure
Console(config)# sntp server 100.1.1.1 poll key 10
Console# show sntp status
Clock is synchronized, stratum 4, reference is 176.1.1.8
Reference time is AFE2525E.70597B34 (00:10:22.438 PDT Jul 5 1993)

Unicast servers:
Server       Preference   Status    Last response     Offset Delay
                                                      [mSec] [mSec]
---------    ----------   --------  ---------------   ------ ------
176.1.1.8    Primary      Up        AFE252C1.6DBDDFF2 7.33   117.79
176.1.8.179  Secondary    Unknown   AFE21789.643287C9 8.98   189.19

Anycast server:
Server       Preference   Status    Last response     Offset Delay
                                                      [mSec] [mSec]
-------      ----------   -------   --------------    -----  ------
VLAN 119     Secondary    Up        19:53:21.789 PDT  7.19   119.89
                                    Feb 19 2002

Broadcast:
Interface    IP address   Last response
-----------  -----------  ------------------------
176.1.1.8    Primary      AFE252C1.6DBDDFF2
176.1.8.179  Secondary    AFE21789.643287C9
```

Defining SNTP Interfaces

The **SNTP Broadcast Interface Table** contains fields for setting SNTP on different interfaces. To open the **SNTP Broadcast Interface Table**, click **System→SNTP→Interfaces Settings**.

The **SNTP Broadcast Interface Table** contains the following fields:

Interface — Contains an interface list on which SNTP can be enabled.

Receive Server Updates —

Remove — Removes SNTP from a specific interface, when selected.

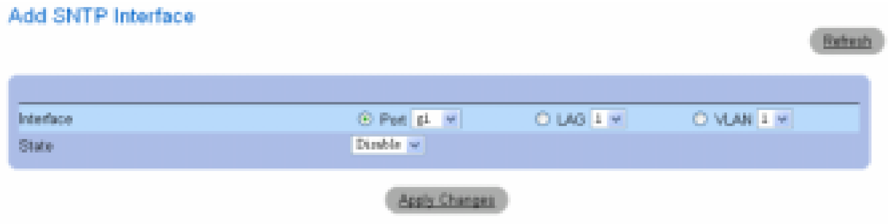
Adding an SNTP Interface

1 Open the **SNTP Broadcast Interface Table** page.

2 Click **Add.**

The **Add SNTP Interface** page opens:

Figure 6-28. Add SNTP Interface Page



Add SNTP Interface

Interface ● Port g1 ○ LAG 1 ○ VLAN 1

State Disable

3 Define the relevant fields.

4 Click **Apply Changes**.

The SNTP interface is added, and the device is updated.

Defining SNTP Interface Settings Using CLI Commands

The following table summarizes the equivalent CLI commands for setting fields displayed in the **SNTP Broadcast Interface Table**.

Table 6-20. SNTP Broadcast CLI Commands

CLI Command	Description
sntp client enable	Enables the Simple Network Time Protocol (SNTP) client on an interface.
show sntp configuration	Shows the configuration of the Simple Network Time Protocol (SNTP).

The following is an example of the CLI commands:

```
Console# show sntp configuration
Polling interval: 7200 seconds.

MD5 Authentication keys: 8, 9
Authentication is required for synchronization.
Trusted Keys: 8,9

Unicast Clients Polling: Enabled.

Server                           Polling            Encryption Key
-----------                      --------           -----------------
176.1.1.8                        Enabled            9
176.1.8.179                      Disabled           Disabled

Broadcast Clients: Enabled
Broadcast Clients Poll: Enabled
Broadcast Interfaces: g1, g3
```

Managing Logs

The **Logs** page contains links to various log pages. To open the **Logs** page, click **System →Logs** in the tree view.

The **Logs** page contains links to various log pages.

Defining Global Log Parameters

The System Logs enable viewing device events in real time, and recording the events for later usage. System Logs record and manage events and report errors or informational messages.

Event messages have a unique format, as per the SYSLOG RFC recommended message format for all error reporting. For example, Syslog and local device reporting messages are assigned a severity code, and include a message mnemonic, which identifies the source application generating the message. It allows messages to be filtered based on their urgency or relevancy. Each message severity determines the set of event logging devices that are sent per each event logging.

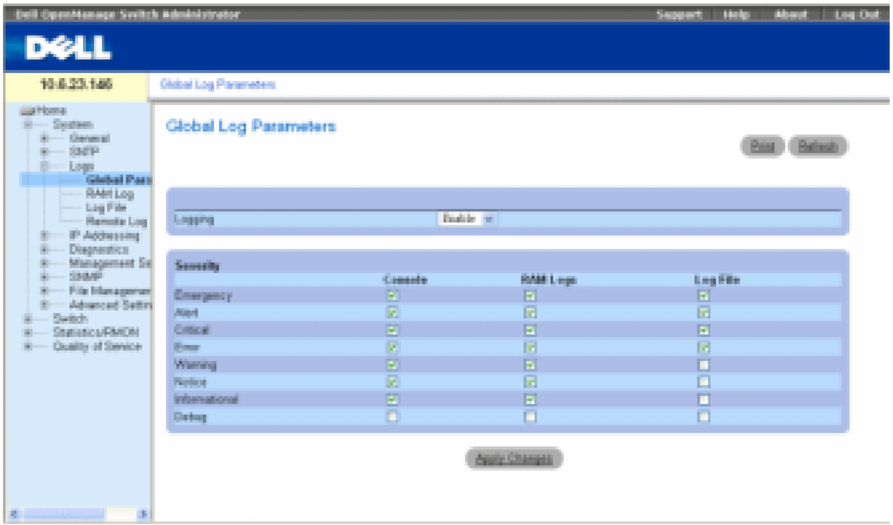
The following table contains the Log Severity Levels:

Table 6-21. Log Severity Levels

Severity Type	Severity Level	Description
Emergency	0	The system is not functioning.
Alert	1	The system needs immediate attention.
Critical	2	The system is in a critical state.
Error	3	A system error has occurred.
Warning	4	A system warning has occurred.
Notice	5	The system is functioning properly, but system notice has occurred.
Informational	6	Provides device information.
Debug	7	Provides detailed information about the log. If a Debug error occurs, contact Dell Online Technical Support

The **Global Log Parameters** page contains fields for defining which events are recorded to which logs. It contains fields for enabling logs globally, and parameters for defining log parameters. The Severity log messages are listed from the highest severity to the lowest. To open the **Global Log Parameters** page, click **System→Logs→Global Parameters** in the tree view.

Figure 6-29. Global Log Parameters



Global Log Parameters

Logging: Enable

Severity

	Console	RAM Logs	Log File
Emergency	☑	☑	☑
Alert	☑	☑	☑
Critical	☑	☑	☑
Error	☑	☑	☑
Warning	☑	☑	□
Notice	☑	☑	□
Informational	☑	☑	□
Debug	□	□	□

Logging — Enables device global logs for Cache, File, and Server Logs. Console logs are enabled by default.

Severity — The following are the available severity logs:

Emergency — The highest warning level. If the device is down or not functioning properly, an emergency log message is saved to the specified logging location.

Alert — The second highest warning level. An alert log is saved if there is a serious device malfunction, for example, all device features are down.

Critical — The third highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional.

Error — A device error has occurred, for example, if a single port is offline.

Warning — The lowest level of a device warning. The device is functioning, but an operational problem has occurred.

Notice — Provides device information.

Informational — Provides device information.

Debug — Provides debugging messages.

NOTE: When a severity level is selected, all severity level choices above the selection are selected automatically.

The **Global Log Parameters** page also contains check boxes which correspond to a distinct logging system:

Console — The minimum severity level from which logs are sent to the console.

RAM Logs — The minimum severity level from which logs are sent to the Log File kept in RAM (Cache).

Log File — The minimum severity level from which logs are sent to the Log File kept in FLASH memory.

Enabling Logs:

1. Open the **Global Log Parameters** page.
2. Select **Enable** in the **Logging** drop-down list.
3. Select the log type and log severity in the **Global Log Parameters** check boxes.
4. Click **Apply Changes.**

   The log settings are saved, and the device is updated.

Enabling Logs Using CLI Commands

The following table summarizes the equivalent CLI commands for setting fields displayed in the **Global Log Parameters** page.

Table 6-22. Global Log Parameters CLI Commands

CLI Command	Description
logging on	Enables error message logging.
logging *{ip-address | hostname}* [**port** *port*] [**severity** *level*] [**facility** *facility*] [**description** *text*]	Logs messages to a syslog server. For a list of the Severity levels, see "Log Severity Levels" .
logging console *level*	Limits messages logged to the console based on severity.
logging buffered *level*	Limits syslog messages displayed from an internal buffer (RAM) based on severity.
logging file *level*	Limits syslog messages sent to the logging file based on severity.
clear logging	Clears logs.
clear logging file	Clears messages from the logging file.

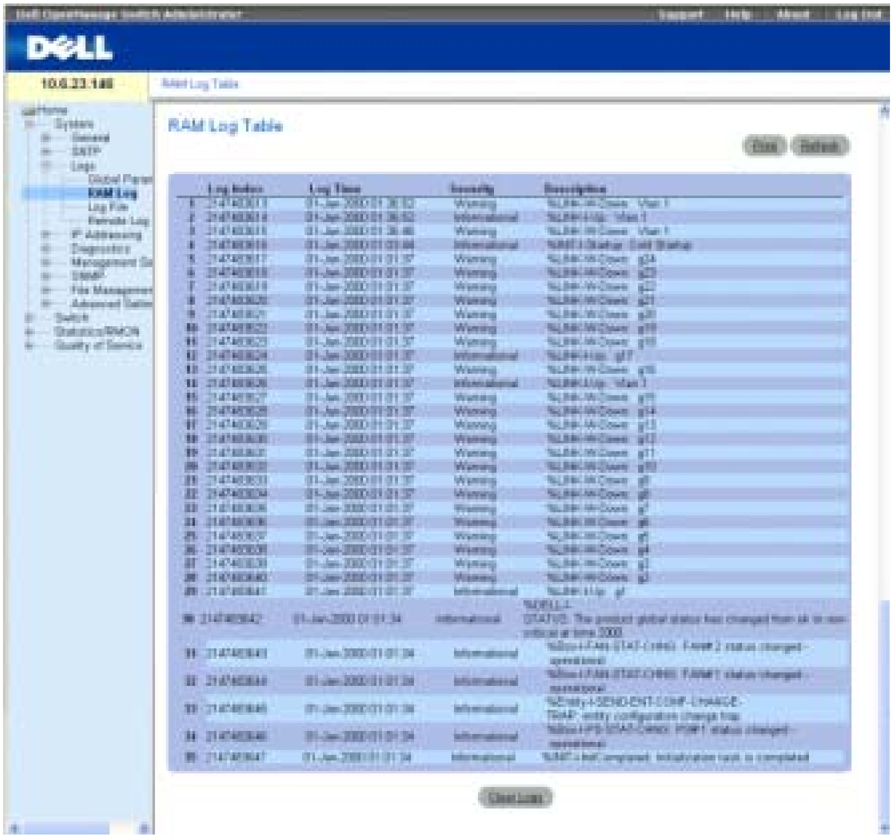
The following is an example of the CLI commands:

```
Console (config)# logging on
Console (config)# logging console errors
Console (config)# logging buffered debugging
Console (config)# logging file alerts
Console (config)# clear logging
Console (config)# exit
Console# clear logging file
Clear Logging File [y/n]y
```

Displaying RAM Log Table

The **RAM Log Table** contains information about log entries kept in RAM, including the time the log was entered, the log severity, and a description of the log. To open the **RAM Log Table**, click **System→Logs→RAM Log** in the tree view.

Figure 6-30. RAM Log Table



Log Index — The log number in the **RAM Log Table**.

Log Time — Specifies the time at which the log was entered into the **RAM Log Table**.

Severity — Specifies the log severity.

Description — The user-defined log description.

Removing Log Information:

1. Open the **RAM Log Table**.
2. Click **Clear Log**.

The log information is removed from the **RAM Log Table**, and the device is updated.

Viewing and Clearing the RAM Log Table Using the CLI Commands

The following table summarizes the equivalent CLI commands for viewing and clearing fields displayed in the **RAM Log Table**.

Table 6-23. RAM Log Table CLI Commands

CLI Command	Description
show logging	Displays the state of logging and the syslog messages stored in the internal buffer.
clear logging	Clears logs.

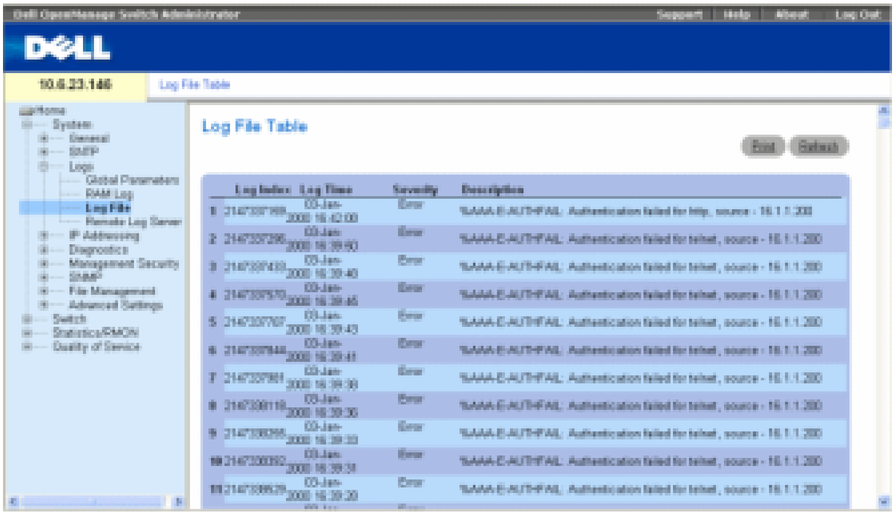
The following is an example of the CLI commands:

```
console# show logging
Logging is enabled.
Console Logging: Level info. Console Messages: 0 Dropped.
Buffer Logging: Level info. Buffer Messages: 26 Logged, 26
Displayed, 200 Max.
File Logging: Level error. File Messages: 157 Logged, 26
Dropped.
1 messages were not logged
01-Jan-2000 01:03:42 :%INIT-I-Startup: Cold Startup
01-Jan-2000 01:01:36 :%LINK-W-Down:  g24
01-Jan-2000 01:01:36 :%LINK-W-Down:  g23
01-Jan-2000 01:01:36 :%LINK-W-Down:  g22
01-Jan-2000 01:01:36 :%LINK-W-Down:  g21
01-Jan-2000 01:01:36 :%LINK-W-Down:  g20
01-Jan-2000 01:01:36 :%LINK-W-Down:  g19
01-Jan-2000 01:01:36 :%LINK-W-Down:  g18
01-Jan-2000 01:01:36 :%LINK-W-Down:  g17
01-Jan-2000 01:01:36 :%LINK-W-Down:  g13
1-Jan-2000 01:01:36 :%LINK-W-Down:  g2
01-Jan-2000 01:01:36 :%LINK-W-Down:  g1


01-Jan-2000 01:01:32 :%INIT-I-InitCompleted:
Initialization task is completed


Console # clear logging
clear logging buffer [y/n]?
Console #
```

Displaying the Log File Table

The **Log File Table** contains information about log entries saved to the Log File in FLASH, including the time the log was entered, the log severity, and a description of the log message. To open the **Log File Table**, click **System→Logs→Log File** in the tree view.

Figure 6-31. Log File Table



	Log Index	Log Time	Severity	Description
1	[illegible]	03-Jan-2000 16:42:00	Error	%AAA-E-AUTHFAIL: Authentication failed for http, source - 16.1.1.200
2	[illegible]	03-Jan-2000 16:39:50	Error	%AAA-E-AUTHFAIL: Authentication failed for telnet, source - 16.1.1.200
3	[illegible]	03-Jan-2000 16:39:40	Error	%AAA-E-AUTHFAIL: Authentication failed for telnet, source - 16.1.1.200
4	[illegible]	03-Jan-2000 16:39:45	Error	%AAA-E-AUTHFAIL: Authentication failed for telnet, source - 16.1.1.200
5	[illegible]	03-Jan-2000 16:39:43	Error	%AAA-E-AUTHFAIL: Authentication failed for telnet, source - 16.1.1.200
6	[illegible]	03-Jan-2000 16:39:41	Error	%AAA-E-AUTHFAIL: Authentication failed for telnet, source - 16.1.1.200
7	[illegible]	03-Jan-2000 16:39:38	Error	%AAA-E-AUTHFAIL: Authentication failed for telnet, source - 16.1.1.200
8	[illegible]	03-Jan-2000 16:39:36	Error	%AAA-E-AUTHFAIL: Authentication failed for telnet, source - 16.1.1.200
9	[illegible]	03-Jan-2000 16:39:33	Error	%AAA-E-AUTHFAIL: Authentication failed for telnet, source - 16.1.1.200
10	[illegible]	03-Jan-2000 16:39:31	Error	%AAA-E-AUTHFAIL: Authentication failed for telnet, source - 16.1.1.200
11	[illegible]	03-Jan-2000 16:39:20	Error	%AAA-E-AUTHFAIL: Authentication failed for telnet, source - 16.1.1.200

Log Index — The log number in the **Log File Table**.

Log Time — Specifies the time at which the log was entered in the **Log File Table**.

Severity — Specifies the log severity.

Description — The log message text.

Displaying the Log File Table Using the CLI Commands

The following table summarizes the equivalent CLI commands for viewing and setting fields displayed in the **Log File Table**.

Table 6-24. Log File Table CLI Commands

CLI Command	Description
show logging file	Displays the logging state and the syslog messages stored in the logging file.
clear logging file	Clears messages from the logging file.

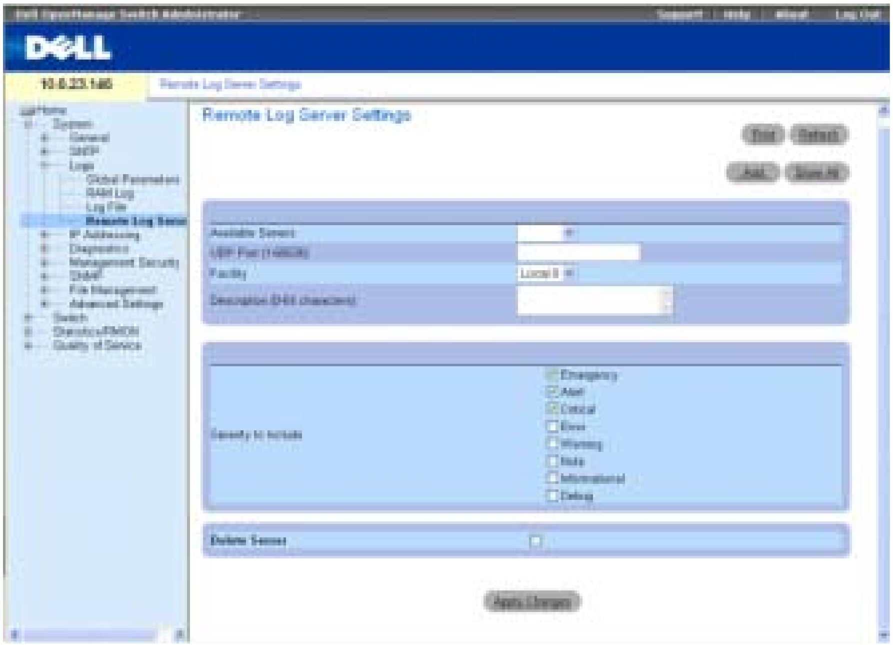
The following is an example of the CLI commands:

```
Console # show logging file

Logging is enabled.

Console Logging: Level info. Console Messages: 0 Dropped.

Buffer Logging: Level info. Buffer Messages: 62 Logged, 62
Displayed, 200 Max.

File Logging: Level debug. File Messages: 11 Logged, 51
Dropped.

SysLog server 12.1.1.2 Logging: warning. Messages: 14
Dropped.

SysLog server 1.1.1.1 Logging: info. Messages: 0 Dropped.

1 messages were not logged

01-Jan-2000 01:12:01 :%COPY-W-TRAP: The copy operation was
completed successfully

01-Jan-2000 01:11:49 :%LINK-I-Up:  g21

01-Jan-2000 01:11:49 :%2SWPHY-I-CHNGCOMBOMEDIA: Media
changed from copper media

to fiber media (1000BASE-SX) on port g21.

01-Jan-2000 01:11:48 :%2SWPHY-I-CHNGCOMBOMEDIA: Media
changed from fiber media to copper media on port g21.

01-Jan-2000 01:11:48 :%LINK-W-Down:  g21

01-Jan-2000 01:11:46 :%LINK-I-Up:  g19

01-Jan-2000 01:11:42 :%LINK-W-Down:  g14

01-Jan-2000 01:11:41 :%LINK-I-Up:  g14

01-Jan-2000 01:11:36 :%LINK-W-Down:  g9

01-Jan-2000 01:11:35 :%LINK-I-Up:  g1

01-Jan-2000 01:11:34 :%LINK-W-Down:  g1

console#
```

Configuring the Remote Log Server Settings Page

The **Remote Log Server Settings** page contains fields for viewing and configuring the available Log Servers. In addition, new log servers can be defined, and the log severity sent to each sever. To open the **Remote Log Server Settings** page, click **System→Logs→Remote Log Server** in the tree view.

Figure 6-32. Remote Log Server Settings



Remote Log Server Settings

Available Servers

UDP Port (1-65535)

Facility: Local 0

Description (0-64 characters)

Severity to Include:
☑ Emergency
☑ Alert
☑ Critical
☐ Error
☐ Warning
☐ Note
☐ Informational
☐ Debug

Delete Server ☐

Available Servers — Contains a list of servers to which logs can be sent.

UDP Port (1-65535) — The UDP port to which the logs are sent for the selected server. The possible range is 1 - 65535. The default value is 514.

Facility — Defines a user-defined application from which system logs are sent to the remote server. Only one facility can be assigned to a single server. If a second facility level is assigned, the first facility level is overridden. All applications defined for a device utilize the same facility on a server. The possible field values are:

Local 0 - Local 7.

Description (0-64 Characters) — The user-defined server description.

Delete Server — Deletes the currently selected server from the Available Servers list, when selected.

The **Remote Log Server Settings** page also contains a severity list. The severity definitions are the same as the severity definitions in the **Global Log Parameters** page.

Sending Logs to a Server:

1. Open the **Remote Log Server Settings** page.
2. Select a server from the **Available Servers** drop-down list.
3. Define the fields.
4. Select the log severity in the **Severity to Include** check boxes.
5. Click **Apply Changes**.

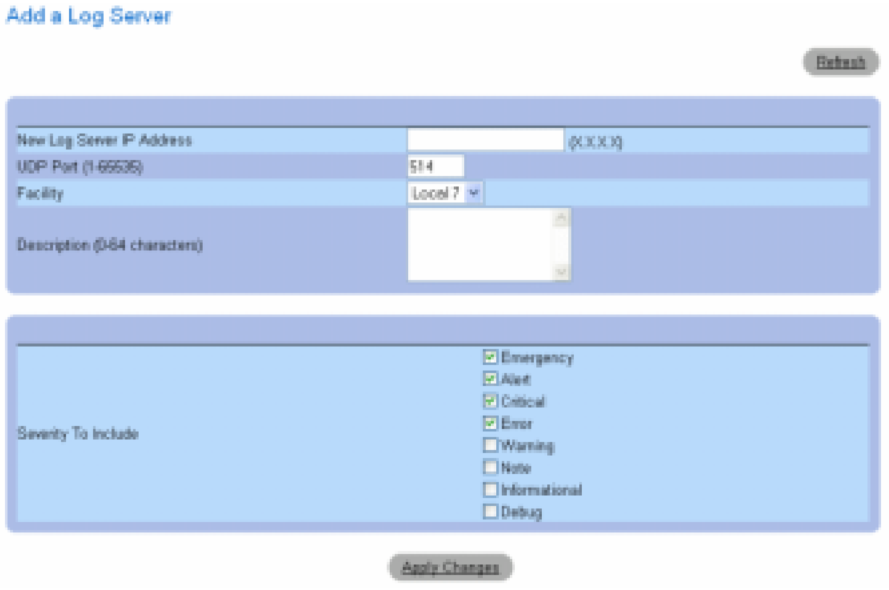
   The log settings are saved, and the device is updated.

Defining a New Server:

1. Open the **Remote Log Server Settings** page.
2. Click **Add.**

   The **Add a Log Server** page opens:

Figure 6-33. Add a Log Server



Add a Log Server

New Log Server IP Address	(X.X.X.X)
UDP Port (1-65535)	514
Facility	Local 7
Description (0-64 characters)	
Severity To Include	☑ Emergency ☑ Alert ☑ Critical ☑ Error □ Warning □ Note □ Informational □ Debug

New Log Server IP Address — Defines the IP address of the new Log Server.

3 Define the fields.

4 Click **Apply Changes**.

The server is defined and added to the **Available Servers** list.

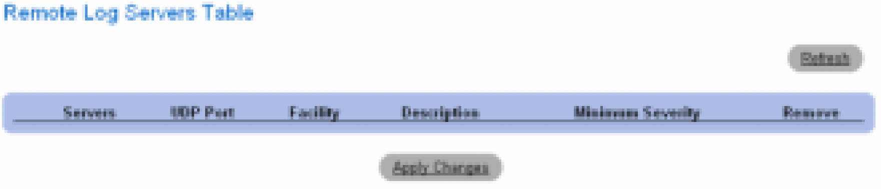
Displaying the Remote Log Servers Table:

1 Open the **Remote Log Server Settings** page.

2 Click **Show All**.

The **Remote Log Servers Table** page opens:

Figure 6-34. Remote Log Servers Table



Remote Log Servers Table

Servers	UDP Port	Facility	Description	Minimum Severity	Remove

Removing a Log Server from the Log Server Table Page:

1 Open the **Remote Log Server Settings** page.

2 Click **Show All**.

The **Remote Log Servers Table** page opens.

3 Select a **Remote Log Servers Table** entry.

4 Select the **Remove** check box to remove the server(s).

5 Click **Apply Changes**.

The **Remote Log Servers Table** entry is removed, and the device is updated.

Working with Remote Server Logs Using the CLI Commands

The following table summarizes the equivqlent CLI command for working with remote server logs.

Table 6-25. Remote Log Server CLI Commands

CLI Command	Description
logging *(ip-address* | *hostname)* [**port** *port*] [**severity** *level*] [**facility** *facility*] **description** *text*]	Logs messages to a remote server.
no logging	Deletes a syslog server.
show logging	Displays the state of logging and the syslog messages.

The following is an example of the CLI commands:

```
console> enable
console# configure
console (config) # logging 10.1.1.1 severity critical


Console# show logging
Logging is enabled.
Console Logging: Level debug. Console Messages: 5 Dropped.
Buffer Logging: Level debug. Buffer Messages: 16 Logged, 16
Displayed, 200 Max.
File Logging: Level error. File Messages: 0 Logged, 209 Dropped.
SysLog server 31.1.1.2 Logging: error. Messages: 22 Dropped.
SysLog server 5.2.2.2 Logging: info. Messages: 0 Dropped.
SysLog server 10.2.2.2 Logging: critical. Messages: 21 Dropped.
SysLog server 10.1.1.1 Logging: critical. Messages: 0 Dropped.
1 messages were not logged
03-Mar-2004 12:02:03 :%LINK-I-Up: g1
03-Mar-2004 12:02:01 :%LINK-W-Down: g2
03-Mar-2004 12:02:01 :%LINK-I-Up: g3
```

Defining Device IP Addresses

The **IP Addressing** page contains links for assigning interface and default gateway IP addresses, and defining ARP and DHCP parameters for the interfaces. To open the **IP Addressing** page, click **System →IP Addressing** in the tree view.

Defining Default Gateways

The **Default Gateway** page contains fields for assigning Gateway devices. Packets are forwarded to the default IP when frames are sent to a remote network. The configured IP address must belong to the same IP address subnet of one of the IP interfaces. To open the **Default Gateway** page, click **System→IP Addressing →Default Gateway** in the tree view.

The **Default Gateway** page contains the following fields:

Default Gateway — The Gateway device IP address.

Remove — Removes Gateway devices from the **Default Gateway** drop-down list, when selected

Selecting a Gateway Device:

1. Open the **Default Gateway** page.
2. Select an IP address in the **Default Gateway** drop-down list.
3. Select the **Active** check box.
4. Click **Apply Changes**.

   The gateway device is selected and the device is updated.

Removing a Default Gateway Device:

1. Open the **Default Gateway** page.
2. Select the **Remove** check box to remove default gateways.
3. Click **Apply Changes**.

   The default gateway entry is removed, and the device is updated.

Defining Gateway Devices Using the CLI Commands

The following table summarizes the equivalent CLI commands for setting fields displayed in the **Default Gateway** page.

Table 6-26. Default Gateway CLI Commands

CLI Command	Description
ip default-gateway *ip-address*	Defines a default gateway.
no ip default-gateway	Removes a default gateway.

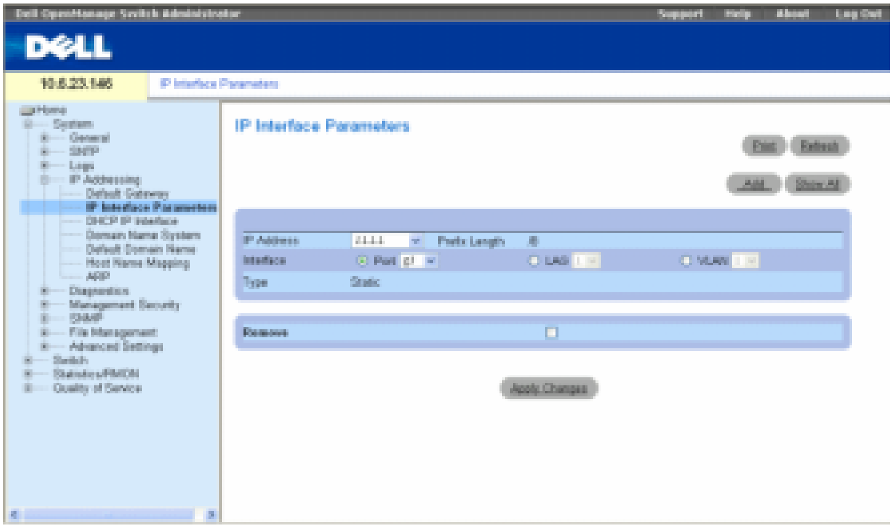
The following is an example of the CLI commands:

```
Console (config)# ip default-gateway 196.210.10.1
Console (config)# no ip default-gateway
```

Defining IP Interfaces

The **IP Interface Parameters** page contains fields for assigning IP parameters to interfaces. To open the **IP Interface Parameters** page, click **System→IP Addressing→Interface Parameters** in the tree view.

Figure 6-35. IP Interface Parameters



IP Interface Parameters

IP Address 2.1.1.1 Prefix Length 8

Interface ● Port g1 ○ LAG 1 ○ VLAN 1

Type Static

Remove □

IP Address — The interface IP address.

Prefix Length — The number of bits that comprise the source IP address prefix, or the network mask of the source IP address.

Interface — The interface type for which the IP address is defined. Select **Port**, **LAG**, or **VLAN**.

For more information, see "Configuring VLANs".

Type — Indicates whether or not the IP address was configured statically.

Forward Directed IP Broadcasts — Enables the translation of a directed broadcast to physical broadcasts. Disabling drops IP-directed broadcasts and does not forward them.

Broadcast Type — Defines an interface broadcast address.

One Fill — The interface broadcast address is one fill (255.255.255.255).

Zero Fill — The interface broadcast address is zero fill (0.0.0.0).

Remove — When selected, removes the interface from the **IP Address** drop-down menu.

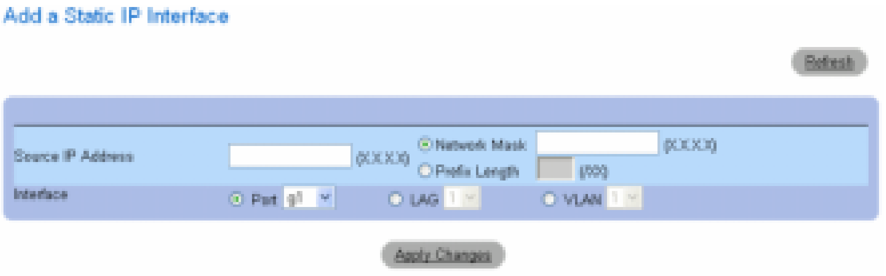
Adding an IP Interface

1 Open the **IP Interface Parameters** page.

2 Click **Add**.

The **Add a Static Interface** page opens:

Figure 6-36. Add a Static Interface



Add a Static IP Interface

Source IP Address (X.X.X.X) ● Network Mask (X.X.X.X) ○ Prefix Length (XX)

Interface ● Port g1 ○ LAG 1 ○ VLAN 1

3 Complete the fields on the page.

Network Mask specifies the subnetwork mask of the source IP address.

4 Click **Apply Changes**.

The new interface is added, and the device is updated.

Modifying IP Address Parameters

1 Open the **IP Interface Parameters** page.

2 Select an IP address in the **IP Address** drop-down menu.

3 Modify the required fields.

4 Click **Apply Changes**.

The parameters are modified, and the device is updated.

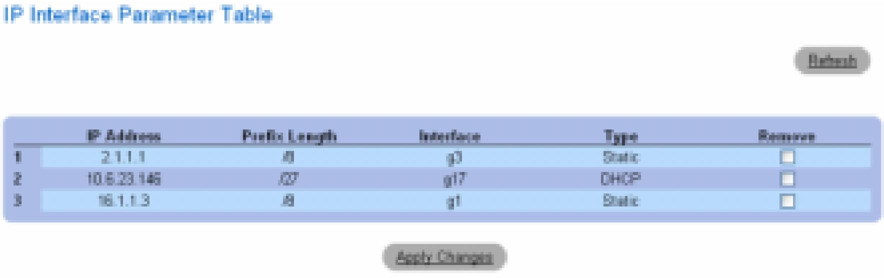
Deleting IP Addresses

1 Open the **IP Interface Parameters** page.

2 Click **Show All**.

The **Interface Parameters Table** opens:

Figure 6-37. IP Interface Parameter Table



IP Interface Parameter Table

	IP Address	Prefix Length	Interface	Type	Remove
1	2.1.1.1	/8	g3	Static	□
2	10.6.23.146	/27	g17	DHCP	□
3	16.1.1.3	/8	g1	Static	□

3 Select an IP address and select the **Remove** check box.

4 Click **Apply Changes**.

The selected IP address is deleted, and the device is updated.

Defining IP Interfaces Using CLI Commands

The following table summarizes the equivalent CLI commands for setting fields displayed in the **IP Interface Parameters** page.

Table 6-27. IP Interface Parameters CLI Commands

CLI Command	Description
ip address *ip-address* {*mask* | *prefix-length*}	Sets an IP address.
no ip address [*ip-address*]	Removes an IP address
show ip interface [**ethernet** *interface-number* | **vlan** *vlan-id* / **port-channel** *number*]	Displays the usability status of interfaces configured for IP.

The following is an example of the CLI commands:

```
   Console (config)# interface vlan 1
   Console (config-if)# ip address 131.108.1.27 255.255.255.0
   Console (config-if)# no ip address 131.108.1.27
Console (config-if)# exitconsole# show ip interface vlan 1
Output
```

Defining DHCP IP Interface Parameters

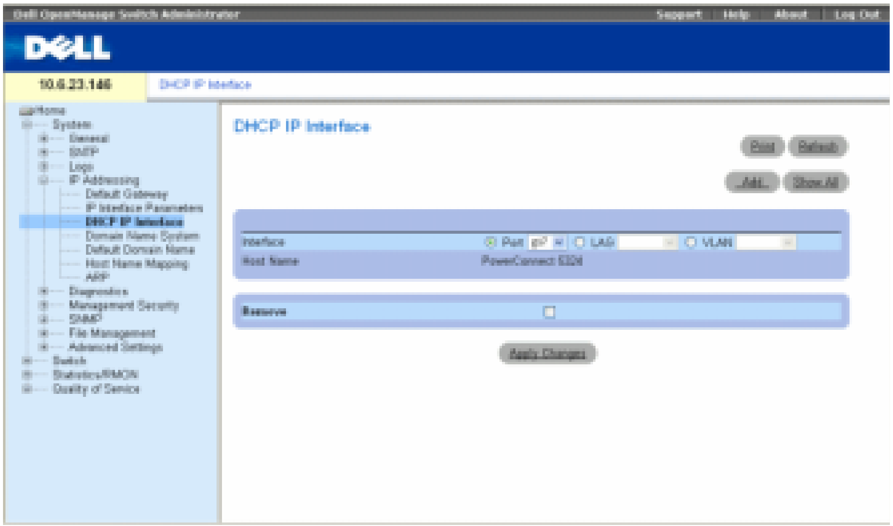
```
console# show ip interface vlan 1
```

Output

```
Gateway IP Address      Activity status
---------------------   ------------------
192.168.1.1             Active

IP address              Interface           Type
-------------------     ------------        ------------
192.168.1.123 /24        VLAN 1              Static
```

The **DHCP IP Interface** page contains fields for specifying the DHCP clients connected to the device. Click **System→IP Addressing→DHCP IP Interface** in the tree view. To open the **DHCP IP Interface** page.

Figure 6-38. DHCP IP Interface



Interface ● Port g? ○ LAG ○ VLAN

Host Name PowerConnect 5324

Remove □

Interface — The specific interface connected to the device. Click the option button next to **Port**, **LAG**, or **VLAN** and select the interface connected to the device.

Host Name — The system name. This field can contain up to 20 characters.

Remove — When selected, removes DHCP clients.

Adding DHCP Clients

1. Open the **DHCP IP Interface** page.
2. Click **Add**.

   The **Add DHCP IP Interface** page opens.
3. Complete the information on the page.
4. Click **Apply Changes**.

   The DHCP Interface is added, and the device is updated.

Modifying a DHCP IP Interface

1. Open the **DHCP IP Interface** page.
2. Modify the fields.
3. Click **Apply Changes**.

   The entry is modified, and the device is updated.

Deleting a DHCP IP Interface

1. Open the **DHCP IP Interface** page.

2. Click **Show All**.

   The **DHCP Client Table** opens.

3. Select a DHCP client entry.
4. Select the **Remove** check box.
5. Click **Apply Changes**.

   The selected entry is deleted, and the device is updated.

Defining DHCP IP Interfaces Using CLI Commands

The following table summarizes the equivalent CLI commands for defining DHCP clients.

Table 6-28. DHCP IP Interface CLI Commands

CLI Command	Description
ip address dhcp [hostname *host-name*]	To acquire an IP address on an Ethernet interface from the Dynamic Host Configuration Protocol (DHCP).

The following is an example of the CLI command:

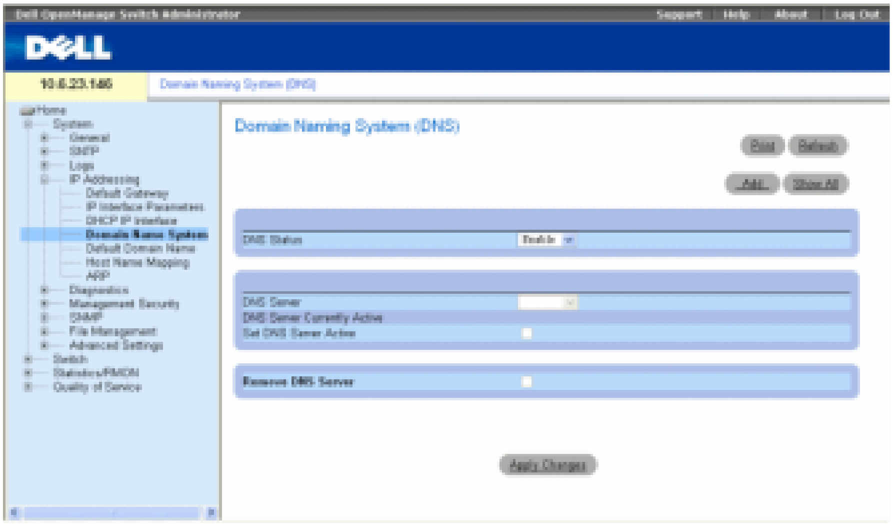
```
console> enable

console# config

console (config#) interface ethernet g1

console (config-if)# ip address dhcp 10.0.0.1 /8
```

Configuring Domain Name Systems

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 **Domain Naming System (DNS)** page contains fields for enabling and activating specific DNS servers. To open the **Domain Naming System (DNS)** page, click **System→IP Addressing→Domain Name System** in the tree view.

Figure 6-39. Domain Naming System (DNS)



Domain Naming System (DNS)

DNS Status Enable

DNS Server

DNS Server Currently Active

Set DNS Server Active □

Remove DNS Server □

DNS Status — Enables or disables translating DNS names into IP addresses.

DNS Server — Contains a list of DNS servers. DNS servers are added in the **Add DNS Server** page.

DNS Server Currently Active — The DNS server that is currently the active DNS server.

Set DNS Server Active — Activates the DNS server selected in the **DNS Server** field.

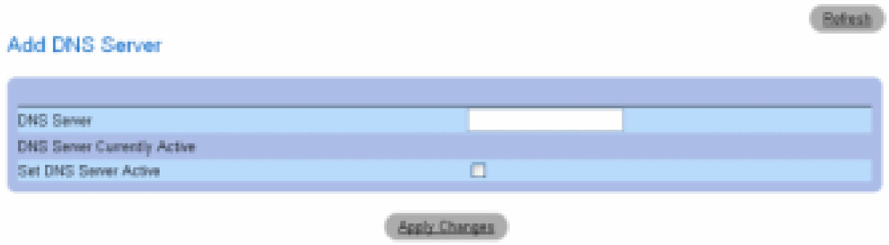
Remove DNS Server — When selected, removes DNS Servers.

Adding a DNS Server

1. Open the **Domain Naming System (DNS)** page.
2. Click **Add**.

   The **Add DNS Server** page opens:

Figure 6-40. Add DNS Server



Add DNS Server

DNS Server	
DNS Server Currently Active	
Set DNS Server Active	□

3 Define the relevant fields.

4 Click **Apply Changes**.

The new DNS server is defined, and the device is updated.

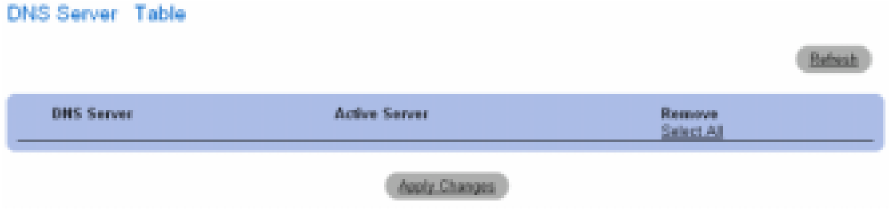
Displaying the DNS Servers Table

1 Open the **Domain Naming System (DNS)** page.

2 Click **Show All.**

The **DNS Server Table** opens:

Figure 6-41. DNS Server Table



DNS Server Table

DNS Server	Active Server	Remove Select All

Removing DNS Servers

1 Open the **Domain Naming System (DNS)** page.

2 Click **Show All.**

3 The **DNS Server Table** opens.

4 Select a **DNS Server Table** entry.

5 Select the **Remove** check box.

6 Click **Apply Changes.**

The selected DNS server is deleted, and the device is updated.

Configuring DNS Servers Using the CLI Commands

The following table summarizes the CLI commands for configuring device system information.

.

Table 6-29. DNS Server CLI Commands

CLI Command	Description
ip name-server *server-address*	Sets the available name servers. Up to eight name servers can be set.
no ip name-server *server-address*	Removes a name server.
ip domain-name *name*	Defines a default domain name that the software uses to complete unqualified host names.
clear host {*name* | *}	Deletes entries from the host name-to-address cache.
show hosts [*name*]	Displays the default domain name, list of name server hosts, the static and the cached list of host names and addresses.

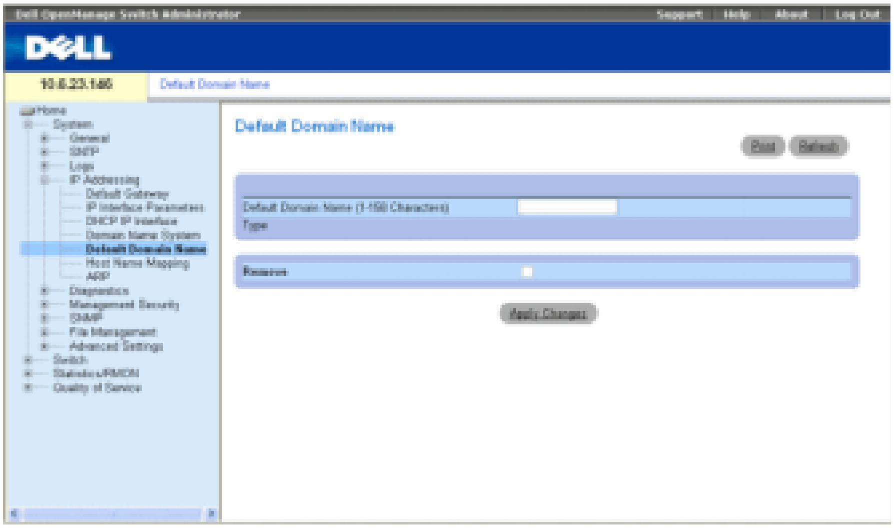
The following is an example of the CLI commands:

```
console> enable
Console# configure
console (config)# ip name-server 176.16.1.18
```

Defining Default Domains

The **Default Domain Name** page provides information for defining default DNS domain names. To open the **Default Domain Name** page, click **System→IP Addressing→Default Domain Name** in the tree view.

Figure 6-42. Default Domain Name



Default Domain Name

Default Domain Name (1-158 Characters)

Type

Remove □

Default Domain Name (1-158 characters) — Contains a user-defined DNS domain name server. When selected, the DNS domain name is the default domain.

Type — The domain type if the domain was statically or dynamically created.

Remove — When selected, removes a selected domain.

Defining DNS Domain Names Using the CLI Commands

The following table summarizes the CLI commands for configuring DNS domain names.

Table 6-30. DNS Domain Name CLI Commands

CLI Command	Description
ip domain-name *name*	Defines a default domain name that the software uses to complete unqualified host names.
no ip domain-name	Disable the use of the Domain Name System (DNS).
show hosts [*name*]	Displays the default domain name, list of name server hosts, the static and the cached list of host names and addresses.

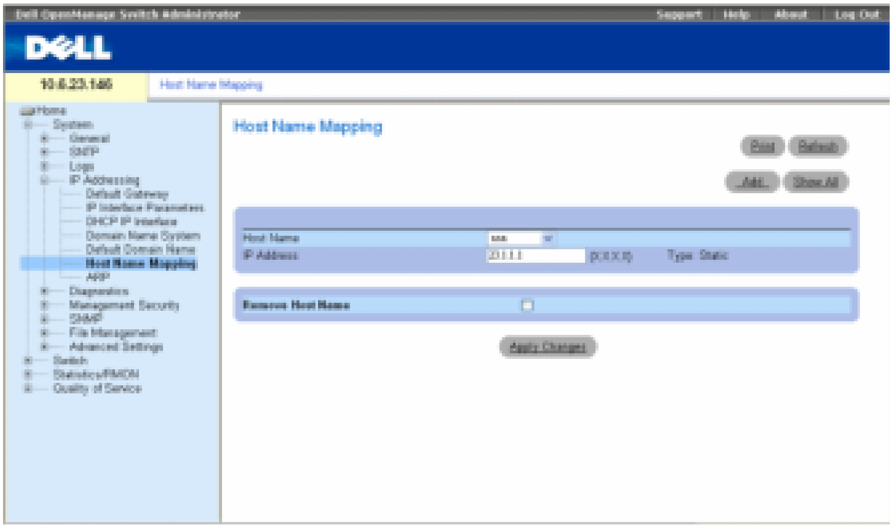
The following is an example of the CLI commands:

```
console> enable

console# configure

console (config)# ip domain-name www.dell.com
```

Mapping Domain Host

The **Host Name Mapping** page provides parameters for assigning static host names IP addresses. The **Host Name Mapping** page provides up to eight IP addresses per host. To open the **Host Name Mapping** page, click **System→IP Addressing→Host Name Mapping.**

Figure 6-43. Host Name Mapping



Host Name Mapping

Host Name

IP Address 2.1.1.1 (X.X.X.X) Type: Static

Remove Host Name ☐

Host Name — Contains a Host Name list. Host Name are defined in the **Add Host Name Mapping** page. Each host provides up to eight IP address. The field values for the Host Name field are:

IP Address (X.X.X.X) — Provides up to eight IP addresses that are assigned to the specified host name.

Type — The IP address type. The possible field values are:

> **Dynamic** — The IP address was created dynamically.
>
> **Static** — The IP address is a static IP address.

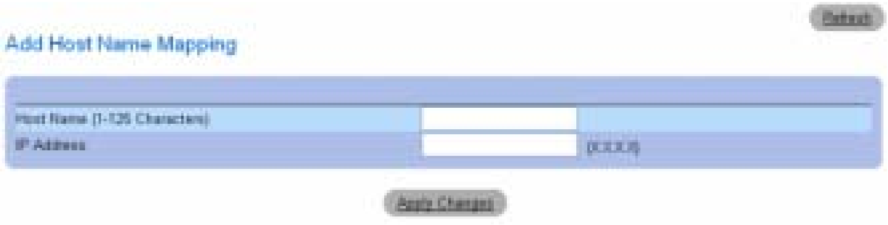
Remove Host Name Mapping — When checked, removes the DNS Host Mapping.

Adding Host Domain Names

1. Open the **Host Name Mapping** page.
2. Click **Add**.

   The **Add Host Name Mapping** page opens:

Figure 6-44. Add Host Name Mapping



Add Host Name Mapping

Host Name (1-126 Characters)		
IP Address		(X.X.X.X)

3 Define the relevant fields.

4 Click **Apply Changes**.

The IP address is mapped to the Host Name, and the is updated.

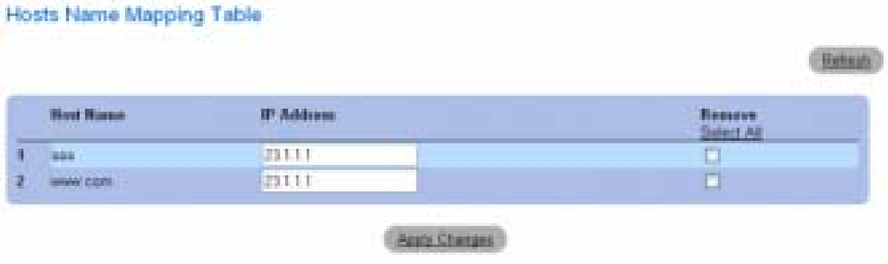
Displaying the Hosts Name Mapping Table

1 Open the **Host Name Mapping** page.

2 Click **Show All**.

The **Hosts Name Mapping Table** opens:

Figure 6-45. Hosts Name Mapping Table



Hosts Name Mapping Table

	Host Name	IP Address	Remove Select All
1	aaa	23.1.1.1	□
2	www.com	23.1.1.1	□

Removing Host Name from IP Address Mapping

1 Open the **Host Name Mapping** page.

2 Click **Show All**

3 The **Host Mapping Table** opens.

4 **Select a Host Mapping Table entry.**

5 **Check the Remove checkbox.**

6 Click **Apply Changes**.

The **Host Mapping Table** entry is deleted, and the is updated.

Mapping IP address to Domain Host Names Using the CLI Commands

The following table summarizes the equivalent CLI commands for mapping Domain Host names to IP addresses.

Table 6-31. Domain Host Name CLI Commands

CLI Command	Description
ip host name address1 [address2 … address8]	Defines the static host name-to-address mapping in the host cache
no ip host name	Removes the name-to-address mapping.
clear host {*name* | *}	Deletes entries from the host name-to-address cache.
show hosts [name]	Displays the default domain name, list of name server hosts, the static and the cached list of host names and addresses.

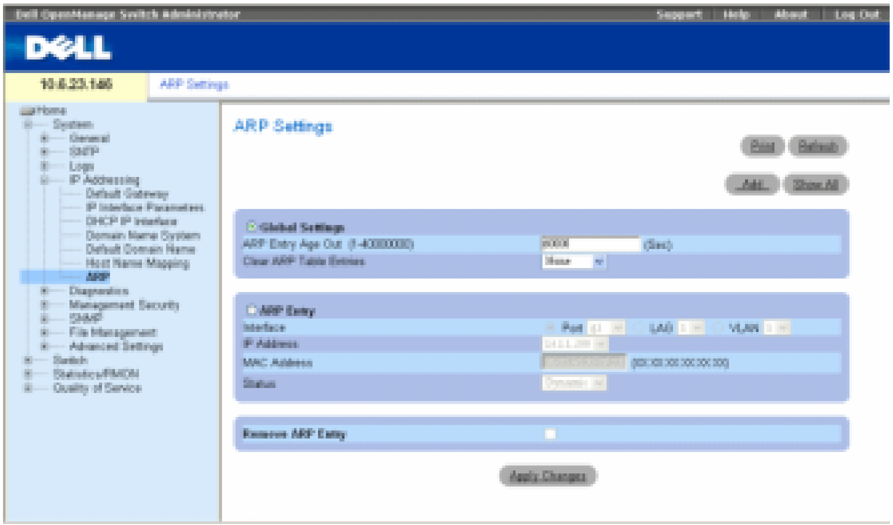
The following is an example of the CLI commands:

```
console# enable
console# configure
console (config)# ip host accounting.abc.com 176.10.23.1
```

Configuring ARP

The Address Resolution Protocol (ARP) is a TCP/IP protocol that converts IP addresses into physical addresses. The static entries can be defined in the **ARP Table.** When static entries are defined, a permanent entry is entered and used to translate IP addresses to MAC addresses. To open the **ARP Settings** page, click **System→IP Addressing→ARP** in the tree view.

Figure 6-46. ARP Settings



ARP Settings

● Global Settings

ARP Entry Age Out (1-40000000) 60000 (Sec)

Clear ARP Table Entries None

○ ARP Entry

Interface ○ Port ○ LAG ○ VLAN

IP Address

MAC Address (XX:XX:XX:XX:XX:XX)

Status Dynamic

Remove ARP Entry □

Global Settings — Select this option to activate the fields for ARP global settings.

ARP Entry Age Out (1-40000000) — For all devices, the amount of time (seconds) that pass between ARP requests about an ARP table entry. After this period, the entry is deleted from the table. The range is **1 - 4000000**, where zero indicates that entries are never cleared from the cache. The default value is 60000 seconds.

Clear ARP Table Entries — The type of ARP entries that are cleared on all devices. The possible values are:

- **None** — ARP entries are not cleared.
- **All** — All ARP entries are cleared.
- **Dynamic** — Only dynamic ARP entries are cleared.
- **Static** — Only static ARP entries are cleared.

ARP Entry — Select this option to activate the fields for ARP settings on a single device.

Interface — The interface number of the port, LAG, or VLAN that is connected to the device.

IP Address — The station IP address, which is associated with the MAC address filled in below.

MAC Address — The station MAC address, which is associated in the ARP table with the IP address.

Status — The ARP Table entry status. Possible field values are:

- **Dynamic** — The ARP entry is learned dynamically.
- **Static** — The ARP entry is a static entry.

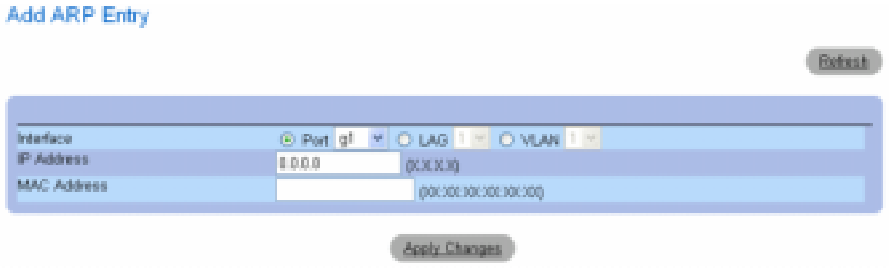
Remove ARP Entry — When selected, removes an ARP entry.

Adding a Static ARP Table Entry:

1. Open the **ARP Settings** page.
2. Click **Add**.

   The **Add ARP Entry** page opens:

Figure 6-47. Add ARP Entry Page



Interface	● Port g1 ○ LAG 1 ○ VLAN 1
IP Address	0.0.0.0 (X.X.X.X)
MAC Address	(XX:XX:XX:XX:XX:XX)

3. Select an interface.
4. Define the fields.
5. Click **Apply Changes**.

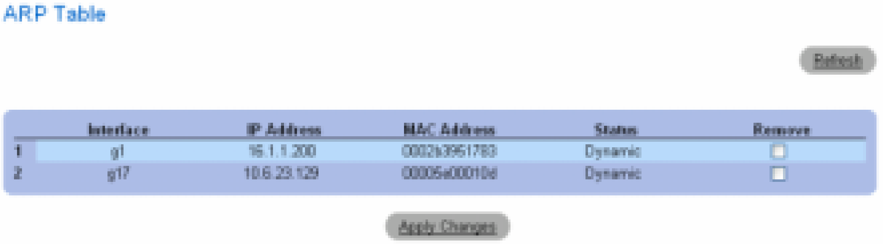
   The **ARP Table** entry is added, and the device is updated.

Displaying the ARP Table

1. Open the **ARP Settings** page.
2. Click **Show All**.

   The **ARP Table** opens:

Figure 6-48. ARP Table Page



ARP Table

	Interface	IP Address	MAC Address	Status	Remove
1	g1	16.1.1.200	0002b3951783	Dynamic	□
2	g17	10.6.23.129	00006a00010d	Dynamic	□

Deleting ARP Table Entry

1. Open the **ARP Settings** page
2. Click **Show All.**

   The **ARP Table** page opens.

3. Select a table entry.
4. Select the **Remove** check box.
5. Click **Apply Changes**.

   The selected **ARP Table** entry is deleted, and the device is updated.

Configuring ARP Using the CLI Commands

The following table summarizes the equivalent CLI commands for setting fields displayed in the **ARP Settings** page.

Table 6-32. ARP Settings CLI Commands

CLI Command	Description
arp *ip_addr hw_addr* {**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*}	Adds a permanent entry in the ARP cache.
arp timeout *seconds*	Configures how long an entry remains in the ARP cache.
clear arp-cache	Deletes all dynamic entries from the ARP cache
show arp	Displays entries in the ARP Table.
no arp	Removes an ARP entry from the ARP Table.

The following is an example of the CLI commands:

```
    Console(config)# arp 198.133.219.232 00-00-0c-40-0f-bc
    Console (config)# exit
    Console# arp timeout 12000
    Console# show arp
    ARP timeout: 80000 Seconds
Interface    IP address       HW address          Status
---------    ----------       ----------          ------
g1           10.7.1.102       00:10:B5:04:DB:4B   Dynamic
g2           10.7.1.135       00:50:22:00:2A:A4   Static
```

Running Cable Diagnostics

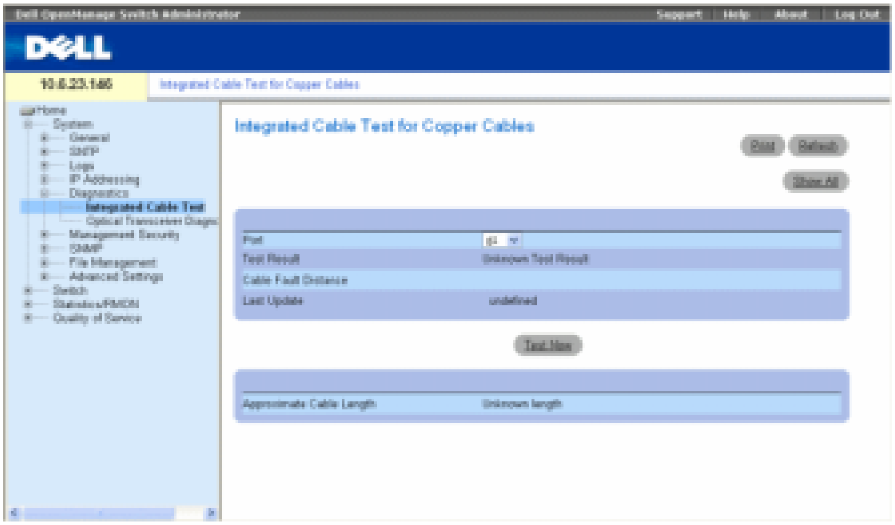
The **Diagnostics** page contains links to pages for performing virtual cable tests on copper and fiber optics cables. To open the **Diagnostics** page, click **System→Diagnostics** in the tree view.

Viewing Copper Cable Diagnostics

The **Integrated Cable Test for Copper Cables** page contains fields for performing tests on copper cables. Cable testing provides information about where errors occurred in the cable, the last time a cable test was performed, and the type of cable error which occurred. The tests use Time Domain Reflectometry (TDR) technology to test the quality and characteristics of a copper cable attached to a port. Cables up to 120 meters long can be tested. Cables are tested when the ports are in the down state, with the exception of the Approximated Cable Length test.

To open the **Integrated Cable Test for Copper Cables** page, click **System→Diagnostics→ Integrated Cable Test** in the tree view.

Figure 6-49. Integrated Cable Test for Copper Cables



Integrated Cable Test for Copper Cables

Port	g1
Test Result	Unknown Test Result
Cable Fault Distance	
Last Update	undefined

Approximate Cable Length	Unknown length

Port — The port to which the cable is connected.

Test Result — The cable test results. Possible values are:

- **No Cable** — There is no cable connected to the port.
- **Open Cable** — The cable is connected on only one side.
- **Short Cable** — A short has occurred in the cable.
- **OK** — The cable passed the test.
- **Fiber Cable** — A fiber cable is connected to the port.

Cable Fault Distance — The distance from the port where the cable error occurred.

Last Update — The last time the port was tested.

Approximate Cable Length — The approximate cable length. This test can only be performed when the port is up and operating at 1 Gbps.

Performing a Cable Test

1 Ensure that both ends of the copper cable are connected to a device.

2 Open the **Integrated Cable Test for Copper Cables** page.

3 Click **Test Now**.

The copper cable test is performed, and the results are displayed on the **Integrated Cable Test for Copper Cables** page.

Displaying Virtual Cable Test Results Table

1 Open the **Integrated Cable Test for Copper Cables** page.

2 Click **Show All**.

The **Virtual Cable Test Results Table** opens.

Performing Copper Cable Tests Using CLI Commands

The following table summarizes the equivalent CLI commands for performing copper cable tests.

Table 6-33. Copper Cable Test CLI Commands

CLI Command	Description
test copper-port tdr *interface*	Performs VCT tests.
show copper-port tdr [*interface*]	Shows results of last VCT tests on ports.
show copper-port cable-length [*interface*]	Displays the estimated copper cable length attached to a port.

The following is an example of the CLI commands:

```
console> enable
Console# test copper-port tdr g3
Cable is open at 100 meters.
Console> show copper-ports tdr
Port      Result       Length [meters]   Date
----      ------       ---------------   ----
g1        OK
g2        Short        50                13:32:00 15 January 2004
g3        Test has not been performed
g4        Open         64                13:32:00 15 January 2004
g5        Fiber        -                 -
```

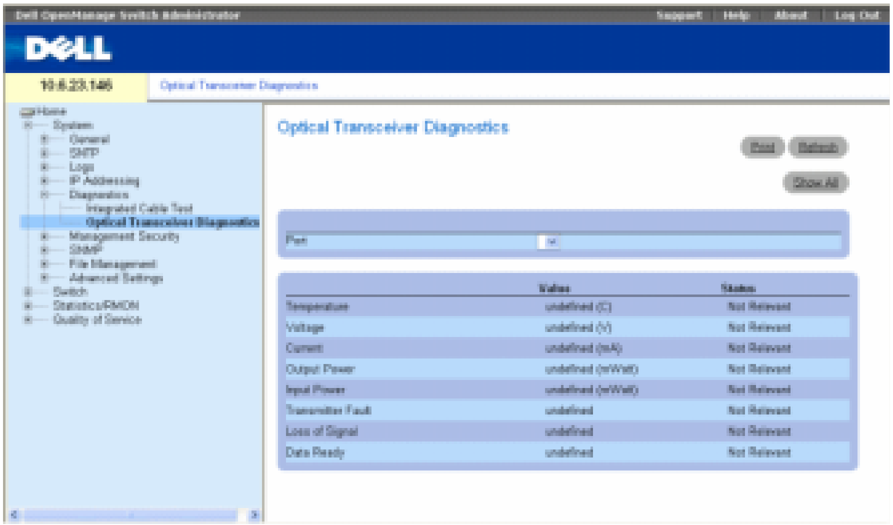
NOTE: The cable length returned is an approximation in the ranges of up to 50 meters, 50m-80m, 80m-110m, 110m-120m, or more than 120m. The deviation may be up to 20 meters.

Viewing Optical Transceiver Diagnostics

The **Optical Transceiver Diagnostics** page contians fields for performing tests on Fiber Optic cables. To open the **Optical Transceiver Diagnostics** page, click **System→Diagnostics→Optical Transceiver Diagnostics** in the tree view.

NOTE: Optical transceiver diagnostics can be performed only when the link is present.

Figure 6-50. Optical Transceiver Diagnostics



Optical Transceiver Diagnostics

Port

	Value	Status
Temperature	undefined (C)	Not Relevant
Voltage	undefined (V)	Not Relevant
Current	undefined (mA)	Not Relevant
Output Power	undefined (mWatt)	Not Relevant
Input Power	undefined (mWatt)	Not Relevant
Transmitter Fault	undefined	Not Relevant
Loss of Signal	undefined	Not Relevant
Data Ready	undefined	Not Relevant

Port — The port to which the fiber cable is connected.

Temperature — The temperature (in Celsius) at which the cable is operating.

Voltage — The voltage at which the cable is operating.

Current — The current at which the cable is operating.

Output Power — The rate at which the output power is transmitted.

Input Power — The rate at which the input power is transmitted.

Transmitter Fault — Indicates if a fault occurred during transmission.

Loss of Signal — Indicates if a signal loss occurred in the cable.

Data Ready — The transceiver has achieved power up and data is ready.

Displaying Optical Transceiver Diagnostics Test Results Table

1. Open the **Optical Transceiver Diagnostics** page.
2. Click **Show All**.

   The test is run and the **Virtual Cable Test Results Table** opens.

Performing Fiber Optic Cable Tests Using CLI Commands

The following table summarizes the equivalent CLI command for performing fiber optic cable tests.

Table 6-34. Fiber Optic Cable Test CLI Commands

CLI Command	Description
show fiber-ports optical-transceiver [*interface*] **[detailed]**	Displays the optical transceiver diagnostics.

The following is an example of the CLI command:

```
console> enable
Console# show fiber-ports optical-transceiver
                                       Power
Port  Temp    Voltage   Current    Output   Input    TX      LOS
      (C)     (Volt)    (mA)       (mWatt)  (mWatt)  Fault

g1    W       OK        E          OK       OK       OK      OK
g2    OK      OK        OK         OK       OK       E       OK
g3    Copper

Temp – Internally measured transceiver temperature.
Voltage - Internally measured supply voltage.
Current – Measured TX bias current.
Output Power – Measured TX output power.
Input Power – Measured RX  received power.
Tx Fault – Transmitter fault
LOS – Loss of signal
```

The **Optical Transceiver Diagnostics Table** contains the following columns:

- **Temp** — Internally measured transceiver temperature.
- **Voltage** — Internally measured supply voltage.
- **Current** — Measured TX bias current.
- **Output Power** — Measured TX output power in milliwatts.
- **Input Power** — Measured RX received power in milliwatts.
- **TX Fault** — Transmitter fault.

NOTE: Finisair transceivers do not support the transmitter fault diagnostic testing.

- **LOS** — Loss of signal.
- **Data Ready** — The transceiver has archived power up and data is ready.
- **N/A** — Not Available, N/S - Not Supported, W - Warning, E - Error.

NOTE: Fiber Optic analysis feature works only on SFPs that support the digital diagnostic standard SFF-4872.

Managing Device Security

The **Management Security** page provides access to security pages that contain fields for setting security parameters for ports, device management methods, user, and server security. To open the **Management Security** page, click **System→Management Security** in the tree view.

Defining Access Profiles

The **Access Profiles** page contains fields for defining profiles and rules for accessing the device. Access to management functions can be limited to user groups, which are defined by ingress interfaces and source IP address and/or source IP subnets.

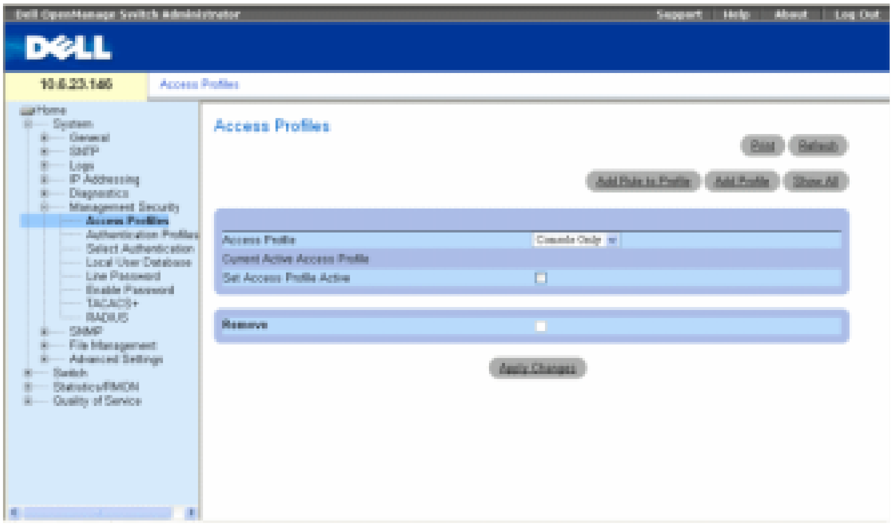
Management access can be separately defined for each type of management access method, including, Web (HTTP), Secure web (HTTPS), Telnet, Secure Telnet and SNMP.

Access to different management methods may differ between user groups. For example, User Group 1 can access the device only via an HTTPS session, while User Group 2 can access the device via both HTTPS and Telnet sessions.

Management Access Lists contain the rules that determine which users can manage the device, and by which methods. Users can also be blocked from accessing the device.

The **Access Profiles** page contains fields for configuring Management Lists and applying them to specific interfaces. To open the **Access Profiles** page, click **System→Management Security→Access Profiles** in the tree view.

Figure 6-51. Access Profiles



Access Profiles

Access Profile: Console Only

Current Active Access Profile

Set Access Profile Active ☐

Remove ☐

Access Profile — User-defined Access Profile lists. The **Access Profile** list contains a default value of **Console List**, to which user-defined access profiles are added. Selecting **Console Only** as the **Access Profile** name disconnects the session, and enables accessing the device from the console only.

Current Active Access Profile — The access profile that is currently active.

Set Access Profile Active — Activates an access profile.

Remove — Removes an access profile from the **Access Profile Name** list, when selected.

Activating a Profile

1. Open the **Access Profiles** page.
2. Select an Access Profile in the **Access Profile** field.
3. Select the **Set Access Profile Active** check box.
4. Click **Apply Changes**.

   The Access Profile is activated.

Adding an Access Profile

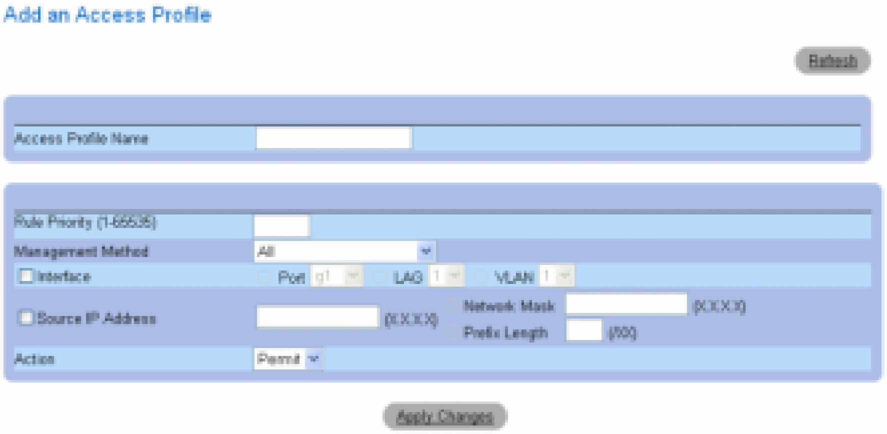
Rules act as filters for determining rule priority, the device management method, interface type, source IP address and network mask, and the device management access action. Users can be blocked or permitted management access. Rule priority sets the order of rule application in a profile.

Defining Rules for an Access Profile:

1. Open the **Access Profiles** page.
2. Click **Add an Access Profile.**

   The **Add An Access Profile** page opens:

Figure 6-52. Add An Access Profile Page



Add an Access Profile

Access Profile Name	

Rule Priority (1-65535)		
Management Method	All	
□ Interface	○ Port g1 ○ LAG 1 ○ VLAN 1	
□ Source IP Address	(X.X.X.X)	○ Network Mask (X.X.X.X) ○ Prefix Length (/XX)
Action	Permit	

Access Profile Name (1-32 Characters) — User-defined name for the access profile.

Rule Priority (1-65535) — The rule priority. When the packet is matched to a rule, user groups are either granted or denied device management access. The rule order is set by defining a rule number within the **Profile Rules Table**. The rule number is essential to matching packets to rules, as packets are matched on a first-fit basis. The rule priorities are assigned in the **Profile Rules Table**.

Management Method — The management method for which the access profile is defined. Users with this access profile can access the device using the management method selected.

Interface — The interface type to which the rule applies. This is an optional field. This rule can be applied to a selected port, LAG, or VLAN by selecting the check box and selecting the appropriate option button and interface.

NOTE: Assigning an access profile to an interface denies access via other interfaces. If an access profile is not assigned to any interface, the device can be accessed by all interfaces.

Source IP Address — The interface source IP address for which the rule applies. This is an optional field and indicates that the rule is valid for a subnetwork.

Network Mask — The IP subnetwork mask.

Prefix Length — The number of bits that comprise the source IP address prefix, or the network mask of the source IP address.

Action — Defines whether to permit or deny management access to the defined interface.

3 Define the **Access Profile Name** field.

4 Define the relevant fields.

5 Click **Apply Changes**.

The new Access Profile is added, and the device is updated.

Adding Rules to Access Profile

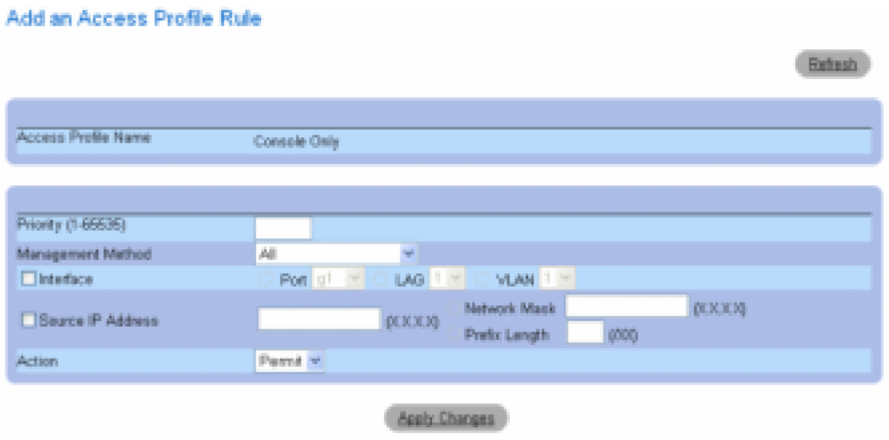
NOTE: The first rule must be defined to beginning matching traffic to access profiles.

1 Open the **Access Profiles** page.

2 Click **Add Profile to Rule**.

The **Add An Access Profile Rule** page opens:

Figure 6-53. Add An Access Profile Rule



Add an Access Profile Rule

Access Profile Name	Console Only

Priority (1-65535)	
Management Method	All
□ Interface	○ Port g1 ○ LAG 1 ○ VLAN 1
□ Source IP Address	(X.X.X.X) ○ Network Mask (X.X.X.X) ○ Prefix Length (XX)
Action	Permit

3 Complete the fields.

4 Click **Apply Changes**.

The rule is added to the access profile, and the device is updated.

Viewing the Profile Rules Table:

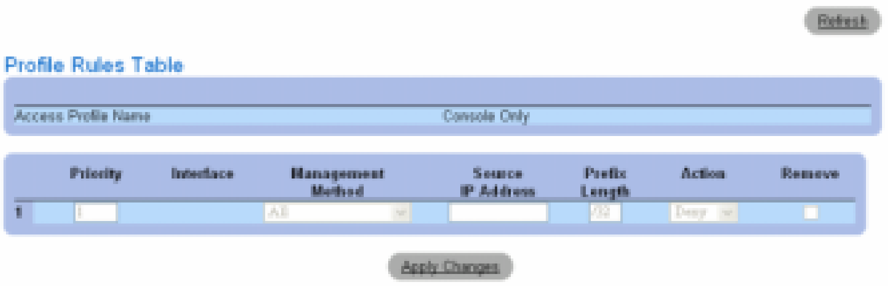
NOTE: The order in which rules appear in the *Profile Rules Table* is important. Packets are matched to the first rule which meets the rule criteria.

1 Open the **Access Profiles** page.

2 Click **Show All.**

The **Profile Rules Table Page** opens:

Figure 6-54. Profile Rules Table Page



Profile Rules Table

Access Profile Name	Console Only

	Priority	Interface	Management Method	Source IP Address	Prefix Length	Action	Remove
1	1		All		/32	Deny	□

Removing a Rule

1 Open the **Access Profiles** page.

2 Click **Show All**.

The **Profile Rules Table** opens.

3 Select a rule.

4 Select the **Remove** check box.

5 Click **Apply Changes**.

The selected rule is deleted, and the device is updated.

Defining Access Profiles Using CLI Commands

The following table summarizes the equivalent CLI commands for setting fields displayed in the **Access Profiles** page.

Table 6-35. Access Profiles CLI Commands

CLI Command	Description
management access-list *name*	Defines an access-list for management, and enters the access-list context for configuration.
permit [**ethernet** *interface-number* | **vlan** *vlan-id* / **port-channel** *number*] [**service** *service*]	Sets port permitting conditions for the management access list.
permit ip-source *ip-address* [**mask** *mask* | *prefix-length*] [**ethernet** *interface-number* | **vlan** *vlan-id* / **port-channel** *number*] [**service** *service*]	Sets port permitting conditions for the management access list, and the selected management method.

Table 6-35. Access Profiles CLI Commands

CLI Command	Description
deny [**ethernet** *interface-number* | **vlan** *vlan-id* / **port-channel** *number*] [**service** *service*]	Sets port denying conditions for the management access list, and the selected management method.
deny ip-source *ip-address* [**mask** *mask* | *prefix-length*] [**ethernet** *interface-number* | **vlan** *vlan-id* / **port-channel** *number*] [**service** *service*]	Sets port denying conditions for the management access list, and the selected management method.
management access-class {**console-only** | *name*}	Defines which access-list is used as the active management connections.
show management access-list [*name*]	Displays the active management access-lists.
show management access-class	Displays information about management access-class.

The following is an example of the CLI commands:

```
Console (config)# management access-list mlist
Console (config-macl)# permit ethernet g1
Console (config-macl)# permit ethernet g9
Console (config-macl)# deny ethernet g2
Console (config-macl)# deny ethernet g10
Console (config-macl)# exit
Console (config)# management access-class mlist
Console (config)# exit
Console# show management access-list
mlist
-----
permit ethernet g1
permit ethernet g9
! (Note: all other access implicitly denied)
Console> show management access-class
Management access-class is enabled, using access list mlist
```

Defining Authentication Profiles

The **Authentication Profiles** page contains fields for selecting the user authentication method on the device. User authentication occurs:

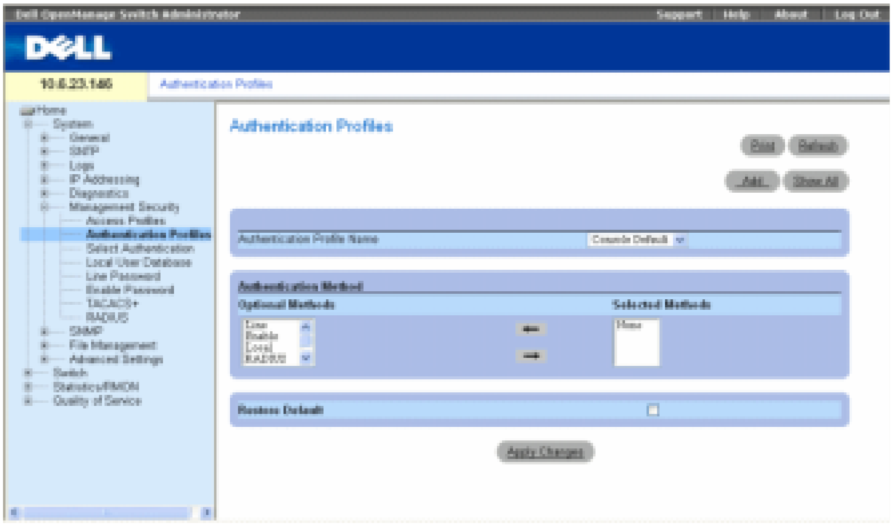
- Locally
- Via an external server

User authentication can also be set to *None*.

User authentication occurs in the order the methods are selected. For example, if both the *Local* and *RADIUS* options are selected, the user is authenticated first locally. If the local user database is empty, the user is then authenticated via the RADIUS server.

If an error occurs during the authentication, the next selected method is used. To open the **Authentication Profiles** page, click **System**→**Management Security**→**Authentication Profiles** in the tree view.

Figure 6-55. Authentication Profiles



Authentication Profiles

Authentication Profile Name: Console Default

Authentication Method

Optional Methods: Line, Enable, Local, RADIUS

Selected Methods: None

Restore Default □

Authentication Profile Name — User-defined authentication profile lists to which user-defined authentication profiles are added. The defaults are **Network Default** and **Console Default**.

Optional Methods — User authentication methods. Possible options are:

None — No user authentication occurs.

Local — User authentication occurs at the device level. The device checks the user name and password for authentication.

RADIUS — User authentication occurs at the RADIUS server. For more information, see "**Configuring RADIUS Global Parameters**."

Line — The line password is used for user authentication.

Enable — The enable password is used for authentication.

TACACS+ — The user authentication occurs at the TACACS+ server.

Restore Default— Restores the default user authentication method on the device.

Selecting an Authentication Profile:

1. Open the **Authentication Profiles** page.
2. Select a profile in the **Authentication Profile Name** field.
3. Select the authentication method using the navigation arrows.
4. Click **Apply Changes**.

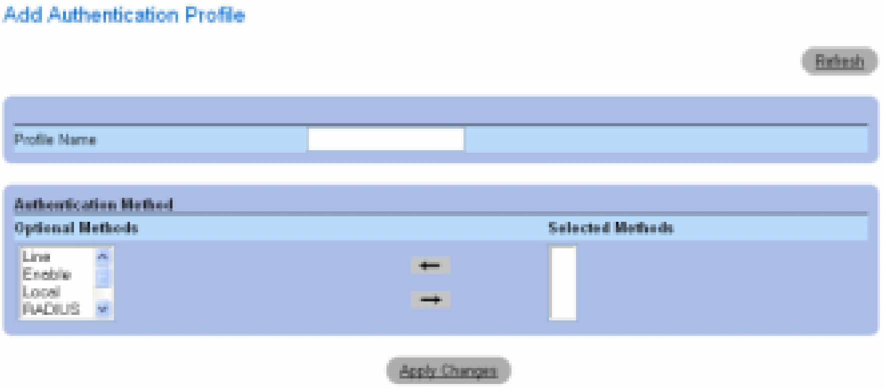
   The user authentication profile is updated to the device.

Adding an Authentication Profile:

1. Open the **Authentication Profiles** page.
2. Click **Add**.

   The **Add Authentication Method Profile Name** page opens:

Figure 6-56. Add Authentication Profile Page



Add Authentication Profile

3. Configure the profile.
4. Click **Apply Changes**.

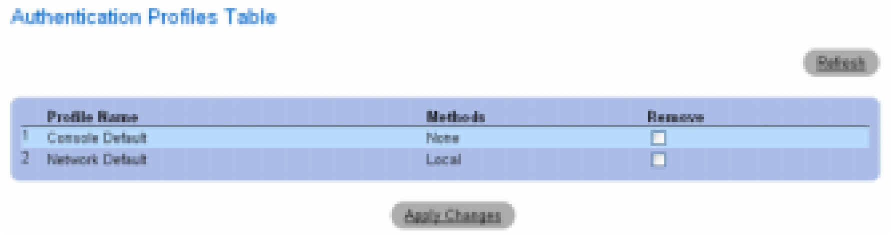
   The authentication profile is updated to the device.

Displaying the Show All Authentication Profiles Page:

1. Open the **Authentication Profiles** page.
2. Click **Show All**.

   The **Authentication Profile** page opens:

Figure 6-57. Authentication Profiles



Authentication Profiles Table

	Profile Name	Methods	Remove
1	Console Default	None	□
2	Network Default	Local	□

Deleting an Authentication Profiles:

1. Open the **Authentication Profiles** page.
2. Click **Show All**.

   The **Authentication Profile** page opens.
3. Select an authentication profile.
4. Select the **Remove** check box.
5. Click **Apply Changes**.

   The selected authenticating profile is deleted.

Configuring an Authentication Profile Using CLI Commands

The following table summarizes the equivalent CLI commands for setting fields displayed in the **Authentication Profiles** page.

Table 6-36. Authentication Profile CLI Commands

CLI Command	Description
aaa authentication login {default | *list-name*} *method1* [*method2*.]	Configures login authentication.
no aaa authentication login {default | *list-name*	Removes a login authentication profile.

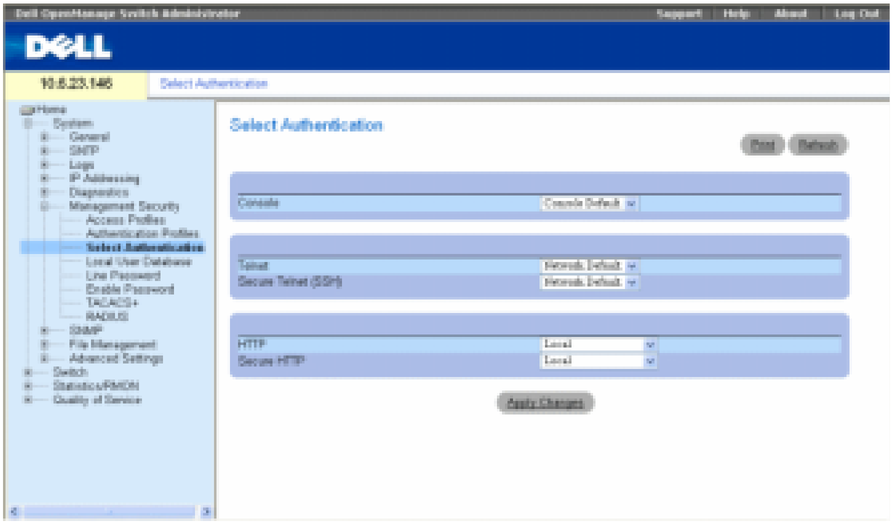
The following is an example of the CLI commands:

```
Console (config)# aaa authentication login default radius local
enable none

Console (config)# no aaa authentication login default
```

Assigning Authentication Profiles

After Authentication Profiles are defined, the Authentication Profiles can be applied to Management Access methods. For example, console users can be authenticated by Authentication Method Lists 1, while Telnet users are authenticated by Authentication Method List 2. To open the **Select Authentication** page, click **System→Management Security→Select Authentication** in the tree view.

Figure 6-58. Select Authentication



Console: Console Default

Telnet: Network Default

Secure Telnet (SSH): Network Default

HTTP: Local

Secure HTTP: Local

Console — Authentication profiles used to authenticate console users.

Telnet — Authentication profiles used to authenticate Telnet users.

Secure Telnet (SSH) — Authentication profiles used to authenticate Secure Shell (SSH) users. SSH provides clients with secure and encrypted remote connections to a device.

HTTP and **Secure HTTP** — Authentication method used for HTTP access and Secure HTTP access, respectively. Possible field values are:

> **None** — No authentication method is used for access.
>
> **Local** — Authentication occurs locally.
>
> **RADIUS** — Authentication occurs at the RADIUS server.

TACACS+ — Authentication occurs at the TACACS+ server.

Applying an Authentication List to Console Sessions

1 Open the **Select Authentication** page.

2 Select an Authentication Profile in the **Console** field.

3 Click **Apply Changes**.

Console sessions are assigned an Authentication List.

Applying an Authentication Profile to Telnet Sessions

1 Open the **Select Authentication** page.

2 Select an Authentication Profile in the **Telnet** field.

3 Click **Apply Changes**.

Telnet sessions are assigned an Authentication List.

Applying an Authentication Profile to Secure Telnet (SSH) Sessions

1 Open the **Select Authentication** page.

2 Select an Authentication Profile in the **Secure Telnet (SSH)** field.

3 Click **Apply Changes**.

Secure Telnet (SSH) sessions are assigned an Authentication Profile.

Assigning HTTP Sessions an Authentication Sequence

1 Open the **Select Authentication** page.

2 Select an authentication sequence in the **HTTP** field.

3 Click **Apply Changes**.

HTTP sessions are assigned an authentication sequence.

Assigning Secure HTTP Sessions an Authentication Sequence

1 Open the **Select Authentication** page.

2 Select an authentication sequence in the **Secure HTTP** field.

3 Click **Apply Changes**.

Secure HTTP sessions are assigned an authentication sequence.

Assigning Access Authentication Profiles or Sequences Using CLI Commands

The following table summarizes the equivalent CLI commands for setting fields displayed in the **Select Authentication** page.

Table 6-37. Select Authentication CLI Commands

CLI Command	Description
enable authentication [**default** | *list-name*]	Specifies the authentication method list when accessing a higher privilege level from a remote Telnet or console.
login authentication [**default** | *list-name*]	Specifies the login authentication method list for a remote Telnet or console.
ip http authentication *method1* [*method2*.]	Specifies authentication methods for HTTP servers.
ip https authentication *method1* [*method2*.]	Specifies authentication methods for HTTPS servers.
show authentication methods	Displays information about the authentication methods.

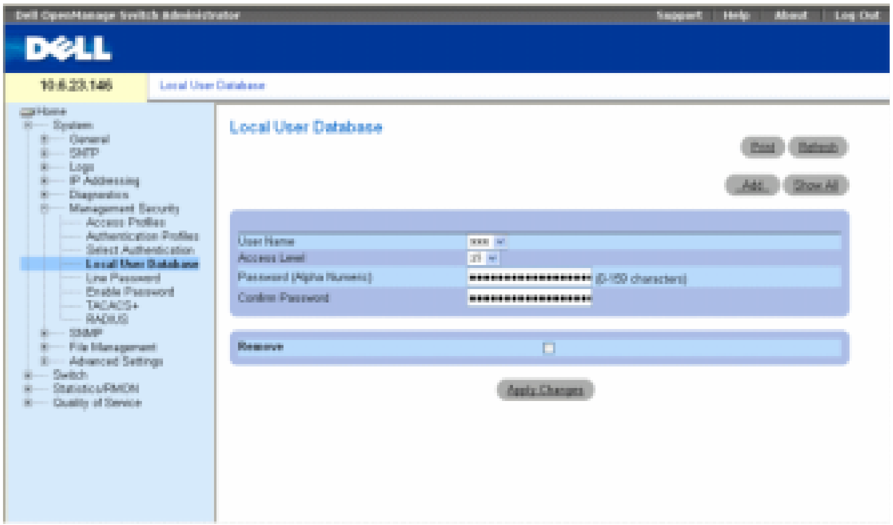
The following is an example of the CLI commands:

```
    Console (config-line)# enable authentication default
    Console (config-line)# login authentication default
    Console (config-line)# exit
    Console (config)# ip http authentication radius local
    Console (config)# ip https authentication radius local
    Console (config)# exit
    Console# show authentication methods
Login Authentication Method Lists
---------------------------------
Default: Radius, Local, Line
Console_Login: Line, None

Enable Authentication Method Lists
----------------------------------
Default: Radius, Enable
Console_Enable: Enable, None



Line    Login Method ListEnable Method List
-------------------------------------------
Console Console_LoginConsole_Enable
TelnetDefaultDefault
SSHDefaultDefault

HTTP: Radius, local
HTTPS: Radius, local
Dot1x: Radius
```

Defining the Local User Databases

The **Local User Database** page contains fields for defining users, passwords and access levels. To open the **Local User Database** page click **System > Management Security > Local User Database** in the tree view.

Figure 6-59. Local User Database



Local User Database

User Name	xxx
Access Level	15
Password (Alpha Numeric)	****************** (0-159 characters)
Confirm Password	******************
Remove	□

User Name — List of users.

Access Level — User access level. The lowest user access level is **1**, and the highest user access level is **15**.

Password (0-159 Characters) — User-defined password. Local user database passwords can have a maximum of 159 characters.

Confirm Password — Confirms the user-defined password.

Remove — When selected, removes users from the **User Name** list.

Assigning Access Rights to a User:

1. Open the **Local User Database** page.
2. Select a user in the **User Name** field.
3. Define the fields.
4. Click **Apply Changes**.

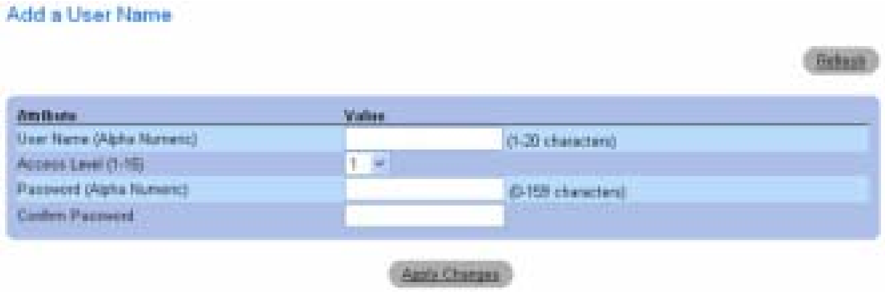
   The user access rights and passwords are defined, and the device is updated.

Defining a New User:

1. Open the **Local User Database** page.
2. Click **Add**.

   The **Add User** page opens:

Figure 6-60. Add User



Add a User Name

Attribute	Value	
User Name (Alpha Numeric)		(1-20 characters)
Access Level (1-15)	1	
Password (Alpha Numeric)		(0-159 characters)
Confirm Password		

3. Define the fields.
4. Click **Apply Changes**.

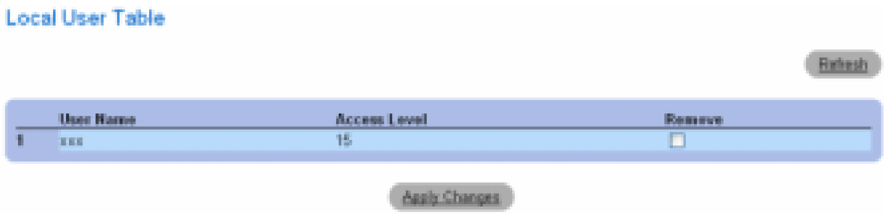
   The new user is defined, and the device is updated.

Displaying the Local User Table:

1. Open the **Local User Database** page.
2. Click **Show All**.

   The **Local User Table** opens:

Figure 6-61. Local User Table Page



Local User Table

	User Name	Access Level	Remove
1	xxx	15	□

Deleting Users:

1. Open the **Local User Database** page.
2. Click **Show All**.

   The **Local User Table** opens.

3 Select a **User Name.**

4 Select the **Remove** check box.

5 Click **Apply Changes**.

The selected user is deleted, and the device is updated.

Assigning Users Using CLI Commands

The following table summarizes the equivalent CLI commands for setting fields displayed in the **Local User Database** page.

Table 6-38. Local User Database CLI Commands

CLI Command	Description
username *name* [**password** *password*] [**level** *level*] [**encrypted**]	Establishes a username-based authentication system.

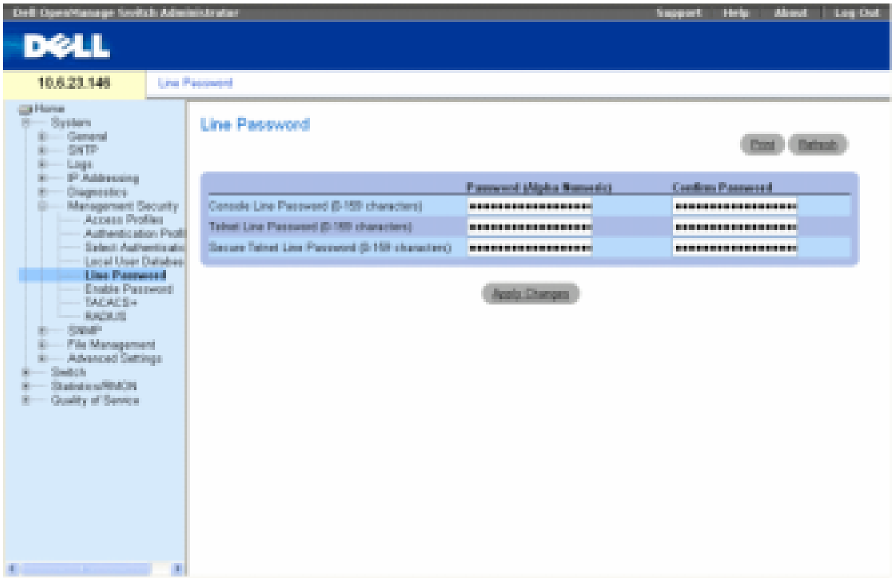
The following is an example of the CLI commands:

```
Console (config)# username bob password lee level 15
```

Defining Line Passwords

The **Line Password** page contains fields for defining line passwords for management methods. To open the **Line Password** page, click **System →Management Security→Line Passwords** in the tree view.

Figure 6-62. Line Password



	Password (Alpha Numeric)	Confirm Password
Console Line Password (0-159 characters)	********************	********************
Telnet Line Password (0-159 characters)	********************	********************
Secure Telnet Line Password (0-159 characters)	********************	********************

Line Password for Console/Telnet/Secure Telnet (0-159 Characters) — The line password for accessing the device via a console, Telnet, or Secure Telnet session. Passwords can contain a maximum of 159 characters.

Confirm Password — Confirms the new line password. The password appears in the ***** format.

Defining Line Passwords for Console Sessions

1. Open the **Line Password** page
2. Define the **Line Password for Console** field.
3. Click **Apply Changes**.

   The line password for console sessions is defined, and the device is updated.

Defining Line Passwords for Telnet Sessions

1. Open the **Line Password** page.
2. Define the **Line Password for Telnet** field.
3. Click **Apply Changes**.

The line password for the Telnet sessions is defined, and the device is updated.

Defining Line Passwords for Secure Telnet Sessions

1 Open the **Line Password** page.

2 Define the **Line Password for Secure Telnet** field.

3 Click **Apply Changes**.

The line password for Secure Telnet sessions is defined, and the device is updated.

Assigning Line Passwords Using CLI Commands

The following table summarizes the equivalent CLI commands for setting fields displayed in the **Line Password** page.

Table 6-39. Line Password CLI Commands

CLI Command	Description
password *password* [**encrypted**]	Specifies a password on a line.

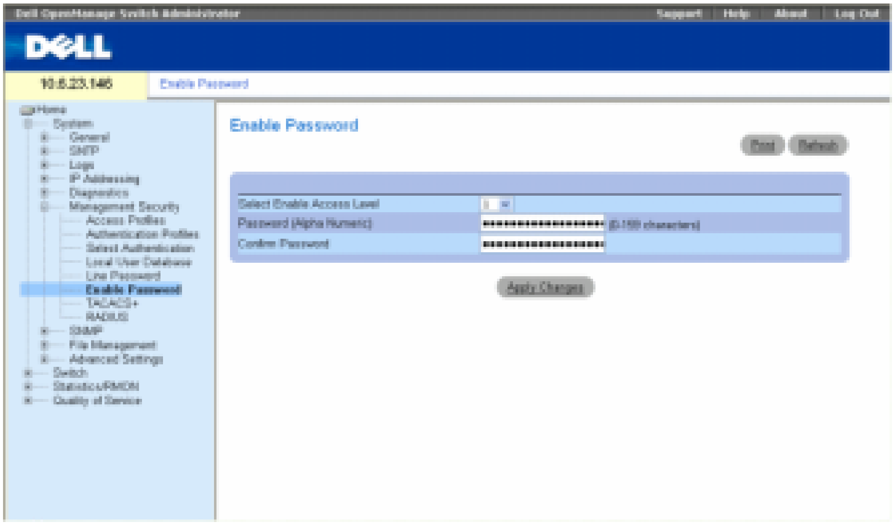
The following is an example of the CLI commands:

```
Console (config-line)# password dell
```

Defining Enable Password

The **Modify Enable Password** page sets a local password to control access to Normal, Privilege, and Global Configuration. To open the **Modify Enable Password** page, click **System →Management Security →Enable Passwords** in the tree view.

Figure 6-63. Modify Enable Password



Enable Password

Select Enable Access Level

Password (Alpha Numeric) ****************** (0-159 characters)

Confirm Password ******************

Select Enable Access Level — Access level associated with the enable password. Possible field values are 1-15.

Password (0-159 Characters) — The currently configured enable password. Enable passwords can contain a maximum of 159 characters.

Confirm Password — Confirms the new enable password. The password appears in the ***** format.

Defining a New Enable Password:

1. Open the **Modify Enable Password** page.
2. Define the **relevant** fields.
3. Click **Apply Changes**.

   The new Enable password is defined, and the device is updated.

Assigning Enable Passwords Using CLI Commands

The following table summarizes the equivalent CLI commands for setting fields displayed in the **Modify Enable Password** page.

Table 6-40. Modify Enable Password CLI Commands

CLI Command	Description
enable password [**level** *level*] *password* [**encrypted**]	Sets a local password to control access to user and privilege levels.
show users accounts	Displays information about the local user database.

The following is an example of the CLI commands:

```
Console (config)# enable password level 15 secret

Console# show users accounts

Username      Privilege

---------     ---------

secret        15
```

Defining TACACS+ Settings

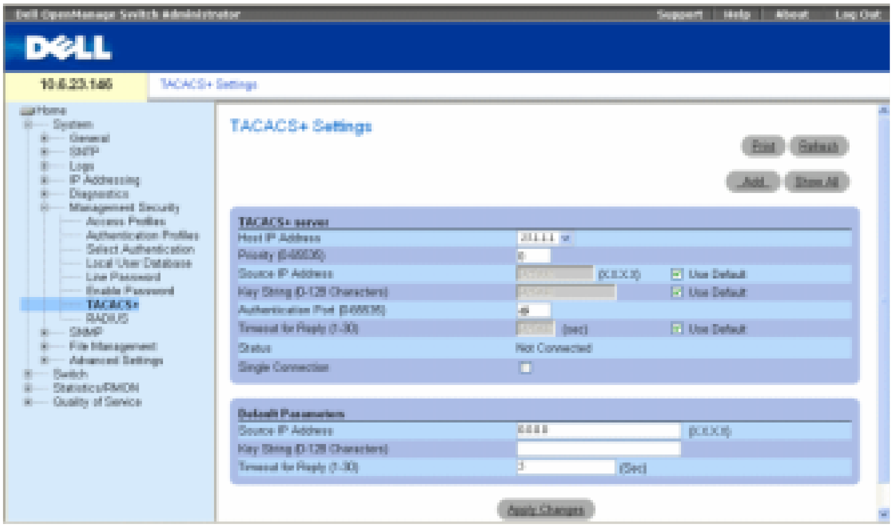
The devices provide Terminal Access Controller Access Control System (TACACS+) client support. TACACS+ provides centralized security for validation of users accessing the device.

TACACS+ provides a centralized user management system, while still retaining consistency with RADIUS and other authentication processes. TACACS+ provides the following services:

- **Authentication** — Provides authentication during login and via user names and user-defined passwords.
- **Authorization** — Performed at login. Once the authentication session is completed, an authorization session starts using the authenticated user name. The TACACS server checks the user privileges.

The TACACS+ protocol ensures network integrity through encrypted protocol exchanges between the device and TACACS+ server. To open the **TACACS+ Settings** page, click **System→ Management Security→TACACS+** in the tree view.

Figure 6-64. TACACS+ Settings



TACACS+ Settings

TACACS+ server			
Host IP Address	2.1.1.1		
Priority (0-65535)	0		
Source IP Address		(X.X.X.X)	☑ Use Default
Key String (0-128 Characters)			☑ Use Default
Authentication Port (0-65535)	49		
Timeout for Reply (1-30)		(sec)	☑ Use Default
Status	Not Connected		
Single Connection	□		

Default Parameters		
Source IP Address	0.0.0.0	(X.X.X.X)
Key String (0-128 Characters)		
Timeout for Reply (1-30)	3	(Sec)

Host IP Address — Specifies the TACACS+ Server IP address.

Priority (0-65535) — Specifies the order in which the TACACS+ servers are used. The default is 0.

Source IP Address — The device source IP address used for the TACACS+ session between the device and the TACACS+ server.

Key String (0-128 Characters) — Defines the authentication and encryption key for TACACS+ communications between the device and the TACACS+ server. This key must match the encryption used on the TACACS+ server.

Authentication Port (0-65535) — The port number through which the TACACS+ session occurs. The default is port 49.

Reply Timeout (1-30) (Sec) — The amount of time that passes before the connection between the device and the TACACS+ server times out. The field range is 1-30 seconds.

Status — The connection status between the device and the TACACS+ server. The possible field values are:

> **Connected** — There is currently a connection between the device and the TACACS+ server.
>
> **Not Connected** — There is not currently a connection between the device and the TACACS+ server.

Single Connection — Maintains a single open connection between the device and the TACACS+ server when selected

The TACACS+ default parameters are user-defined defaults. The default settings are applied to newly defined TACACS+ servers. If default values are not defined, the system defaults are applied to the new TACACS+ new servers. The following are the TACACS+ defaults:

Source IP Address — The default device source IP address used for the TACACS+ session between the device and the TACACS+ server.

Key String (0-128 Characters) — The default authentication and encryption key for TACACS+ communication between the device and the TACACS+ server.

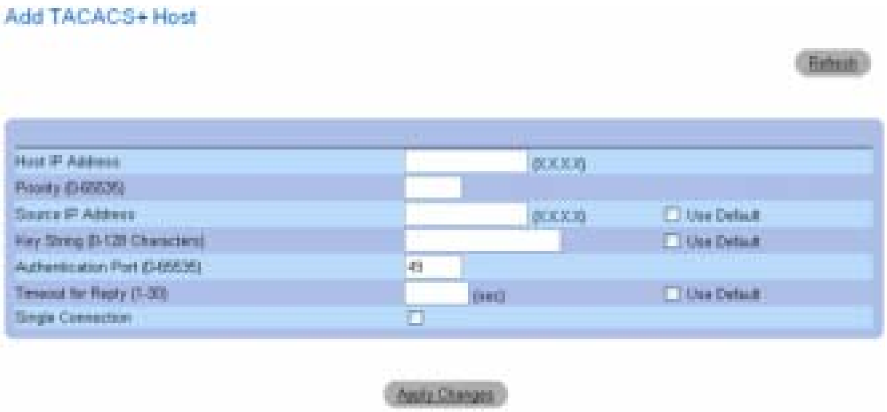
Timeout for Reply (1-30) — The default time that passes before the connection between the device and the TACACS+ times out.

Adding a TACACS+ Server

1. Open the **TACACS+ Settings** page.
2. Click **Add.**

   The **Add TACACS+ Host** page opens:

Figure 6-65. Add TACACS+ Host



Host IP Address	(X.X.X.X)		
Priority (0-65535)			
Source IP Address	(X.X.X.X)	□ Use Default	
Key String (0-128 Characters)		□ Use Default	
Authentication Port (0-65535)	49		
Timeout for Reply (1-30)	(sec)	□ Use Default	
Single Connection	□		

3. Define the fields.
4. Click **Apply Changes**.

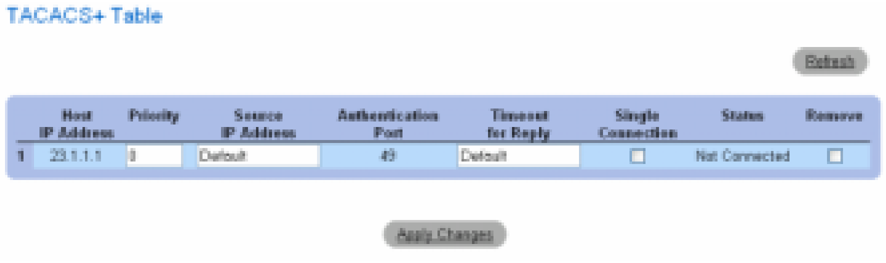
   The TACACS+ server is added, and the device is updated.

Displaying the TACACS+ Table

1. Open the **TACACS+ Settings** page.
2. Click **Show All**.

   The **TACACS+ Table** opens:

Figure 6-66. TACACS+ Table



TACACS+ Table

	Host IP Address	Priority	Source IP Address	Authentication Port	Timeout for Reply	Single Connection	Status	Remove
1	23.1.1.1	0	Default	49	Default	□	Not Connected	□

Removing a TACACS+ Server

1. Open the **TACACS+ Settings** page.
2. Click **Show All**.

   The **TACACS+ Table** opens.
3. Select a **TACACS+ Table** entry.
4. Select the **Remove** check box.
5. Click **Apply Changes**.

   The TACACS+ server is removed, and the device is updated.

Defining TACACS+ Settings Using CLI Commands

The following table summarizes the equivalent CLI commands for setting fields displayed in the **TACACS+ Settings** page.

Table 6-41. TACACS+ CLI Commands

CLI Command	Description
TACACS-server host (*ip-address* | *hostname*) [**single-connection**] [**port** *port-number*] [**timeout** *timeout*] [**key** *key-string*] [**source** *source*] [**priority** *priority*]	Specifies a TACACS+ host.
no TACACS-server host (*ip-address* | *hostname*)	Deletes a TACACS+ host.
tacacs-server key *key-string*	Specifies the authentication and encryption key for all TACACS+ communications between the device and the TACACS+ server. This key must match the encryption used on the TACACS+ daemon. (Range: 0 - 128 characters.)
tacacs-server timeout *timeout*	Specifies the timeout value in seconds. (Range: 1 - 30.)

Table 6-41. TACACS+ CLI Commands

CLI Command	Description
tacacs-server source-ip *source*	Specifies the source IP address. (Range: Valid IP Address.)
show TACACS [*ip-address*]	Displays configuration and statistics for a TACACS+ server.

The following is an example of the CLI commands:

```
Console# show tacacs
Router Configuration


-----------  ---------  -----  ----------  ----------  ---------  ---------


IP address   Status     Port   Single      TimeOut     Source IP  Priority
                               Connection
-----------  ---------  -----  ----------  ----------  ---------  ---------
12.1.1.2     Not        49     Yes         1           12.1.1.1   1
             Connected

Global values
-----------------


TimeOut : 5
Router Configuration
-----------------
Source IP : 0.0.0.0
console#
```

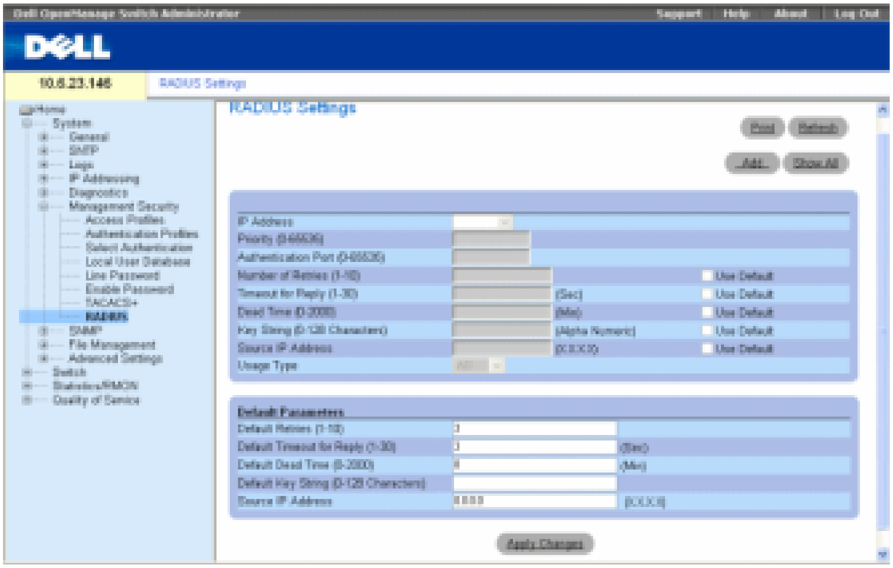
Configuring RADIUS Global Parameters

Remote Authorization Dial-In User Service (RADIUS) servers provide additional security for networks. RADIUS servers provide a centralized authentication method for:

- Telnet Access
- Web Access
- Console to Device Access

To open the **RADIUS Settings** page, click **System →Management Security →RADIUS** in the tree view.

Figure 6-67. RADIUS Settings



RADIUS Settings

IP Address			
Priority (0-65535)			
Authentication Port (0-65535)			
Number of Retries (1-10)			□ Use Default
Timeout for Reply (1-30)		(Sec)	□ Use Default
Dead Time (0-2000)		(Min)	□ Use Default
Key String (0-128 Characters)		(Alpha Numeric)	□ Use Default
Source IP Address		(X.X.X.X)	□ Use Default
Usage Type	All		

Default Parameters

Default Retries (1-10)	3	
Default Timeout for Reply (1-30)	3	(Sec)
Default Dead Time (0-2000)	0	(Min)
Default Key String (0-128 Characters)		
Source IP Address	0.0.0.0	(X.X.X.X)

IP Address — The list of Authentication Server IP addresses.

Priority (1-65535) — Specifies the server priority. The possible values are 1-65535, where 1 is the highest value. This is used to configure the order in which servers are queried.

Authentication Port — Identifies the authentication port. The authentication port is used to verify the RADIUS server authentication.

Number of Retries (1-10) — Specifies the number of transmitted requests sent to RADIUS server before a failure occurs. The possible field values are 1 - 10. Three is the default value.

Timeout for Reply (1-30) — Specifies the amount of the time in seconds the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server. The possible field values are 1 - 30. The default is 3.

Dead Time (0-2000) — Specifies the amount of time (in seconds) that a RADIUS server is bypassed for service requests. The range is 0-2000.

Key String (1-128 Characters) — Specifies the Key string used for authenticating and encrypting all RADIUS communications between the device and the RADIUS server. This key is encrypted.

Source IP Address — Specifies the source IP address that is used for communication with RADIUS servers.

The following fields set the RADIUS default values:

Default Timeout for Reply (1-30) — Specifies the default amount of the time (in seconds) the device waits for an answer from the RADIUS server before timing out.

NOTE: If host-specific Timeouts, Retries, or Dead time values are not specified, the Global values (Defaults) are applied to each host.

Default Retries (1-10) — Specifies the default number of transmitted requests sent to RADIUS server before a failure occurs.

Default Dead time (0-2000) — Specifies the default amount of time (in seconds) that a RADIUS server is bypassed for service requests. The range is 0-2000.

Default Key String (1-128 Characters) — Specifies the Default Key string used for authenticating and encrypting all RADIUS communications between the device and the RADIUS server. This key is encrypted.

Source IP Address — Specifies the source IP address that is used for communication with RADIUS servers.

Usage Type — Specifies the server usage type. Can be one of the following values: **login**, **802.1x** or **all**. If unspecified, defaults to **all**.

Defining RADIUS Parameters:

1 Open the **RADIUS Settings** page.

2 Define the fields.

3 Click **Apply Changes**.

The RADIUS setting are updated to the device.

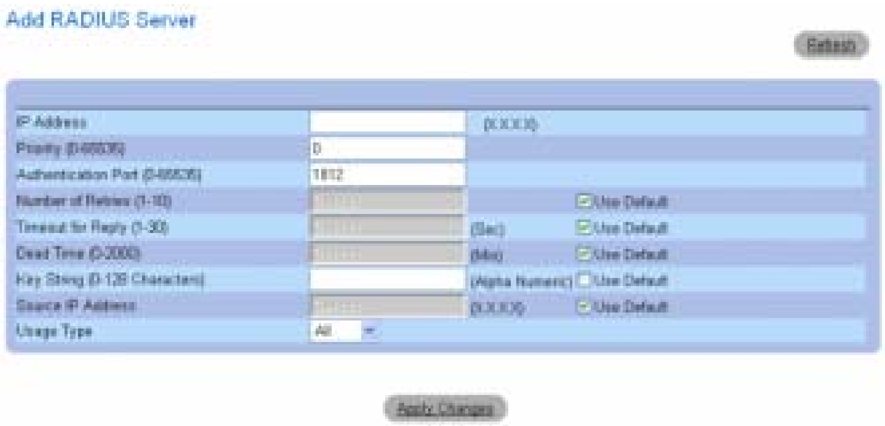
Adding a RADIUS Server:

1 Open the **RADIUS Settings** page.

2 Click **Add**.

The **Add RADIUS Server** page opens:

Figure 6-68. Add RADIUS Server Page



IP Address		(X.X.X.X)	
Priority (0-65535)	0		
Authentication Port (0-65535)	1812		
Number of Retries (1-10)			☑ Use Default
Timeout for Reply (1-30)		(Sec)	☑ Use Default
Dead Time (0-2000)		(Min)	☑ Use Default
Key String (0-128 Characters)		(Alpha Numeric)	□ Use Default
Source IP Address		(X.X.X.X)	☑ Use Default
Usage Type	All		

3 Define the fields.

4 Click **Apply Changes**.

The new RADIUS server is added, and the device is updated.

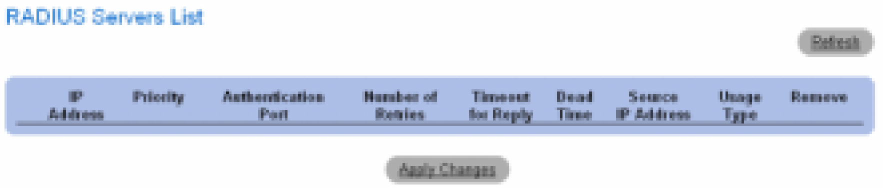
Displaying the RADIUS Server List:

1 Open the **RADIUS Settings** page.

2 Click **Show All**.

The **Show all RADIUS Servers** page opens:

Figure 6-69. Show all RADIUS Servers



IP Address	Priority	Authentication Port	Number of Retries	Timeout for Reply	Dead Time	Source IP Address	Usage Type	Remove

Modifying the RADIUS Server Settings:

1 Open the **RADIUS Settings** page.

2 Click **Show All**.

The **RADIUS Servers List** page opens.

3 Modify the relevant fields.

4 Click **Apply Changes**.

The RADIUS Server settings are modified, and the device is updated.

Deleting a RADIUS Server for the RADIUS Servers List:

1. Open the **RADIUS Settings** page.
2. Click **Show All**.

   The **RADIUS Servers List** page opens.
3. Select a RADIUS Server in the **RADIUS Servers List**.
4. Select the **Remove** check box.
5. Click **Apply Changes**.

   The RADIUS server is removed from the **RADIUS Servers List**.

Defining RADIUS Servers Using CLI Commands

The following table summarizes the equivalent CLI commands for setting fields displayed in the **RADIUS Settings** page.

Table 6-42. RADIUS Settings CLI Commands

CLI Command	Description
radius-server timeout *timeout*	Sets the default interval for which a device waits for a server host to reply.
radius-server retransmit *retries*	Specifies the default number of times the software searches the list of RADIUS server hosts.
radius-server deadtime *deadtime*	Configures unavailable default servers to be skipped.
radius-server key [*key-string*]	Sets the default authentication and encryption key for all RADIUS communications between the device and the RADIUS environment.
radius-server host {*ip-address* | *hostname*} [**auth-port** *auth-port-number*] [**timeout** *timeout*] [**retransmit** *retries*] [**deadtime** *deadtime*] [**key** *key-string*] [**source** *source*] [**priority** *priority*] [**usage** *type*]	Specifies a RADIUS server host and any non-default settings.
show radius-servers	Displays the RADIUS server settings.

The following is an example of the CLI commands:

```
Console (config)# radius-server timeout 5

Console (config)# radius-server retransmit 5

Console (config)# radius-server deadtime 10

Console (config)# radius-server key dell-server

Console (config)# radius-server host 196.210.100.1 auth-port
1645 timeout 20
```

```
Console# show radius-servers
             Port
IP address  Auth   Acct   TimeOut   Retransmit   Deadtime  Source    Priority   Usage
                                                           IP
---------   ----   ----   -------   ----------   -------   -----     -------    -----


33.1.1.1    1812   1813   6         4            10        0.0.0.0   0          All
172.16.1.2  1645   1646   11        8            Global    Global    2          All
Global values
--------------
TimeOut: 5
Retransmit: 5
Deadtime: 10
Source IP: 0.0.0.0
```

Defining SNMP Parameters

Simple Network Management Protocol (SNMP) provides a method for managing network devices. Devices supporting SNMP run a local software (agent).

The SNMP agents maintain a list of variables, which are used to manage the device. The variables are defined in the Management Information Base (MIB). The MIB contains the variables controlled by the agent. The SNMP protocol defines the MIB specification format, as well as the format used to access the information over the network.

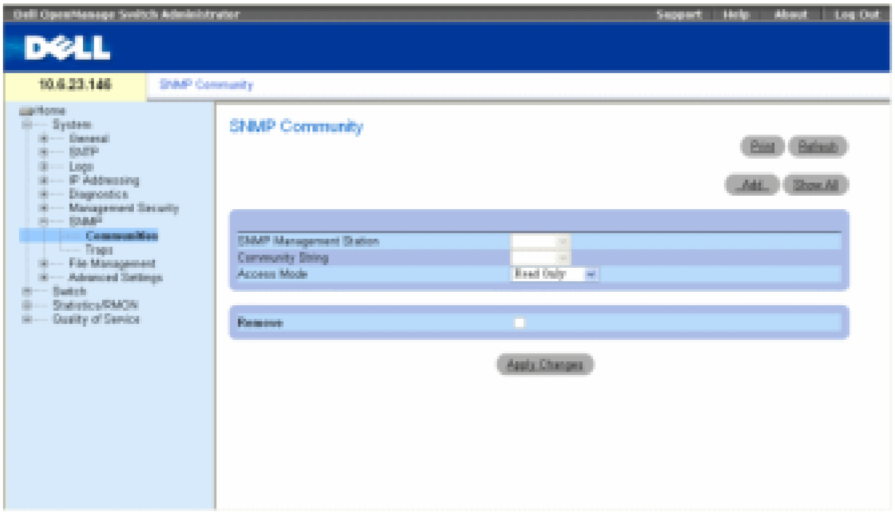
Access rights to the SNMP agents are controlled by access strings. To communicate with the device, the Embedded Web Server submits a valid community string for authentication. To open the SNMP page, click **System →SNMP** in the tree view.

This section contains information for managing the SNMP configuration.

Defining Communities

Access rights are managed by defining communities in the **Community Table**. When the community names are changed, access rights are also changed. To open the **SNMP Community** page, click **System →SNMP →Communities** in the tree view.

Figure 6-70. SNMP Community



SNMP Community

SNMP Management Station	
Community String	
Access Mode	Read Only

Remove	□

SNMP Management Station — A list of management station IP addresses.

Community String — Functions as a password and used to authenticate the selected management station to the device.

Access Mode — Defines the access rights of the community. The possible field values are:

> **Read Only** — The management access is restricted to read-only, for all MIBs except the community table, for which there is no access.
>
> **Read Write** — The management access is read-write, for all MIBs except the community table, for which there is no access.
>
> **SNMP Admin** — The management access is read-write for all MIBs, including the community table.

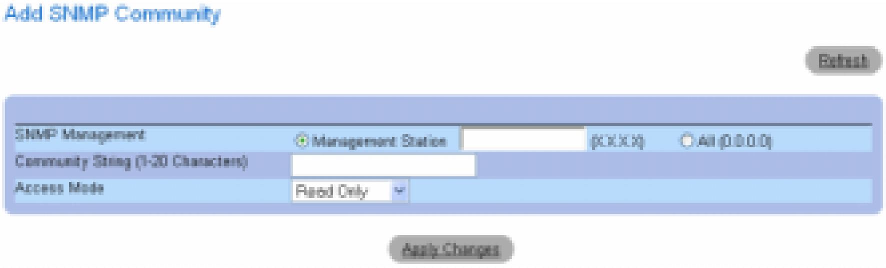
Remove — Removes a community, when selected.

Defining a New Community

1. Open the **SNMP Community** page.
2. Click **Add**.

   The **Add SNMP Community** page opens:

Figure 6-71. Add SNMP Community



Add SNMP Community

SNMP Management	● Management Station		(X.X.X.X)	○ All (0.0.0.0)
Community String (1-20 Characters)				
Access Mode	Read Only			

3. Select one of the following:

   Management Station — Defines an SNMP community for a specific management station. (A value of 0.0.0.0 specifies all management stations.)

   All — Defines an SNMP community for all management stations.

4. Define the remaining fields.
5. Click **Apply Changes**.

   The new community is saved, and the device is updated.

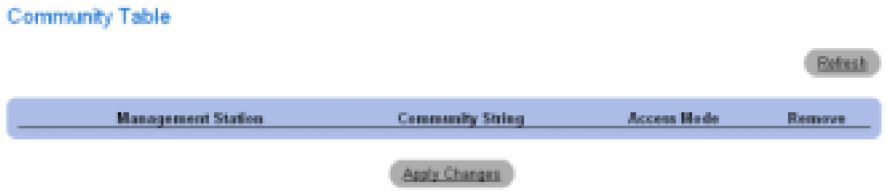
Displaying all Communities

1 Open the **SNMP Community** page.

2 Click **Show All.**

The **Community Table** opens:

Figure 6-72. Community Table



Management Station	Community String	Access Mode	Remove

Deleting Communities

1 Open the **SNMP Community** page.

2 Click **Show All.**

The **Community Table** opens.

3 Select a community from the **Community Table.**

4 Select the **Remove** check box.

5 Click **Apply Changes**.

The selected community entry is deleted, and the device is updated.

Configuring Communities Using CLI Commands

The following table summarizes the equivalent CLI commands for setting fields displayed in the **SNMP Community** page.

Table 6-43. SNMP Community CLI Commands

CLI Command	Description
snmp-server community *string* [**ro** | **rw** | **su**] [*ip-address*]	Sets up the community access string to permit access to SNMP protocol.
snmp-server host {*ip-address* | *hostname*} *community-string* [**1** | **2**]	Determines the trap type sent to the selected recipient.
show snmp	Checks the SNMP communications status.

The following is an example of the CLI commands:

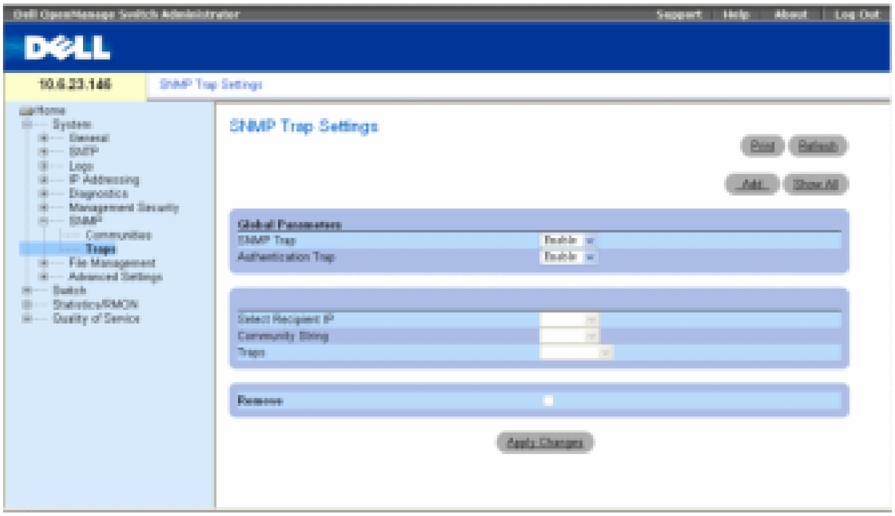
```
console(config)# snmp-server community public_1 su 1.1.1.1
console(config)# snmp-server community public_2 rw 2.2.2.2
console(config)# snmp-server community public_3 ro 3.3.3.3
console(config)# snmp-server host 1.1.1.1 public_1 1
console(config)# snmp-server host 2.2.2.2 public_2 2
console(config)#

console# show snmp

Community-String      Community-Access     IP address
-------------------------------------
public_1              super                1.1.1.1
public_2              readwrite            2.2.2.2
public_3              readonly             3.3.3.3

Traps are enabled.
Authentication-failure trap is enabled.

Trap-Rec-Address      Trap-Rec-Community   Version
```

```
-----------------     -------------------   ---------
1.1.1.1               public_1              1
2.2.2.2               public_2              2

System Contact: 345 6789
System Location: 1234 5678
console#
```

Defining Traps

From the **SNMP Trap Settings** page, the user can enable or disable the device to send SNMP traps or notifications. To open the **SNMP Trap Settings** page, click **System →SNMP→Traps** in the tree view.

Figure 6-73. SNMP Trap Settings



SNMP Trap Settings

Global Parameters

SNMP Trap: Enable

Authentication Trap: Enable

Select Recipient IP

Community String

Traps

Remove □

SNMP Trap — Enables sending SNMP traps or SNMP notifications from the device to defined trap recipients.

Authentication Trap — Enables sending SNMP traps when authentication failed to define recipients.

Select Recipient IP — Specifies the IP address to whom the traps are sent.

Community String — Identifies the community string of the trap manager.

Traps — Determines the trap type sent to the selected recipient. The possible field values are:

> **SNMP V1** — SNMP Version 1 traps are sent
>
> **SNMP V2c** — SNMP Version 2 traps are sent

Remove — Removes **Trap Manager Table** entries, when selected.

Enabling SNMP traps on the Device

1. Open **SNMP Trap Settings** page.
2. Select **Enable** in the **SNMP Trap** drop-down list.
3. Define the fields.
4. Click **Apply Changes**.

SNMP traps are enabled on the device.

Enabling Authentication Traps on the Device

1. Open the **SNMP Trap Settings** page.
2. Select **Enable** in the **Authentication Trap** drop-down list.
3. Define the fields.
4. Click **Apply Changes**.

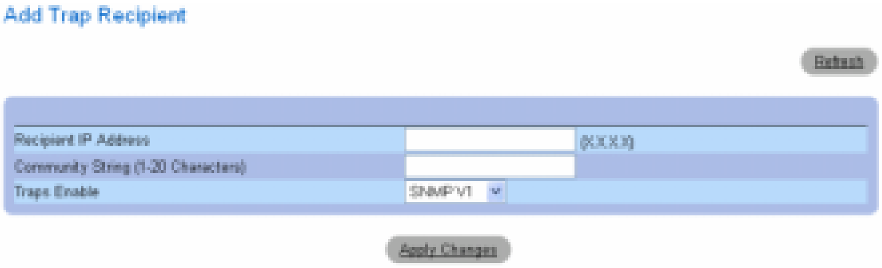
   Authentication traps are enabled on the device.

Adding a New Trap Recipient:

1. Open the **SNMP Trap Settings** page.
2. Click **Add**.

   The **Add Trap Receiver/Manager** page opens:

Figure 6-74. Add Trap Receiver/Manager



Recipient IP Address		(X.X.X.X)
Community String (1-20 Characters)		
Traps Enable	SNMPV1	

3. Define the fields. Configuring 0.0.0.0 means "All", and the traps are broadcast.
4. Click **Apply Changes**.

   The Trap Recipient/Manager is added, and the device is updated.

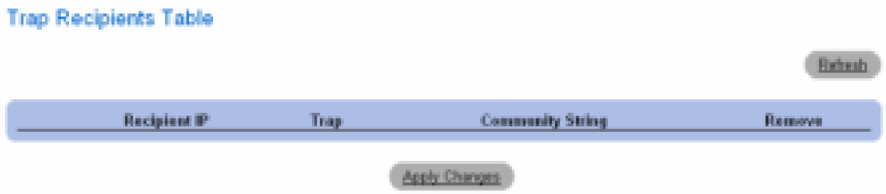
Displaying the Trap Managers Table

The **Trap Managers Table** contains fields for configuring trap types.

1. Open **SNMP Trap Settings** page.
2. Click **Show All.**

   The **Trap Managers Table** page opens:

Figure 6-75. Trap Managers Table



Deleting a Trap Manager Table Entry

1. Open **SNMP Trap Settings** page.
2. Click **Show All.**

   The **Trap Managers Table** page opens.
3. Select a **Trap Managers Table** entry.
4. Select the **Remove** check box.
5. Click **Apply Changes**.

   The selected trap manager is deleted, and the device is updated.

Configuring Traps Using CLI Commands

The following table summarizes the equivalent CLI commands for setting fields displayed in the **SNMP Trap Settings** page.

Table 6-44. SNMP Trap Settings CLI Commands

CLI Command	Description
snmp-server enable traps	Enables the device to send SNMP traps or SNMP notifications.
snmp-server trap authentication	Enables the device to send SNMP traps when authentication failed.
snmp-server host *host-addr community-string* [1 | 2]	Determines the trap type sent to the selected recipient.
show snmp	Displays the SNMP communications status.

The following is an example of the CLI commands:

```
console(config)# snmp-server community public_1 su 1.1.1.1
console(config)# snmp-server community public_2 rw 2.2.2.2
console(config)# snmp-server community public_3 ro 3.3.3.3
console(config)# snmp-server host 1.1.1.1 public_1 1
console(config)# snmp-server host 2.2.2.2 public_2 2
console(config)# snmp-server enable traps
console(config)# snmp-server trap authentication
console(config)#

console# show snmp

Community-String      Community-Access     IP address
------------------------------------
public_1              super                1.1.1.1
public_2              readwrite            2.2.2.2
public_3              readonly             3.3.3.3

Traps are enabled.
Authentication-failure trap is enabled.

Trap-Rec-Address      Trap-Rec-Community   Version
-----------------     ------------------   ---------
1.1.1.1               public_1             1
2.2.2.2               public_2             2

System Contact: 345 6789
System Location: 1234 5678
console#
```

Managing Files

The **File Management** page contains fields for managing device software, the Image Files, and the Configuration Files. Files can be downloaded from a TFTP server.

File Management Overview

The configuration file structure consists of the following configuration files:

- **Startup Configuration File** — Contains the commands required to reconfigure the device to the same settings as when the device is powered down or rebooted. The Startup file is created by copying the configuration commands from the Running Configuration file or the Backup Configuration file.
- **Running Configuration File** — Contains all Startup file commands, as well as all commands entered during the current session. After the device is powered down or rebooted, all commands stored in the Running Configuration file are lost. During the startup process, all commands in the Startup file are copied to the Running Configuration File and applied to the device. During the session, all new commands entered are added to the commands existing in the Running Configuration file. Commands are not overwritten. To update the Startup file, before powering down the device, the Running Configuration file must be copied to the Startup Configuration file. The next time the device is restarted, the commands are copied back into the Running Configuration file from the Startup Configuration file.
- **Backup Configuration File** — Contains a backup copy of the device configuration. The Backup file is generated when the Running Configuration file or the Startup file is copied to the Backup file. The commands copied into the file replaces the existing commands saved in the Backup file. The Backup file contents can be copied to either the Running Configuration or the Startup Configuration files.
- **Image files** — System file images are saved in two Flash Files called images (Image 1 and Image 2). The active image stores the active copy, while the other image stores a second copy. The device boots and runs from the active image. If the active image is corrupted, the system automatically boots from the non-active image. This is a safety feature for faults occurring during the Software Upgrade process.

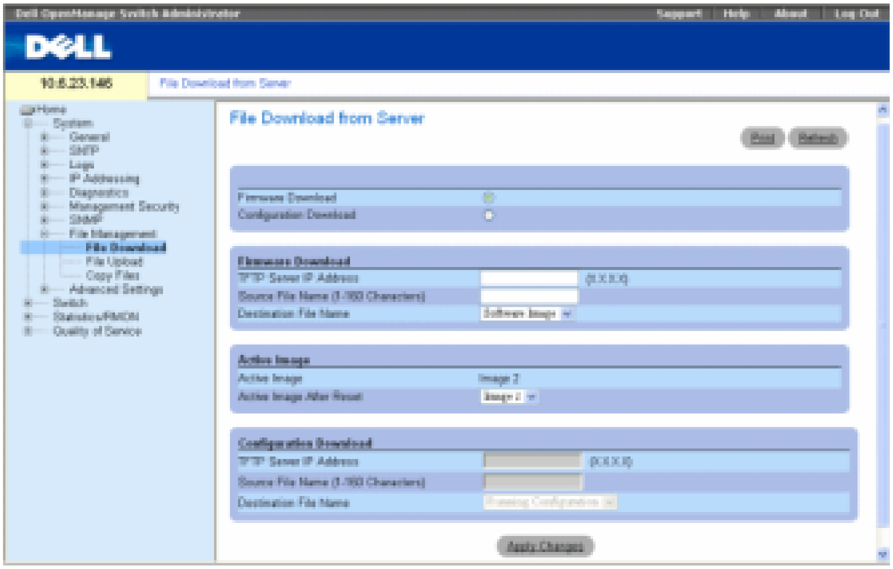
To open the **File Management** page, click **System→File Management** in the tree view. The **File Management** page contains links to:

- File Download
- File Upload
- Copy Files

Downloading Files

The **File Download From Server** page contains fields for downloading system image and Configuration files from the TFTP server to the device. To open the **File Download From Server** page, click **System →File Management→File Download** in the tree view.

Figure 6-76. File Download From Server



File Download from Server

Firmware Download	●
Configuration Download	○

Firmware Download

TFTP Server IP Address	(X.X.X.X)
Source File Name (1-160 Characters)	
Destination File Name	Software Image

Active Image

Active Image	Image 2
Active Image After Reset	Image 2

Configuration Download

TFTP Server IP Address	(X.X.X.X)
Source File Name (1-160 Characters)	
Destination File Name	Running Configuration

Firmware Download — The Firmware file is downloaded. If **Firmware Download** is selected, the **Configuration Download** fields are grayed out.

Configuration Download — The Configuration file is downloaded. If **Configuration Download** is selected, the **Firmware Download** fields are grayed out.

Firmware Download TFTP Server IP Address — The TFTP Server IP Address from which files are downloaded.

Firmware Download Source File Name — Specifies the file to be downloaded.

Firmware Download Destination File — The destination file type to which to the file is downloaded. The possible field values are:

- **Software Image** — Downloads the Image file.
- **Boot Code** — Downloads the Boot file.

Active Image — The Image file that is currently active.

Active Image After Reset — The Image file that is active after the device is reset.

Configuration Download File TFTP Server IP Address — The TFTP Server IP Address from which the configuration files are downloaded.

Configuration Download File Source File Name — Specifies the configuration files to be downloaded.

Configuration Download File Destination — The destination file to which to the configuration file is downloaded. The possible field values are:

> **Running Configuration** — Downloads commands into the Running Configuration file.
>
> **Startup Configuration —** Downloads the Startup Configuration file, and overwrites it.
>
> **Backup Configuration** — Downloads the Backup Configuration file, and overwrites it.

Downloading Files:

1. Open the **File Download From Server** page.
2. Define the file type to download.
3. Define the fields.
4. Click **Apply Changes**.

   The software is downloaded to the device.

NOTE: To activate the selected Image file, reset the device. For information on resetting the device, see "Resetting the Device" .

Downloading Files Using CLI Commands

The following table summarizes the equivalent CLI commands for setting fields displayed in the **File Download From Server** page.

Table 6-45. File Download CLI Commands

CLI Command	Description
copy *source-url destination-url* [**snmp**]	Copies any file from a source to a destination.

The following is an example of the CLI commands:

```
console# copy running-config tftp://11.1.1.2/pp.txt
```

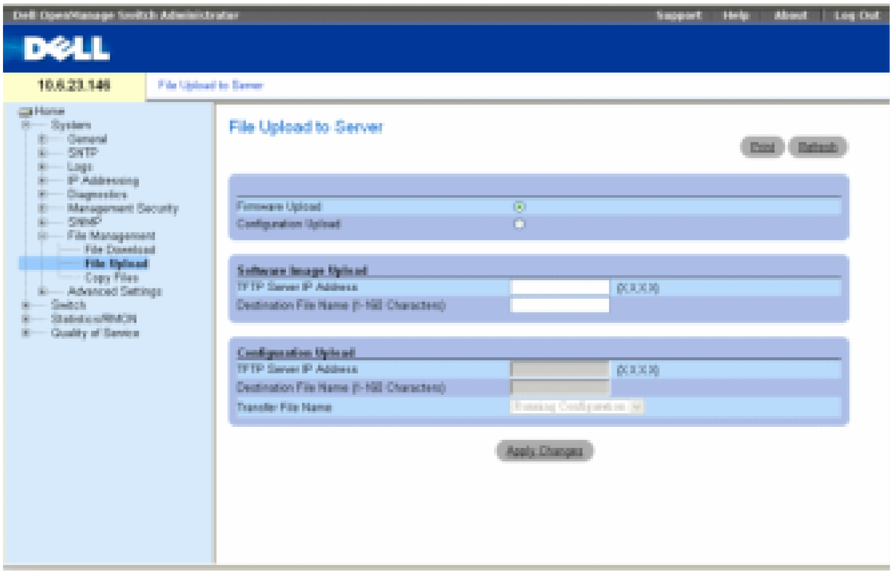
NOTE: Each "!" indicates that ten packets were successfully transferred.

```
Accessing file 'file1' on 172.16.101.101.

Loading file1 from 172.16.101.101:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! [OK]

Copy took 0:01:11 [hh:mm:ss]
```

Uploading Files

The **File Upload to Server** page contains fields for uploading the software from the TFTP server to the device. The Image file can also be uploaded from the **File Upload to Server** page. To open the **File Upload to Server** page, click **System** →**File Management** →**File Upload** in the tree view.

Figure 6-77.   File Upload to Server



File Upload to Server

Firmware Upload	●	
Configuration Upload	○	
Software Image Upload		
TFTP Server IP Address		(X.X.X.X)
Destination File Name (1-160 Characters)		
Configuration Upload		
TFTP Server IP Address		(X.X.X.X)
Destination File Name (1-160 Characters)		
Transfer File Name	Running Configuration	

Firmware Upload — The Firmware file is uploaded. If **Firmware Upload** is selected, the **Configuration Upload** fields are grayed out.

Configuration Upload — The Configuration file is uploaded. If **Configuration Upload** is selected, the **Software Image Upload** fields are grayed out.

Software Image Upload TFTP Server IP Address — The TFTP Server IP Address to which the Software Image is uploaded.

Software Image Upload Destination — Specifies the Software Image file path to which the file is uploaded.

Configuration Upload TFTP Server IP Address — The TFTP Server IP Address to which the Configuration file is uploaded.

Configuration Upload Destination — Specifies the Configuration file path to which the file is uploaded.

Configuration Upload Transfer file name — The software file to which the configuration is uploaded. The possible field values are:

> **Running Configuration** — Uploads the Running Configuration file
>
> **Startup Configuration** — Uploads the Startup Configuration file
>
> **Backup Configuration** — Uploads the Backup Configuration file

Uploading Files

1. Open the **File Upload to Server** page.

2 Define the file type to upload.

3 Define the fields.

4 Click **Apply Changes**.

The software is uploaded to the device.

Uploading Files Using CLI Commands

The following table summarizes the equivalent CLI commands for setting fields displayed in the **File Upload to Server** page.

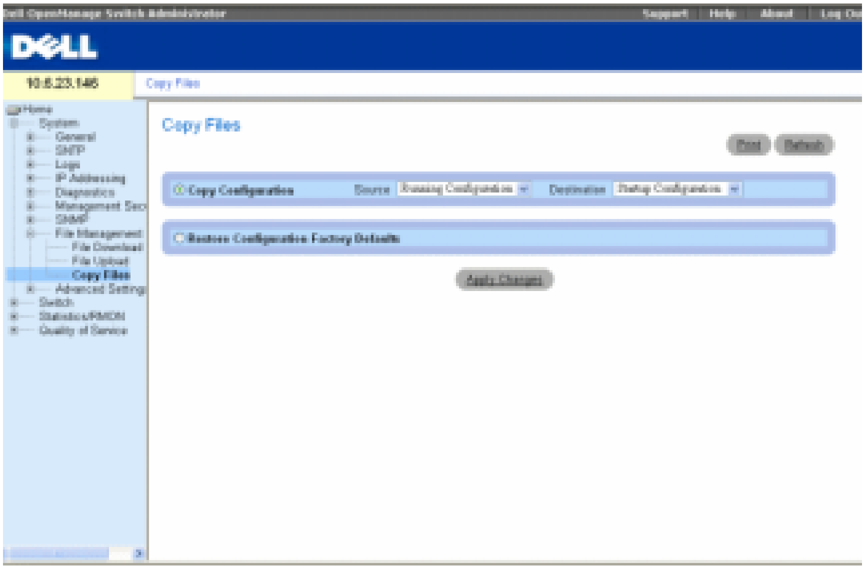
Table 6-46. File Upload CLI Commands

CLI Command	Description
copy *source-url destination-url* [snmp]	Copies any file from a source to a destination.

Copying Files

Files can be copied and deleted from the **Copy Files** page. To open the **Copy Files** page, click **System→File Management→Copy Files** in the tree view.

Figure 6-78. Copy Files



● Copy Configuration Source Running Configuration Destination Startup Configuration

○ Restore Configuration Factory Defaults

Copy Configuration — When selected, copies either the Running Configuration, Startup Configuration or Backup Configuration files. The possible field values are:

Source — Copies either the Running Configuration, Startup Configuration or Backup Configuration files.

Destination — The file to which the Running Configuration, Startup Configuration or Backup Configuration file is copied.

Restore Configuration Factory Defaults — When selected, specifies that the factory configuration default files should be reset. When unselected, maintains the current configuration settings.

Copying Files

1. Open the **Copy Files** page.
2. Define the **Source** and **Destination** fields.
3. Click **Apply Changes**.

   The file is copied, and the device is updated.

Restoring Company Factory Default Settings

1. Open the **Copy Files** page.
2. Click **Restore Company Factory Defaults**.
3. Click **Apply Changes**.

   The company factory default settings are restored, and the device is updated.

Copying and Deleting Files Using CLI Commands

The following table summarizes the equivalent CLI commands for setting fields displayed in the **Copy Files** page.

Table 6-47. Copy Files CLI Commands

CLI Command	Description
copy *source-url destination-url* [snmp]	Copies any file from a source to a destination.
delete startup-config	Deletes the startup-config file.

The following is an example of the CLI commands:

```
Console # copy tftp://172.16.101.101/file1 image

Accessing file 'file1' on 172.16.101.101.

Loading file1 from 172.16.101.101:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!! [OK]

Copy took 0:01:11 [hh:mm:ss]

Console# delete startup-config


Console# copy running-config startup-config

01-Jan-2000 01:55:03 %COPY-W-TRAP: The copy operation was
completed successfully

Copy succeeded
```

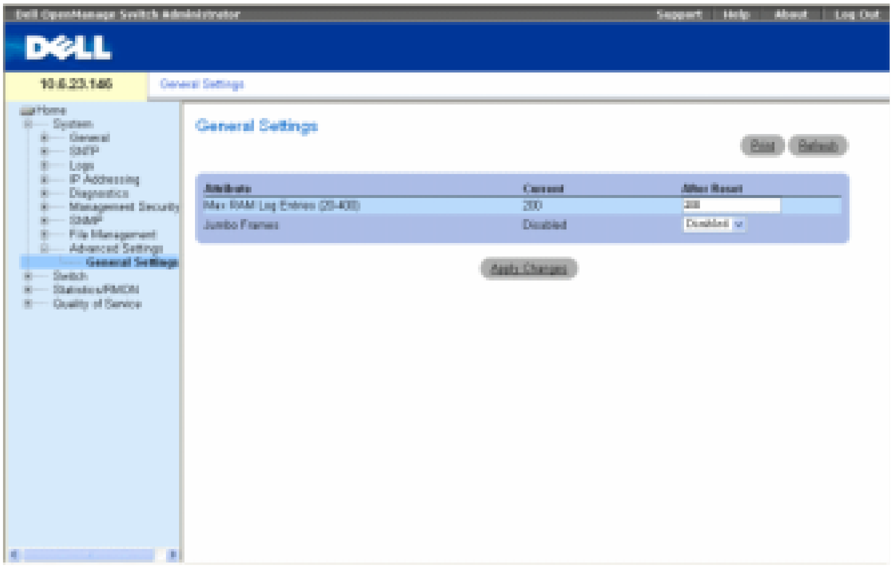
Defining Advanced Settings

The the **Advanced Settings** page contains a link for configuring general settings. Use Advanced Settings to set miscellaneous global attributes for the device. The changes to these attributes are applied only after the device is reset. To open the **Advanced Settings** page, click **System** → **Advanced Settings** in the tree view.

Configuring General Device Tuning Parameters

The **General Settings** page provides information for defining general device parameters. To open the **General Settings** page, click **System**→**Advanced Settings**→**General** in the tree view.

Figure 6-79. General Settings



General Settings

Attribute	Current	After Reset
Max RAM Log Entries (20-400)	200	200
Jumbo Frames	Disabled	Disabled

Attribute — The general setting attribute.

Current — The currently configured value.

After Reset — The future (after reset) value. By entering a value in the After Reset column, memory is allocated to the field table.

Max RAM Log Entries (20-400) — The maximum number of RAM Log entries. When the Log entries are full, the log is cleared and the Log file is restarted.

Jumbo Frames — Enables or disables the Jumbo Frames feature. Jumbo Frames enable the transportation of identical data in fewer frames. This ensures less overhead, lower processing time, and fewer interrupts.

Viewing RAM Log Entries Counter Using the CLI Commands

The following table summarizes the equivalent CLI commands for setting fields displayed in the **General Settings** page.

Table 6-48. General Settings CLI Commands

CLI Command	Description
logging buffered size *number*	Sets the number of syslog messages stored in the internal buffer (RAM).
port jumbo-frame	Enables jumbo frames for the device.

The following is an example of the CLI commands:

```
Console (config)# logging buffered size 300
```

7

Configuring Device Information

This section provides all system operation and general information for configuring network security, ports, Address tables, GARP, VLANs, Spanning Tree, Port Aggregation, and Multicast Support.

Configuring Network Security

The device enables network security through both Access Control Lists and Locked Ports. To open the **Network Security** page select **Switch →Network Security**.

Network Security Overview

This section describes the network security features.

Port Based Authentication (802.1x)

Port based authentication enables authenticating system users on a per-port basis via a external server. Only authenticated and approved system users can transmit and receive data. Ports are authenticated via the RADIUS server using the Extensible Authentication Protocol (EAP). Port Authentication includes:

- **Authenticators** — Specifies the port that is authenticated before permitting system access.
- **Supplicants** — Specifies host connected to the authenticated port requesting to access the system services.
- **Authentication Server** — Specifies the external server, for example, the RADIUS server that performs the authentication on behalf of the authenticator, and indicates whether the user is authorized to access system services.

Port based authentication creates two access states:

- **Controlled Access** — Permits communication between the user and the system, if the user is authorized.
- **Uncontrolled Access** — Permits uncontrolled communication regardless of the port state.

The device currently supports Port Based Authentication via RADIUS servers.

Advanced Port Based Authentication

Advanced Port Based Authentication enables multiple hosts to be attached to a single port. Advanced Port Based Authentication requires only one host to be authorized for all hosts to have system access. If the port is unauthorized all attached hosts are denied access to the network.

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.

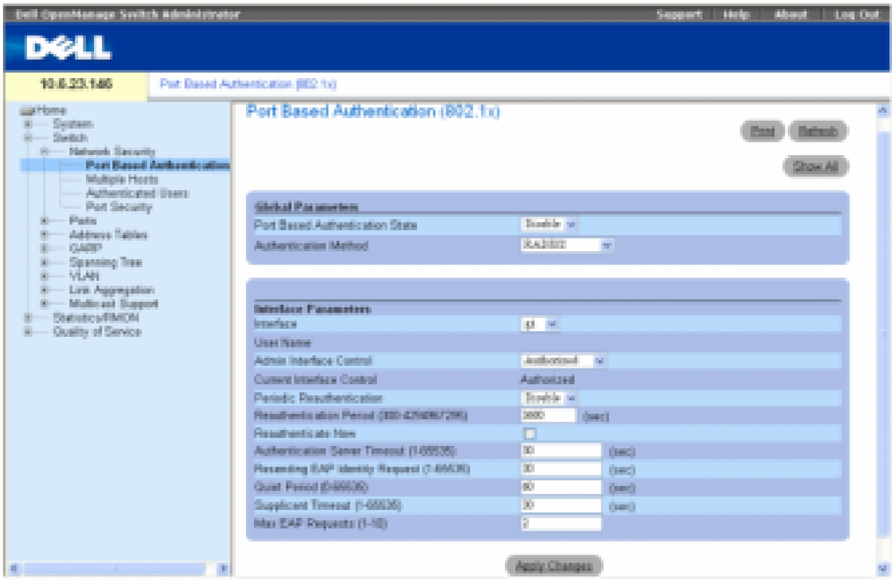
Advanced Port Based Authentication is implemented in the following modes:

- **Single Host Mode** — Enables only the authorized host to access the port.
- **Multiple Host Mode** — Enables multiple hosts to 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 network access.

Configuring Port Based Authentication

The **Port Based Authentication** page contains fields for configuring port based authentication. To open the **Port Based Authentication** page, click **Switch →Network Security →Port Based Authentication**.

Figure 7-80. Port Based Authentication



Port Based Authentication (802.1x)

Global Parameters

Port Based Authentication State	Enable	
Authentication Method	RADIUS	

Interface Parameters

Interface	g1	
User Name		
Admin Interface Control	Authorized	
Current Interface Control	Authorized	
Periodic Reauthentication	Enable	
Reauthentication Period (300-4294967295)	3600	(sec)
Reauthenticate Now	□	
Authentication Server Timeout (1-65535)	30	(sec)
Resending EAP Identity Request (1-65535)	30	(sec)
Quiet Period (0-65535)	60	(sec)
Supplicant Timeout (1-65535)	30	(sec)
Max EAP Requests (1-10)	2	

Port Based Authentication State — Permits port based authentication on the device. The possible field values are:

Enable — Enables port based authentication on the device.

Disable — Disables port based authentication on the device.

Authentication Method — The Authentication method used. The possible field values are:

None — No authentication method is used to authenticate the port.

RADIUS — Port authentication is performed using the RADIUS server.

RADIUS, None — Port authentication is performed first using the RADIUS server. If the port is not authenticated, then no authentication method is used, and the session is permitted.

Interface — Contains an interface list.

User Name — The user name as configured in the RADIUS server.

Admin Interface Control — Defines the port authorization state. The possible field values are:

Authorized — Set the interface state to authorized (permit traffic).

Unauthorized — Set the interface state to unauthorized (deny traffic).

Auto — Authorize state is set by the authorization method.

Current Interface Control — The currently configured port authorization state.

Periodic Reauthentication — Reauthenticates the selected port periodically, when enabled. The reauthentication period is defined in the **Reauthentication Period (300-4294967295)** field.

Reauthentication Period (300-4294967295) — Indicate the time span in which the selected port is reauthenticated. The field value is in seconds. The field default is 3600 seconds.

Reauthenticate Now — Permits immediate port reauthentication, when selected.

Authentication Server Timeout (1-65535) — Defines the amount of time that lapses before the device resends a request to the authentication server. The field value is in seconds. The field default is 30 seconds.

Resending EAP Identity Request (1-65535) — Defines the amount of time that lapses before EAP request are resent. The field default is 30 seconds.

Quiet Period (0-65535) — The number of seconds that the device remains in the quiet state following a failed authentication exchange. The possible field range is 0-65535. The field default is 60 seconds.

Supplicant Timeout (1-65535) — The amount of time that lapses before EAP requests are resent to the user. The field value is in seconds. The field default is 30 seconds.

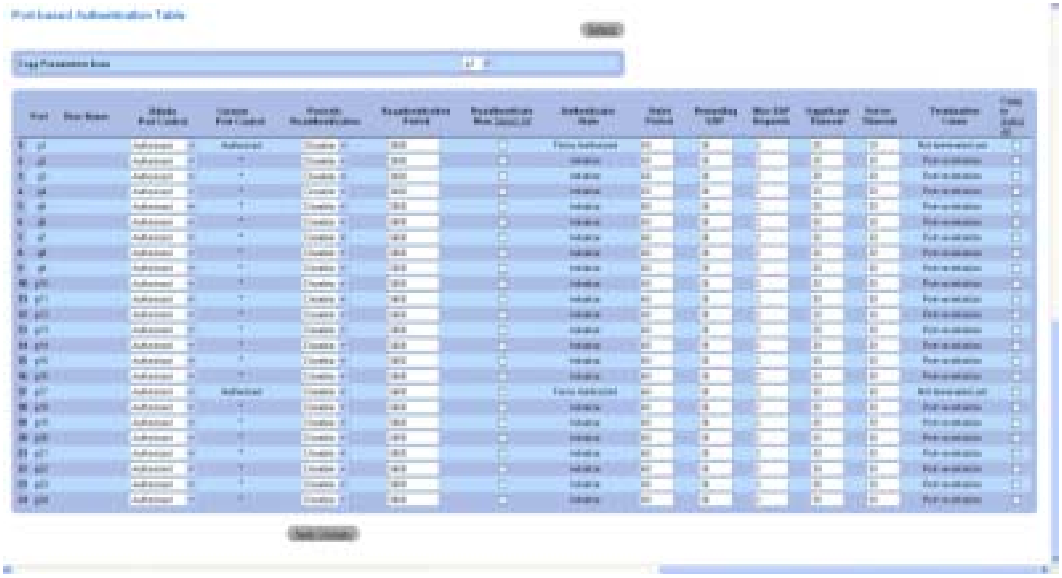
Max EAP Requests (1-10) — The total amount of EAP requests sent. If a response is not received after the defined period, the authentication process is restarted. The field default is 2 retries.

Displaying the Port Based Authentication Table

1. Display the **Port Based Authentication** page.
2. Click **Show All**.

   The **Port Based Authentication Table** opens:

Figure 7-81. Port Based Authentication Table



Termination Cause — The reason for which the port authentication was terminated.

Copy To Checkbox — Copies port parameters from one port to the selected ports.

Select All — Selects all ports in the **Port Based Authentication Table**.

Copying Parameters in the Port Based Authentication Table

1. Open the **Port Based Authentication** page.
2. Click **Show All**.

   The **Port Based Authentication Table** opens.
3. Select the interface in the **Copy Parameters from** field.
4. Select an interface in the **Port Based Authentication Table**.
5. Select the **Copy to** check box to define the interfaces to which the Port based authentication parameters are copied.
6. Click **Apply Changes**.

   The parameters are copied to the selected port in the **Port Based Authentication Table**, and the device is updated.

Enabling Port Based Authentication Using the CLI Commands

The following table summarizes the equivalent CLI commands for enabling the port based authentication as displayed in the **Port Based Authentication** page.

.

Table 7-49. Port Authentication CLI Commands

CLI Command	Description
aaa authentication dot1x default *method1* [*method2*.]	Specifies one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X.
dot1x max-req *count*	Sets the maximum number of times that the device sends an EAP to the client, before restarting the authentication process.
dot1x re-authenticate [**ethernet** *interface*]	Manually initiates a re-authentication of all 802.1X-enabled ports or the specified 802.1X-enabled port.
dot1x re-authentication	Enables periodic re-authentication of the client.
dot1x timeout quiet-period *seconds*	Sets the number of seconds that the device remains in the quiet state following a failed authentication exchange.
dot1x timeout re-authperiod *seconds*	Sets the number of seconds between re-authentication attempts.
dot1x timeout server-timeout *seconds*	Sets the time for the retransmission of packets to the authentication server.
dot1x timeout supp-timeout *seconds*	Sets the time for the retransmission of an EAP request frame to the client.
dot1x timeout tx-period *seconds*	Sets the number of seconds that the device waits for a response to an EAP - request/identity frame, from the client, before resending the request.
show dot1x [**ethernet** *interface*]	Displays 802.1X status for the device or for the specified interface.
show dot1x users [**username** *username*]	Displays 802.1X users for the device.

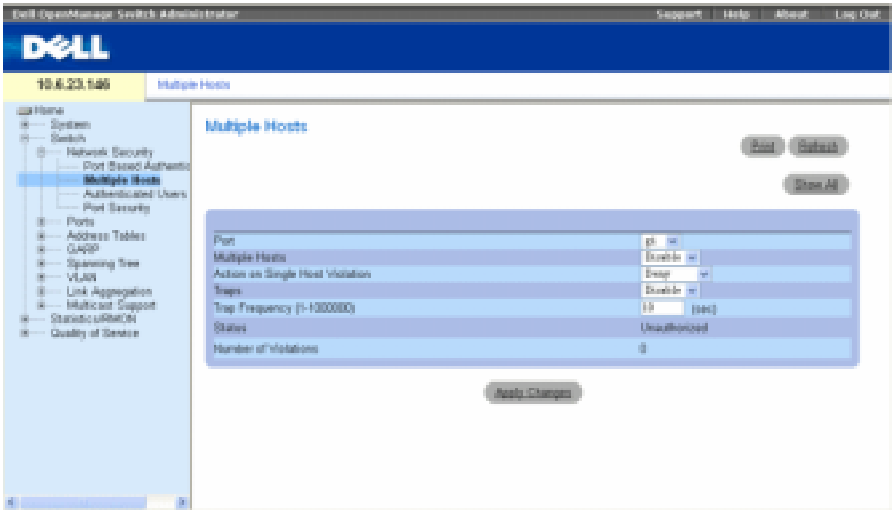
The following is an example of the CLI commands:

```
console> enable
Console# show dot1x

Interface  Admin Mode  Oper Mode     Reauth     Reauth       Username
                                     Control    Period
---------  ----------  ----------    --------   ------       --------
g1         Auto        Authorized    Ena        3600         Bob
g2         Auto        Authorized    Ena        3600         John
g3         Auto        Unauthorized  Ena        3600         Clark
g4         Force-auth  Authorized    Dis        3600         n/a
```

Configuring Advanced Port Based Authentication

The **Multiple Hosts** page provides information for defining advanced port based authentication settings for specific ports. To open the **Multiple Hosts**, click **Switch →Network Security →Multiple Hosts**.

Figure 7-82. Multiple Hosts



Multiple Hosts

Port	g1
Multiple Hosts	Disable
Action on Single Host Violation	Discard
Traps	Disable
Trap Frequency (1-1000000)	10 (sec)
Status	Unauthorized
Number of Violations	0

Port — The port number for which Advanced Port Based Authentication is enabled.

Multiple Hosts — Enables or disables a single host to authorize multiple hosts for system access. This setting must be enabled in order to either disable the ingress-filter, or to use port-lock security on the selected port.

Action on Single Host Violation — Defines the action to be applied to packets arriving in single-host mode, from a host whose MAC address is not the client (supplicant) MAC address. The **Action on Single Host Violation** field can be defined only if the **Multiple Hosts** field is defined as **Disable**. The possible field values are:

> **Permit** — Forwards the packets from an unknown source, however, the MAC address is not learned.
>
> **Deny** — Discards the packets from any unlearned source. This is the default value.
>
> **Shutdown** — Discards the packet from any unlearned source and locks the port. Ports remain locked until they are activated, or the device is reset.

Traps — Enables or disables sending traps to the host if a violation occurs.

Trap Frequency (1-1000000) (Sec) — Defines the time period by which traps are sent to the host. The **Trap Frequency (1-1000000)** field can be defined only if the **Multiple Hosts** field is defined as **Disable**. The default is 10 seconds.

Status — The host status. The possible field values are:

> **Unauthorized** — Clents (supplicants) have full port access.
>
> **Authorized** — Clents (supplicants) have limited port access.
>
> **No single-host** — **Multiple Hosts** is enabled.

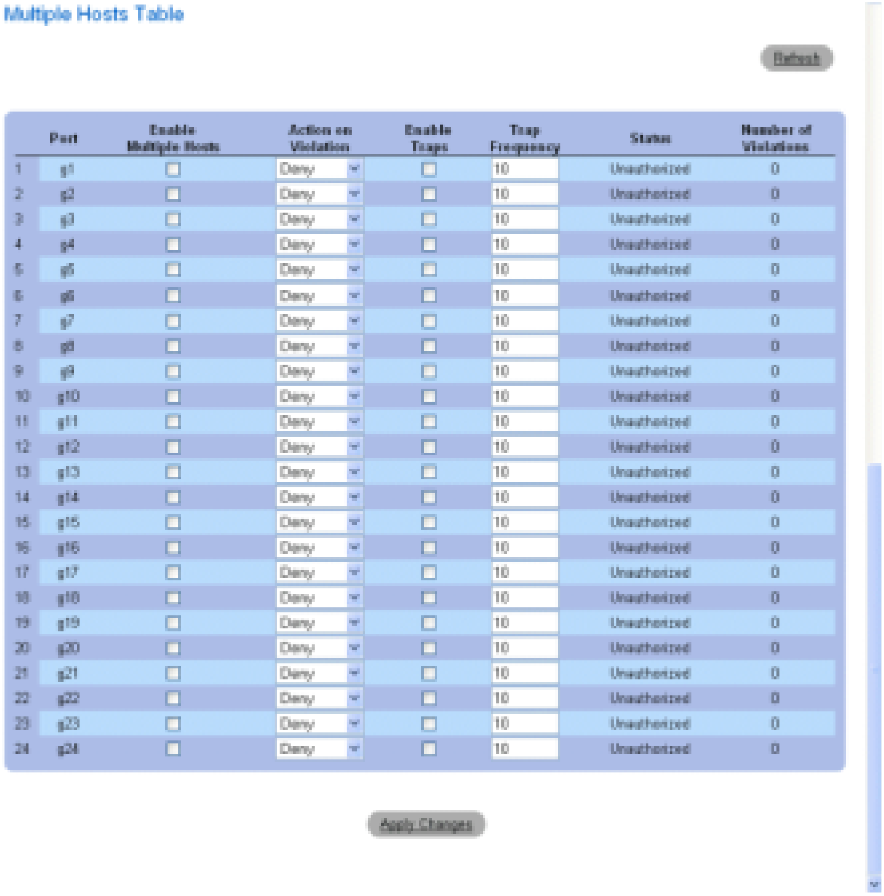
Number of Violations — The number of packets that arrived on the interface in single-host mode, from a host whose MAC address is not the client (supplicant) MAC address.

Displaying the Multiple Hosts Table

1. Open the **Multiple Hosts** page.
2. Click **Show All**.

   The **Multiple Hosts Table** opens:

Figure 7-83. Multiple Hosts Table



Multiple Hosts Table

	Port	Enable Multiple Hosts	Action on Violation	Enable Traps	Trap Frequency	Status	Number of Violations
1	g1	□	Deny	□	10	Unauthorized	0
2	g2	□	Deny	□	10	Unauthorized	0
3	g3	□	Deny	□	10	Unauthorized	0
4	g4	□	Deny	□	10	Unauthorized	0
5	g5	□	Deny	□	10	Unauthorized	0
6	g6	□	Deny	□	10	Unauthorized	0
7	g7	□	Deny	□	10	Unauthorized	0
8	g8	□	Deny	□	10	Unauthorized	0
9	g9	□	Deny	□	10	Unauthorized	0
10	g10	□	Deny	□	10	Unauthorized	0
11	g11	□	Deny	□	10	Unauthorized	0
12	g12	□	Deny	□	10	Unauthorized	0
13	g13	□	Deny	□	10	Unauthorized	0
14	g14	□	Deny	□	10	Unauthorized	0
15	g15	□	Deny	□	10	Unauthorized	0
16	g16	□	Deny	□	10	Unauthorized	0
17	g17	□	Deny	□	10	Unauthorized	0
18	g18	□	Deny	□	10	Unauthorized	0
19	g19	□	Deny	□	10	Unauthorized	0
20	g20	□	Deny	□	10	Unauthorized	0
21	g21	□	Deny	□	10	Unauthorized	0
22	g22	□	Deny	□	10	Unauthorized	0
23	g23	□	Deny	□	10	Unauthorized	0
24	g24	□	Deny	□	10	Unauthorized	0

Enabling Multiple Hosts Using the CLI Commands

The following table summarizes the equivalent CLI commands for enabling the advanced port based authentication as displayed in the **Multiple Hosts** page.

Table 7-50. Multiple Hosts CLI Commands

CLI Command	Description
dot1x multiple-hosts	Allows multiple hosts (clients) on an 802.1X-authorized port that has the dot1x port-control interface configuration command set to auto.
dot1x single-host-violation {**forward** |**discard** |**discard-shutdow**n}[**trap** seconds]	Configures the action to be taken when a station, whose MAC address is not the client (supplicant) MAC address, attempts to access the interface.

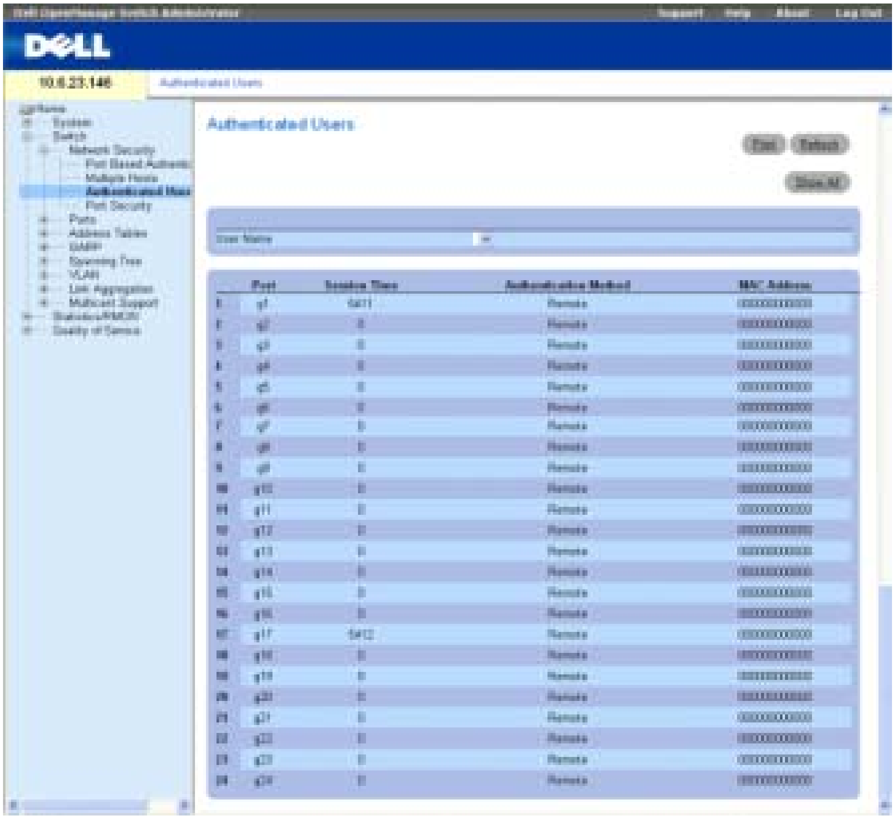
The following is an example of the CLI Command.

```
Neyland# configure
Neyland(config)# interface ethernet g1
Neyland(config-if)# dot1x multiple-hosts
```

Authenticating Users

The **Authenticated Users** page displays user port access lists. The User Access Lists are defined in the **Add User Name** page. To open the **Authenticated Users** page, click **Switch →Network Security →Authenticated Users**.

Figure 7-84. Authenticated Users



User Name

	Port	Session Time	Authentication Method	MAC Address
1	g1	5411	Remote	000000000000
2	g2	0	Remote	000000000000
3	g3	0	Remote	000000000000
4	g4	0	Remote	000000000000
5	g5	0	Remote	000000000000
6	g6	0	Remote	000000000000
7	g7	0	Remote	000000000000
8	g8	0	Remote	000000000000
9	g9	0	Remote	000000000000
10	g10	0	Remote	000000000000
11	g11	0	Remote	000000000000
12	g12	0	Remote	000000000000
13	g13	0	Remote	000000000000
14	g14	0	Remote	000000000000
15	g15	0	Remote	000000000000
16	g16	0	Remote	000000000000
17	g17	5412	Remote	000000000000
18	g18	0	Remote	000000000000
19	g19	0	Remote	000000000000
20	g20	0	Remote	000000000000
21	g21	0	Remote	000000000000
22	g22	0	Remote	000000000000
23	g23	0	Remote	000000000000
24	g24	0	Remote	000000000000

User Name — List of users authorized via the RADIUS Server.

Port — The port number(s) used for authentication - per user name.

Session Time — The amount of time the user was logged on to the device. The field format is **Day:Hour:Minute:Seconds**, for example, 3 days: 2 hours: 4 minutes: 39 seconds.

Last Authentication — The amount of time that has passed since the user was last authenticated. The field format is **Day:Hour:Minute:Seconds**, for example, 3 days:2 hours: 4 minutes: 39 seconds.

Authentication Method — The method by which the last session was authenticated. The possible field values are:

> **Remote** — The user was authenticated from a remote server.
>
> **None** — The user was not authenticated.

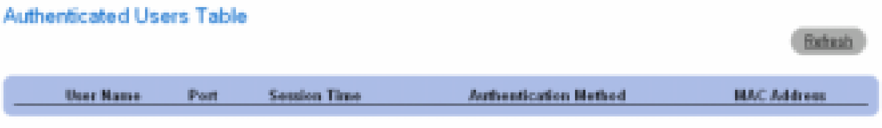
MAC Address — The client (supplicant) MAC address.

Displaying the Authenticated Users Table

1. Open the **Add User Name** page.
2. Click **Show All**.

   The **Authenticated Users Table** opens:

Figure 7-85. Authenticated Users Table



User Name	Port	Session Time	Authentication Method	MAC Address

Authenticating Users Using the CLI Commands

The following table summarizes the equivalent CLI commands for authenticating users as displayed in the **Add User Name** page.

Table 7-51. Add User Name CLI Commands

CLI Command	Description
show dot1x users [**username** *username*	Displays 802.1X users for the device

The following is an example of the CLI commands:

```
console# show dot1x users


Username  Session   Last   Auth     MAC Address        Interface
          Time      Auth   Method
--------  --------  -----  -------- -----------------  --------
Bob       1d3h      58m    Remote   00:08:3b:79:87:87  g1
John      8h19m     2m     None     00:08:3b:89:31:27  g2
```

Configuring Port Security

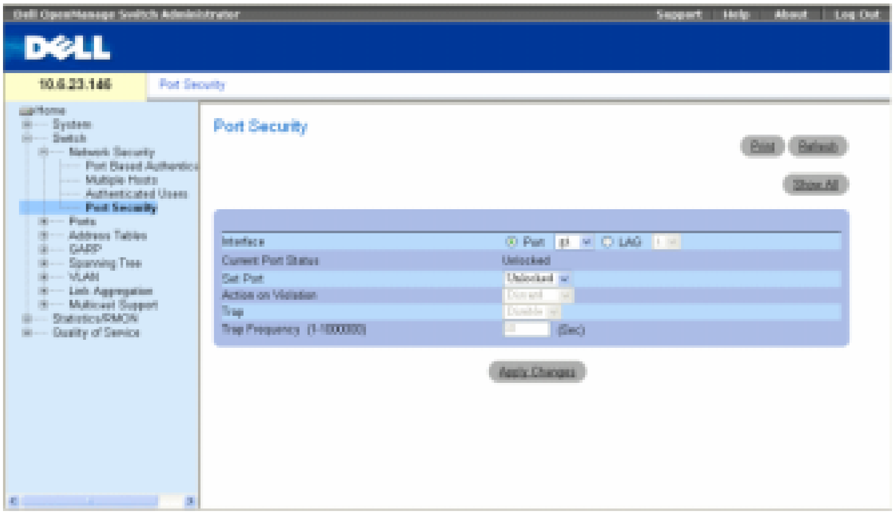
Network security can be increased by limiting access on a specific port only to users with specific MAC addresses. The MAC addresses can be dynamically learned, up to that point, or they can be statically configured. Locked port security monitors both received and learned packets that are received on specific ports. Access to the locked port is limited to users with 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 packet is received on a locked port, and the packet's source MAC address is not tied to that port (either it was learned on a different port, or is unknown to the system), the protection mechanism is invoked, and can provide various options. Unauthorized packets arriving to a locked port are either:

- Forwarded
- Discarded with no trap
- Discarded with a trap
- The ingress port is disabled

Locked port security also enables storing a list of MAC addresses in the configuration file. The MAC address list can be restored after the device has been reset.

Disabled ports are activated from the **Port Parameters** page, see "Defining Port Parameters". To open the **Port Security** page, click **Switch→Network Security→Port Security**.

Figure 7-86. Port Security



Port Security

Interface	● Port g1 ○ LAG 1
Current Port Status	Unlocked
Set Port	Unlocked
Action on Violation	Discard
Trap	Disable
Trap Frequency (1-1000000)	10 (Sec)

Interface — The selected interface type on which Locked Port is enabled.

Port — The selected interface type is a port.

LAG — The selected interface type is a LAG.

Current Port Status — The currently configured Port status.

Set Port — The port is either locked or unlocked. The possible field values are:

Unlocked — Unlocks Port. This is the default value.

Locked — Locks Port.

Action on Violation — The action to be applied to packets arriving on a locked port. The possible field values are:

Forward — Forwards the packets from an unknown source, however, the MAC address is not learned.

Discard — Discards the packets from any unlearned source. This is the default value.

Shutdown — Discards the packet from any unlearned source and locks the port. Port remained locked until they are activated, or the device is reset.

Trap — Enables traps being sent when a packet is received on a locked port.

Trap Frequency (1-1000000) — The amount of time (in seconds) between traps. This field only applies to Locked ports. The default value is 10 seconds.

Defining a Locked Port

1. Open the **Port Security** page.
2. Select an interface type and number.
3. Define the fields.
4. Click **Apply Changes**.

   The locked port is added to the **Port Security Table**, and the device is updated.

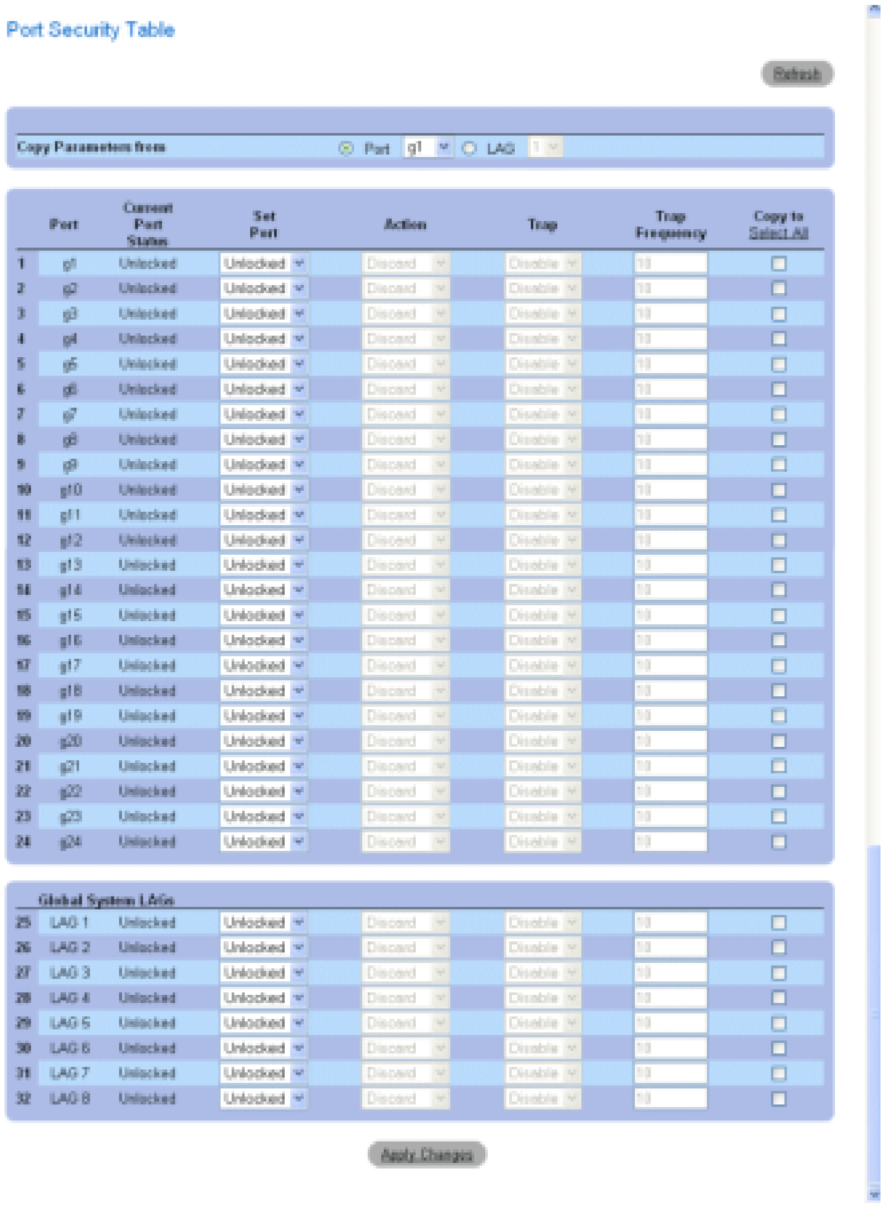
Displaying the Locked Port Table

1. Open the **Port Security** page.
2. Click **Show All.**

   The **Port Security Table** opens:

   Locked Ports can also be defined from the **Locked Ports Table,** as well as the **Port Security** page.

Figure 7-87. Port Security Table



Port Security Table

Refresh

Copy Parameters from ● Port g1 ○ LAG 1

	Port	Current Port Status	Set Port	Action	Trap	Trap Frequency	Copy to Select All
1	g1	Unlocked	Unlocked	Discard	Disable	10	□
2	g2	Unlocked	Unlocked	Discard	Disable	10	□
3	g3	Unlocked	Unlocked	Discard	Disable	10	□
4	g4	Unlocked	Unlocked	Discard	Disable	10	□
5	g5	Unlocked	Unlocked	Discard	Disable	10	□
6	g6	Unlocked	Unlocked	Discard	Disable	10	□
7	g7	Unlocked	Unlocked	Discard	Disable	10	□
8	g8	Unlocked	Unlocked	Discard	Disable	10	□
9	g9	Unlocked	Unlocked	Discard	Disable	10	□
10	g10	Unlocked	Unlocked	Discard	Disable	10	□
11	g11	Unlocked	Unlocked	Discard	Disable	10	□
12	g12	Unlocked	Unlocked	Discard	Disable	10	□
13	g13	Unlocked	Unlocked	Discard	Disable	10	□
14	g14	Unlocked	Unlocked	Discard	Disable	10	□
15	g15	Unlocked	Unlocked	Discard	Disable	10	□
16	g16	Unlocked	Unlocked	Discard	Disable	10	□
17	g17	Unlocked	Unlocked	Discard	Disable	10	□
18	g18	Unlocked	Unlocked	Discard	Disable	10	□
19	g19	Unlocked	Unlocked	Discard	Disable	10	□
20	g20	Unlocked	Unlocked	Discard	Disable	10	□
21	g21	Unlocked	Unlocked	Discard	Disable	10	□
22	g22	Unlocked	Unlocked	Discard	Disable	10	□
23	g23	Unlocked	Unlocked	Discard	Disable	10	□
24	g24	Unlocked	Unlocked	Discard	Disable	10	□

	Global System LAGs						
25	LAG 1	Unlocked	Unlocked	Discard	Disable	10	□
26	LAG 2	Unlocked	Unlocked	Discard	Disable	10	□
27	LAG 3	Unlocked	Unlocked	Discard	Disable	10	□
28	LAG 4	Unlocked	Unlocked	Discard	Disable	10	□
29	LAG 5	Unlocked	Unlocked	Discard	Disable	10	□
30	LAG 6	Unlocked	Unlocked	Discard	Disable	10	□
31	LAG 7	Unlocked	Unlocked	Discard	Disable	10	□
32	LAG 8	Unlocked	Unlocked	Discard	Disable	10	□

Apply Changes

Configuring Locked Port Security with CLI Commands

The following table summarizes the equivalent CLI commands for configuring Locked Port security as displayed in the **Port Security** page.

Table 7-52. Port Security CLI Commands

CLI Command	Description
shutdown	Disables interfaces.
set interface active {**ethernet** *interface* | **port-channel** *port-channel-number*}	Reactivates an interface that is shutdown due to port security reasons.
port security [**forward** | **discard** | **discard-shutdown**] [**trap** *seconds*]	Locks learning of new addresses on an interface.
show ports security {**ethernet** *interface* | **port-channel** *port-channel-number*}	Displays port lock status.

The following is an example of the CLI commands:

```
Console # show ports security


Port   Status      Action       Trap       Frequency  Counter
-----  -------     -------      -------    ---------  --------
g7     Unlocked    Discard      Enable     100        88
g8     Unlocked    Discard,     Disable
                   Shutdown
g3     Unlocked    -            -          -          -
```

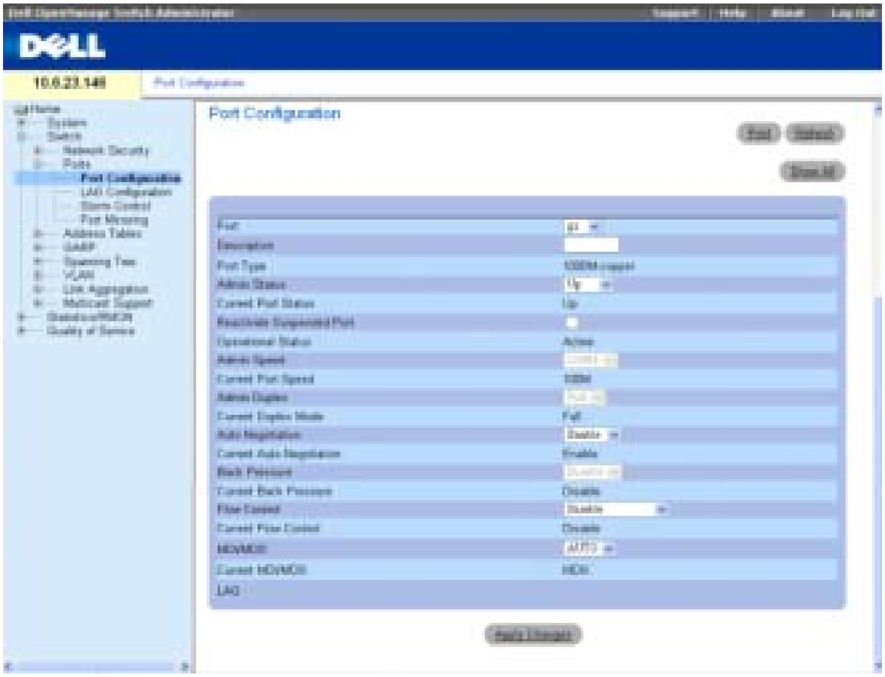
Configuring Ports

The **Ports** page contians links to port functionality pages including advanced features, such as Storm Control and Port Mirroring. To open the **Ports** page, click **Switch** →**Ports**.

Defining Port Parameters

The **Port Configuration** page contains fields for defining port parameters. To open the **Port Configuration** page, click **Switch** →**Ports** →**Port Configuration** in the tree view.

Figure 7-88. Port Configuration



Port Configuration

Port	g1
Description	
Port Type	1000M-copper
Admin Status	Up
Current Port Status	Up
Reactivate Suspended Port	□
Operational Status	Active
Admin Speed	[illegible]
Current Port Speed	100M
Admin Duplex	Full
Current Duplex Mode	Full
Auto Negotiation	Enable
Current Auto Negotiation	Enable
Back Pressure	Disable
Current Back Pressure	Disable
Flow Control	Disable
Current Flow Control	Disable
MDI/MDIX	AUTO
Current MDI/MDIX	MDIX
LAG	

Port — The port number for which port parameters are defined.

Description (0-64 Characters) — A brief interface description, such as Ethernet.

Port Type — The type of port.

Admin Status — Enables or disables traffic forwarding through the port. The new port status is displayed in the **Current Port Status** field.

Current Port Status — Specifies whether the port is currently operational or non-operational.

Re-Activate Port — Reactivates a port if the port has been disabled through the locked port security option.

Operational Status — The port operational status. Possible field values are:

> **Suspended** — The port is currently active, and is currently not receiving or transmitting traffic.
>
> **Active** — The port is currently active and is currently receiving and transmitting traffic.
>
> **Disable** — The port is currently disabled, and is not currently receiving or transmitting traffic.

Admin Speed — The configured rate for the port. The port type determines what speed setting options are available. Admin speed can only be designated when auto negotiation is disabled on the configured port.

Current Port Speed — The actual currently configured port speed (bps).

Admin Duplex — The port duplex mode can be either **Full** or **Half**. **Full** indicates that the interface supports transmission between the device and its link partner in both directions simultaneously. **Half** indicates that the interface supports transmission between the device and the client in only one direction at a time.

Current Duplex Mode — The currently configured port duplex mode.

Auto Negotiation — Enables Auto Negotiation on the port. Auto Negotiation is a protocol between two link partners that enables a port to advertise its transmission rate, duplex mode and flow control abilities to its partner.

Current Auto Negotiation — The currently configured Auto Negotiation setting.

Back Pressure — Enables Back Pressure mode on the port. Back Pressure mode is used with Half Duplex mode to disable ports from receiving messages.

Current Back Pressure — The currently configured Back Pressure setting.

Flow Control — Enables or disables flow control or enables the auto negotiation of flow control on the port. Operates when port is in **Full** duplex mode.

Current Flow Control — The currently configured Flow Control setting.

MDI/MDIX — Allows the device to decipher between crossed and uncrossed cables.

Hubs and switches are deliberately wired opposite 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 are 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 ensure that the correct pairs are connected. The possible field values are:

> **Auto** — Used to automatically detect the cable type.
>
> **MDI (Media Dependent Interface)** — Used for end stations.
>
> **MDIX (Media Dependent Interface with Crossover)** — Used for hubs and switches.

Current MDI/MDIX— The currently configured device MDI/MDIX settings.

LAG — Specifies if the port is part of a LAG.

Defining Port Parameters

1. Open the **Port Configuration** page.
2. Select a port in the **Port** Field.
3. Define the remaining fields.
4. Click **Apply Changes**.

   The port parameters are saved to the device.

Modifying Port Parameters

1. Open the **Port Configuration** page.
2. Select a port in the **Port** Field.
3. Modify the remaining fields.
4. Click **Apply Changes**.

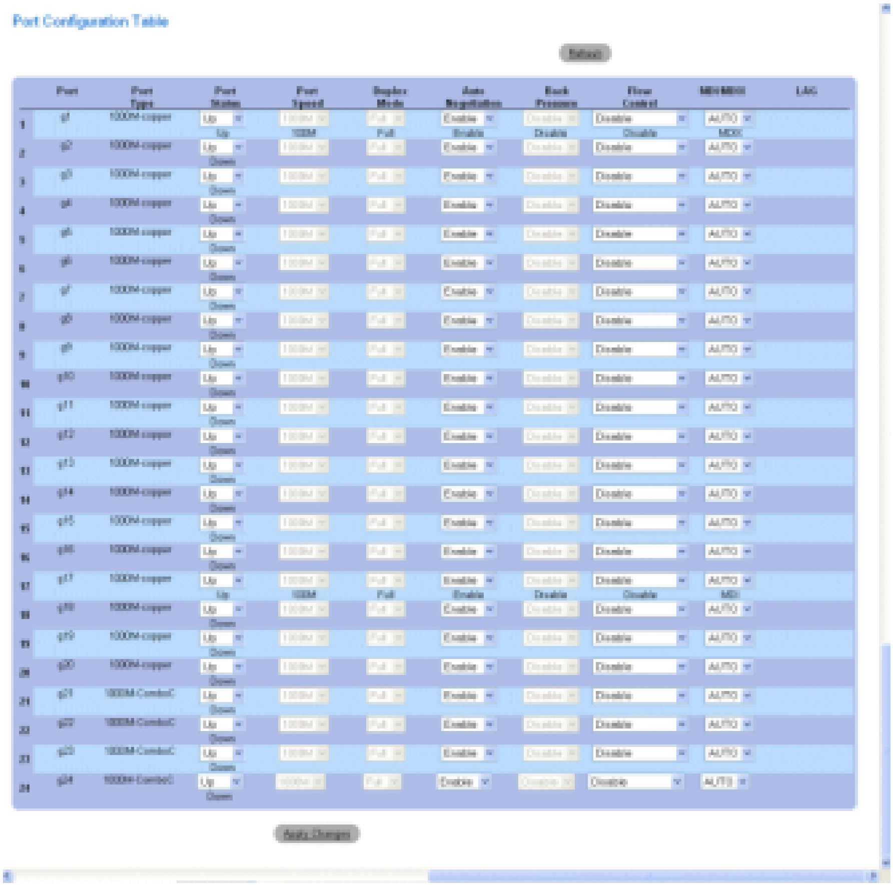
   The port parameters are saved to the device.

Displaying the Port Configuration Table:

1. Open the **Port Configuration** page.
2. Click **Show All.**

   The **Ports Configuration Table** opens:

Figure 7-89. Ports Configuration Table



Port Configuration Table

	Port	Port Type	Port Status	Port Speed	Duplex Mode	Auto Negotiation	Back Pressure	Flow Control	MDI/MDIX	LAG
1	g1	1000M-copper	Up Up	1000M 100M	Full Full	Enable Enable	Disable Disable	Disable Disable	AUTO MDIX	
2	g2	1000M-copper	Up Down	1000M	Full	Enable	Disable	Disable	AUTO	
3	g3	1000M-copper	Up Down	1000M	Full	Enable	Disable	Disable	AUTO	
4	g4	1000M-copper	Up Down	1000M	Full	Enable	Disable	Disable	AUTO	
5	g5	1000M-copper	Up Down	1000M	Full	Enable	Disable	Disable	AUTO	
6	g6	1000M-copper	Up Down	1000M	Full	Enable	Disable	Disable	AUTO	
7	g7	1000M-copper	Up Down	1000M	Full	Enable	Disable	Disable	AUTO	
8	g8	1000M-copper	Up Down	1000M	Full	Enable	Disable	Disable	AUTO	
9	g9	1000M-copper	Up Down	1000M	Full	Enable	Disable	Disable	AUTO	
10	g10	1000M-copper	Up Down	1000M	Full	Enable	Disable	Disable	AUTO	
11	g11	1000M-copper	Up Down	1000M	Full	Enable	Disable	Disable	AUTO	
12	g12	1000M-copper	Up Down	1000M	Full	Enable	Disable	Disable	AUTO	
13	g13	1000M-copper	Up Down	1000M	Full	Enable	Disable	Disable	AUTO	
14	g14	1000M-copper	Up Down	1000M	Full	Enable	Disable	Disable	AUTO	
15	g15	1000M-copper	Up Down	1000M	Full	Enable	Disable	Disable	AUTO	
16	g16	1000M-copper	Up Down	1000M	Full	Enable	Disable	Disable	AUTO	
17	g17	1000M-copper	Up Up	1000M 100M	Full Full	Enable Enable	Disable Disable	Disable Disable	AUTO MDI	
18	g18	1000M-copper	Up Down	1000M	Full	Enable	Disable	Disable	AUTO	
19	g19	1000M-copper	Up Down	1000M	Full	Enable	Disable	Disable	AUTO	
20	g20	1000M-copper	Up Down	1000M	Full	Enable	Disable	Disable	AUTO	
21	g21	1000M-ComboC	Up Down	1000M	Full	Enable	Disable	Disable	AUTO	
22	g22	1000M-ComboC	Up Down	1000M	Full	Enable	Disable	Disable	AUTO	
23	g23	1000M-ComboC	Up Down	1000M	Full	Enable	Disable	Disable	AUTO	
24	g24	1000M-ComboC	Up Down	1000M	Full	Enable	Disable	Disable	AUTO	

Configuring Ports with CLI Commands

The following table summarizes the equivalent CLI commands for configuring ports as displayed in the **Ports Configuration Table** page.

Table 7-53. Port Configuration CLI Commands

CLI Command	Description
interface ethernet *interface*	Enters the interface configuration mode to configure an ethernet type interface.
description *string*	Adds a description to an interface configuration.

Table 7-53. Port Configuration CLI Commands

CLI Command	Description
shutdown	Disables interfaces that are part of the currently set context.
set interface active {ethernet *interface* | **port-channel** *port-channel-number***}**	Reactivates an interface that is shutdown due to security reasons.
speed *bps*	Configures the speed of a given ethernet interface when not using auto negotiation.
autobaud	Sets the line for automatic baud rate detection.
duplex {**half** | **full**}	Configures the full/half duplex operation of a given ethernet interface when not using auto negotiation.
negotiation	Enables auto negotiation operation for the speed and duplex parameters of a given interface.
back-pressure	Enables Back Pressure on a given interface.
flowcontrol {**auto** | **on** | **off** | **rx** | **tx**}	Configures the Flow Control on a given interface.
mdix {**on** | **auto**}	Enables automatic crossover on a given interface or Port-channel.
show interfaces configuration [ethernet *interface* |**port-channel** *port-channel-number***]**	Displays the configuration for all configured interfaces.
show interfaces status [ethernet *interface* | **port-channel** *port-channel-number***]**	Displays the status for all configured interfaces.
show interfaces description [ethernet *interface* | **port-channel** *port-channel-number***]**	Displays the description for all configured interfaces.

The following is an example of the CLI commands:

```
Console (config)# interface ethernet g5
Console (config-if)# description RD SW#3
Console (config-if)# shutdown
Console (config-if)# no shutdown
Console (config-if)# speed 100
Console (config-if)# duplex full
Console (config-if)# negotiation
Console (config-if)# back-pressure
Console (config-if)# flowcontrol on
Console (config-if)# mdix auto
Console (config-if)# exit
Console (config)# exit
Console# show interfaces configuration ethernet g5

Port   Type   Duplex  Speed    Neg      Flow       Admin   Back      Mdix
                                        Control    State   Pressure
                                                                     Mode
----   -----  ------  ------   ----     ------     -----   ------    ----
g5     1G     Full    100      Enabled  On         Up      Enable    Auto
console#
console# show interfaces status ethernet g5

Port   Type   Duplex  Speed    Neg      Flow       Link    Back      Mdix
                                        Control    State   Pressure
                                                                     Mode
----   -----  ------  ------   ----     ------     -----   ------    ----
g5     1G     Full    100      Enabled  On         Up      Disabled  on
console#
```

```
Console# show interfaces status

Port   Type   Duplex  Speed    Neg      Flow     Link      Back      Mdix
                                        Control  State     Pressure
                                                                     Mode
----   -----  ------  ------   ----     ------   -----     ------    ----
g1     1G     Full    100      Auto     On       Up        Enable    On
g1     100    Full    100      Off      Off      Down      Disable   Off
g2     100    Full    1000     Off      Off      Up        Disable   On


Ch     Type   Duplex  Speed    Neg      Flow     Back      Link
                                        Control  Pressure  State
---    ----   -----   ---      -----    -------  -------   ------
1      1000   Full    1000     Off      Off      Disable   Up
```

Defining LAG Parameters

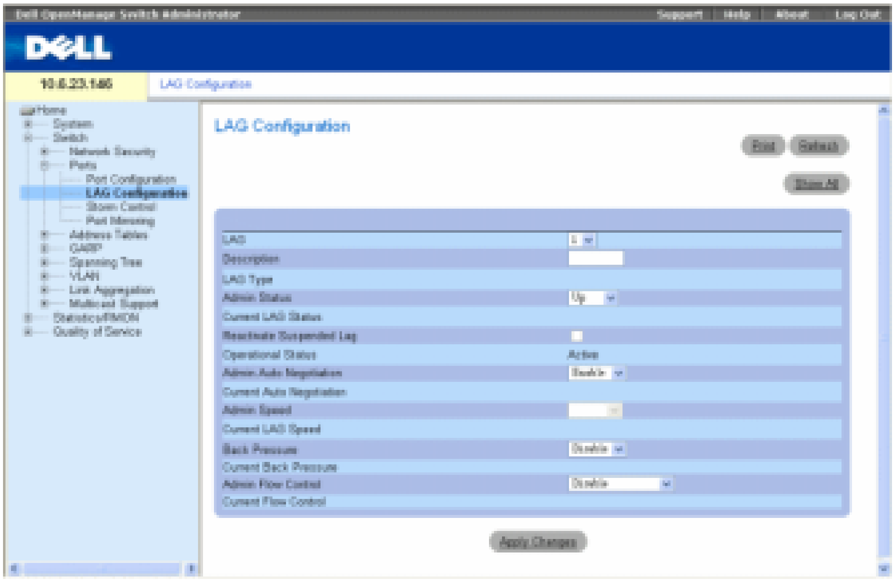
The **LAG Configuration** page contains fields for configuring parameters for configured LAGs. The device supports up to eight ports per LAG, and eight LAGs per system.

For information about Link Aggregated Groups (LAG) and assigning ports to LAGs, refer to **Aggregating Ports**.

To open the **LAG Configuration** page, click **Switch→Ports→LAG Configuration** in the tree view.

NOTE: If port configuration is modified while the port is a LAG member, the configuration change is only effective after the port is removed from the LAG.

Figure 7-90. LAG Configuration



LAG	1
Description	
LAG Type	
Admin Status	Up
Current LAG Status	
Reactivate Suspended Lag	☐
Operational Status	Active
Admin Auto Negotiation	Enable
Current Auto Negotiation	
Admin Speed	
Current LAG Speed	
Back Pressure	Disable
Current Back Pressure	
Admin Flow Control	Disable
Current Flow Control	

LAG — The LAG number.

Description (0-64 Characters) — Provides a user-defined description of the configured LAG.

LAG Type — The port types that comprise the LAG.

Admin Status — Enables or disables traffic forwarding through the selected LAG.

Current LAG Status — Indicates if the LAG is currently operating.

Re-Activate Suspended LAG — Reactivates a suspended LAG.

Operational Status — Operational status of the LAG.

Admin Auto Negotiation — Enables or disables Auto Negotiation on the LAG. Auto-negotiation is a protocol between two link partners that enables a LAG to advertise its transmission rate, duplex mode and flow control (the flow control default is disabled) abilities to its partner.

Current Auto Negotiation — The currently configured Auto Negotiation setting.

Admin Speed — The speed at which the LAG is operating.

Current LAG Speed — The currently configured speed at which the LAG is operating.

Admin Back Pressure — Enables or disables Back Pressure mode on the LAG. Back Pressure mode is effective on the ports operating in Half Duplex in the LAG.

Current Back Pressure — The currently configured Back Pressure setting.

Admin Flow Control — Enables/disables flow control, or enables the auto negotiation of flow control on the LAG. Flow Control mode is effective on the ports operating in Full Duplex in the LAG.

Current Flow Control — The user-designated flow control setting.

Defining LAG Parameters

1. Open the **LAG Configuration** page.
2. Select a LAG in the **LAG** field.
3. Define the fields.
4. Click **Apply Changes**.

   The LAG parameters are saved to the device.

Modifying LAG Parameters

1. Open the **LAG Configuration** page.
2. Select a LAG in the **LAG** field.
3. Modify the fields.
4. Click **Apply Changes**.

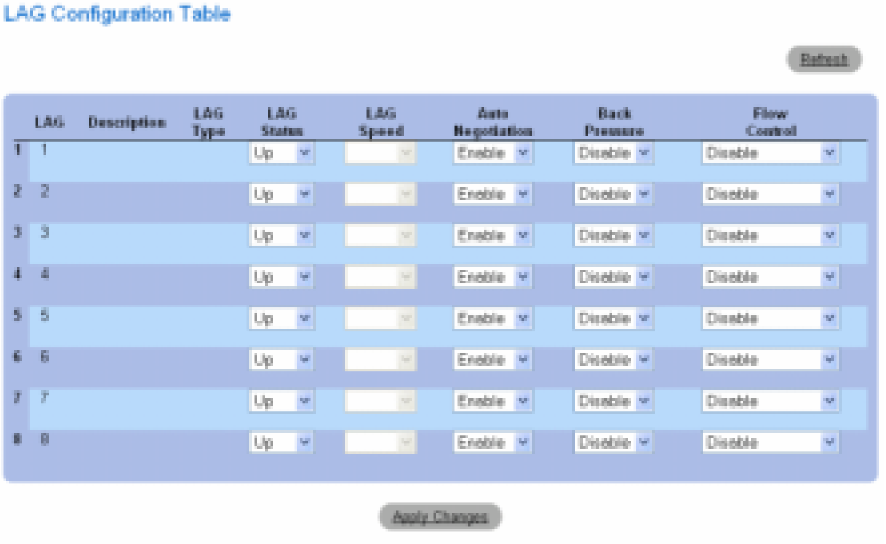
   The LAG parameters are saved to the device.

Displaying the LAG Configuration Table:

1. Open the **LAG Configuration** page.
2. Click **Show All.**

   The **LAG Configuration Table** opens:

Figure 7-91. LAG Configuration Table



	LAG	Description	LAG Type	LAG Status	LAG Speed	Auto Negotiation	Back Pressure	Flow Control
1	1			Up		Enable	Disable	Disable
2	2			Up		Enable	Disable	Disable
3	3			Up		Enable	Disable	Disable
4	4			Up		Enable	Disable	Disable
5	5			Up		Enable	Disable	Disable
6	6			Up		Enable	Disable	Disable
7	7			Up		Enable	Disable	Disable
8	8			Up		Enable	Disable	Disable

Configuring LAGs with CLI Commands

The following table summarizes the equivalent CLI commands for configuring LAGs as displayed in the **LAG Configuration** page.

Table 7-54. LAG Configuration CLI Commands

CLI Command	Description
interface port-channel *port-channel-number*	Enters the interface configuration mode of a specific port-channel.
description *string*	Adds a description to an interface configuration.
shutdown	Disables interfaces that are part of the currently set context.
speed *bps*	Configures the speed of a given ethernet interface when not using auto negotiation.
autobaud	Sets the line for automatic baud rate detection .
negotiation	Enables auto negotiation operation for the speed and duplex parameters of a given interface.
back-pressure	Enables Back Pressure on a given interface

Table 7-54. LAG Configuration CLI Commands

CLI Command	Description
flowcontrol {**auto** | **on** | **off** | **rx** | **tx**}	Configures the Flow Control on a given interface.
show interfaces configuration [**ethernet** *interface* | **port-channel** *port-channel-number*]	Displays the configuration for all configured interfaces.
show interfaces status [**ethernet** *interface* | **port-channel** *port-channel-number*]	Displays the status for all configured interfaces.
show interfaces description [**ethernet** *interface* | **port-channel** *port-channel-number*]	Displays the description for all configured interfaces.
show interfaces port-channel [*port-channel-number*]	Displays Port-channel information (which ports are members of that port-channel, and whether they are currently active or not).

The following is an example of the CLI commands:

```
console(config-if)# channel-group 1 mode on
console(config-if)# exit
console(config)# interface range e g21-24
console(config-if)# channel-group 1 mode on
console(config-if)# ex
console(config)# interface ethernet g5
console(config-if)# channel-group 2 mode on
console(config-if)# exit
console(config)# exit

console# show interfaces port-channel
Channel              Ports
---------            ---------
ch1                  Inactive: g(21-24)
ch2                  Active: g5
```

```
ch3
ch4
ch5
ch6
ch7
ch8
console#
```

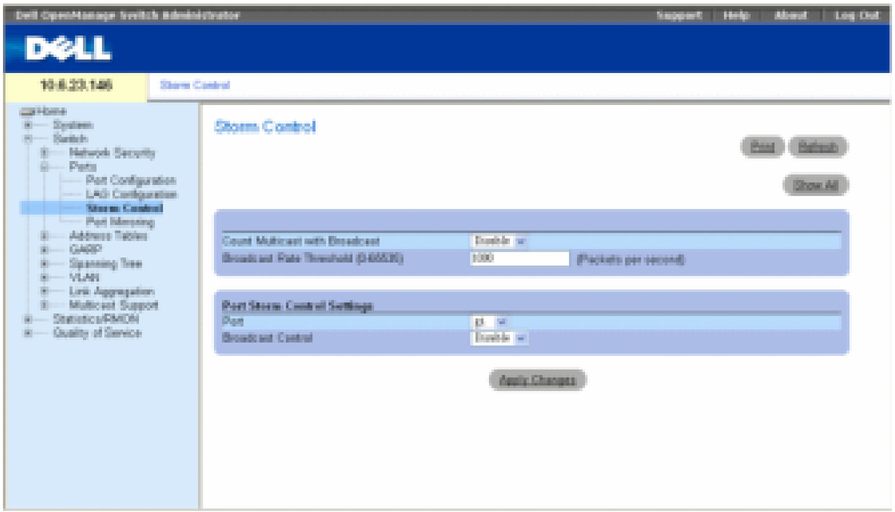
Enabling Storm Control

A Broadcast Storm is a result of an excessive amount of broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses are heaped onto the network, straining network resources or causing the network to time out.

The system measures the incoming Broadcast and Multicast frame rate separately on each port, and discard frames when the rate exceeds a user-defined rate.

The **Storm Control** page provides fields for enabling and configuring Storm Control. To open the **Storm Control** page, click **Switch→Ports→Storm Control** in the tree view.

Figure 7-92. Storm Control



Count Multicast with Broadcast: Disable
Broadcast Rate Threshold (0-65535): 1000 (Packets per second)

Port Storm Control Settings
Port: g1
Broadcast Control: Disable

Count Multicast with Broadcast — Counts Broadcast and Multicast traffic. The possible field values are:

- **Enable** — Counts Broadcast and Multicast traffic.

- **Disable** — Counts only Broadcast traffic.

Broadcast Rate Threshold (1-1000000)— The maximum rate (packets per second) at which unknown packets are forwarded. The range is 0-1000000. The default value is zero. All values are rounded to the nearest 64Kbps. If the field value is under 64Kbps, the value is rounded up to 64Kbps, with the exception of the value zero.

Port — The port from which storm control is enabled.

Broadcast Control — Enables or disables forwarding broadcast packet types on the device.

Enabling Storm Control on the Device

1. Open the **Storm Control** page.
2. Select an interface on which to implement storm control.
3. Define the fields.
4. Click **Show All**.

   The Storm Control is enabled on the device.

Modifying Storm Control Port Parameters

1. Open the **Storm Control** page.
2. Modify the fields.
3. Click **Show All**.

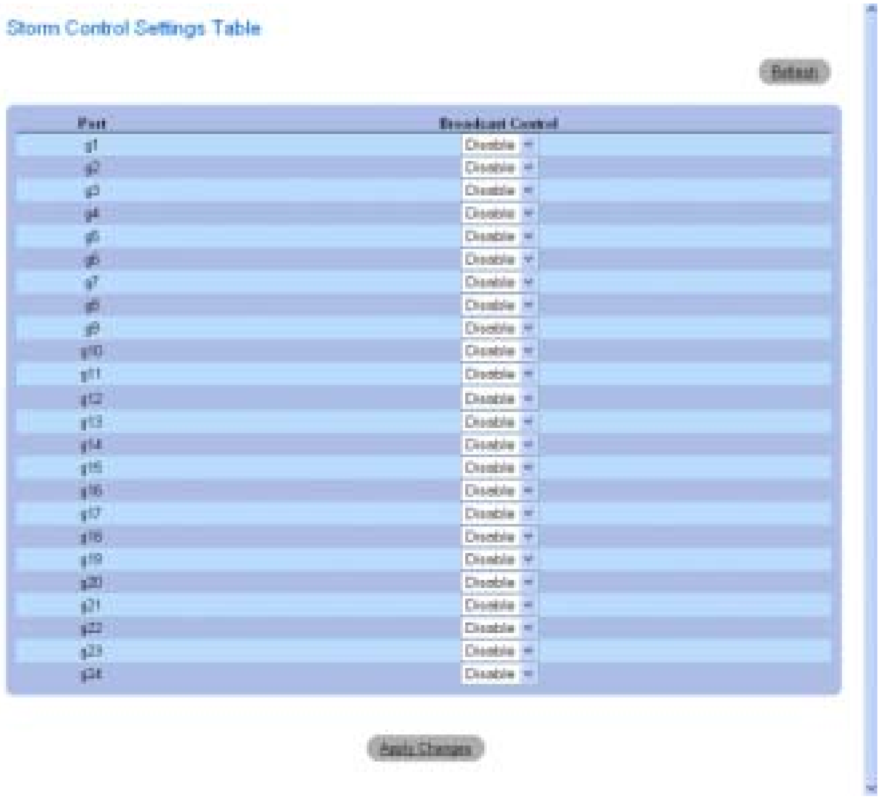
   The Storm Control port parameters are saved to the device.

Displaying the Port Parameters Table

1. Open the **Storm Control** page.
2. Click **Show All.**

   The **Storm Control Settings Table** opens:

Figure 7-93. Storm Control Settings Table



Port	Broadcast Control
g1	Disable
g2	Disable
g3	Disable
g4	Disable
g5	Disable
g6	Disable
g7	Disable
g8	Disable
g9	Disable
g10	Disable
g11	Disable
g12	Disable
g13	Disable
g14	Disable
g15	Disable
g16	Disable
g17	Disable
g18	Disable
g19	Disable
g20	Disable
g21	Disable
g22	Disable
g23	Disable
g24	Disable

Configuring Storm Control with CLI Commands

The following table summarizes the equivalent CLI commands for configuring Storm Control as displayed on the **Storm Control** page.

Table 7-55. Storm Control CLI Commands

CLI Command	Description
port storm-control include-multicast	Enables the device to count Multicast packets together with broadcast packets.
port storm-control broadcast enable	Enables broadcast storm control.
port storm-control broadcast rate *rate*	Configures the maximum broadcast rate.
show ports storm-control [**ethernet** *interface*]	Displays the storm control configuration.

The following is an example of the CLI commands:

```
console> enable
console# configure
Console(config)# port storm-control include-multicast
Console(config)# port storm-control broadcast rate 8000
Console(config)# interface ethernet g1
Console(config-if)# port storm-control broadcast enable
Console(config-if)# end
Console# show ports storm-control
Port                 Broadcast Storm control [Packets/sec]
-----                -------------------------------------
g1                   8000
g2                   Disabled
g4                   Disabled
```

Defining Port Mirroring Sessions

Port mirroring monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from one port to a monitoring port.

Port mirroring is configured by selecting a specific port to copy all packets, and different ports from which the packets copied. Before configuring Port Mirroring, note the following:

Before configuring Port Mirroring, note the following:

- Monitored port cannot operate faster than the monitoring port.
- All the RX/TX packets should be monitored to the same port.

The following restrictions apply to ports configured to be destination ports:

- Ports cannot be configured as a source port.
- Ports cannot be a LAG member.
- IP interfaces are not configured on the port.
- GVRP is not enabled on the port.
- The port is not a VLAN member.
- Only one destination port can be defined.

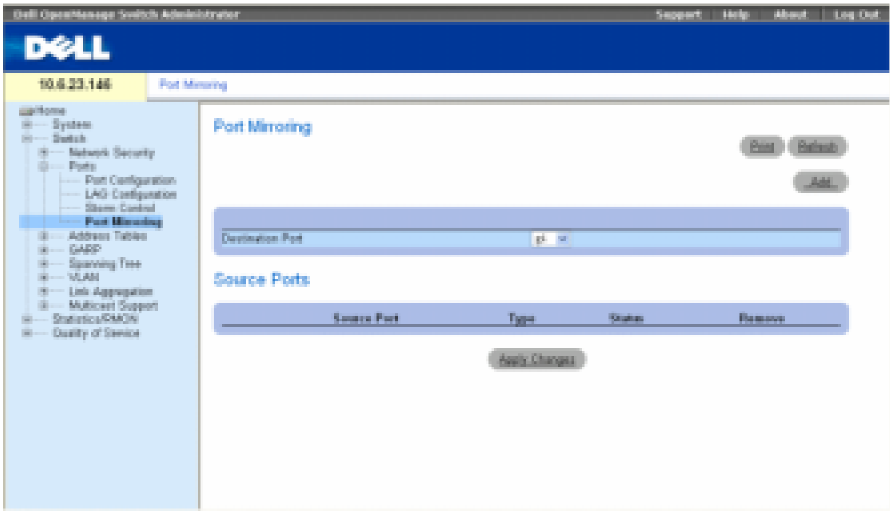
The following restrictions apply to ports configured to be source ports:

- Source Ports cannot be a LAG member.
- Ports cannot be configured as a destination port.
- All packets are transmitted tagged from the destination port.
- Monitored all RX/TX packets to the same port.

To open the **Port Mirroring** page, click **Switch→Ports→Port Mirroring** in the tree view.

NOTE: When a port is set to be a target port for a port-mirroring session, all normal operations on it are suspended. This includes Spanning Tree and LACP.

Figure 7-94. Port Mirroring



Destination Port — The port number to which port traffic is copied.

Source Port — Defines the port number from which port traffic is mirrored.

Type — Indicates if the source port is RX, TX, or both RX and TX.

Status — Indicates if the port is currently monitored (**Active**) or not monitored (**Ready**).

Remove — When selected, removes the port mirroring session.

Adding a Port Mirroring Session

1. Open the **Port Mirroring** page.
2. Click **Add**.

   The **Add Source Port** page opens.
3. Select the destination port from the **Destination Port** drop-down menu.

4 Select the source port from the **Source Port** drop-down menu.

5 Define the **Type** field.

6 Click **Apply Changes**.

The new source port is defined, and the device is updated.

Deleting a Copy Port from a Port Mirroring Session

1 Open the **Port Mirroring** page.

2 Select the **Remove** check box.

3 Click **Apply Changes**.

The selected port mirroring session is deleted, and the device is updated.

Configuring a Port Mirroring Session Using CLI Commands

The following table summarizes the equivalent CLI commands for configuring a Port Mirroring session as displayed in the **Port Mirroring** page.

Table 7-56. Port Mirroring CLI Commands

CLI Command	Description
port monitor *src-interface* [**rx** | **tx**]	Starts a port monitoring session.

The following is an example of the CLI commands:

```
Console(config)# interface ethernet g1
Console(config-if)# port monitor g8
Console# show ports monitor

Source Port   Destination Port    Type            Status      VLAN Tagging
-----------   ----------------    ------------    -------     ------------
g8            g1                  RX, TX          Active      No
g2            g8                  RX, TX          Active      No
g18           g8                  Rx              Active      No
```

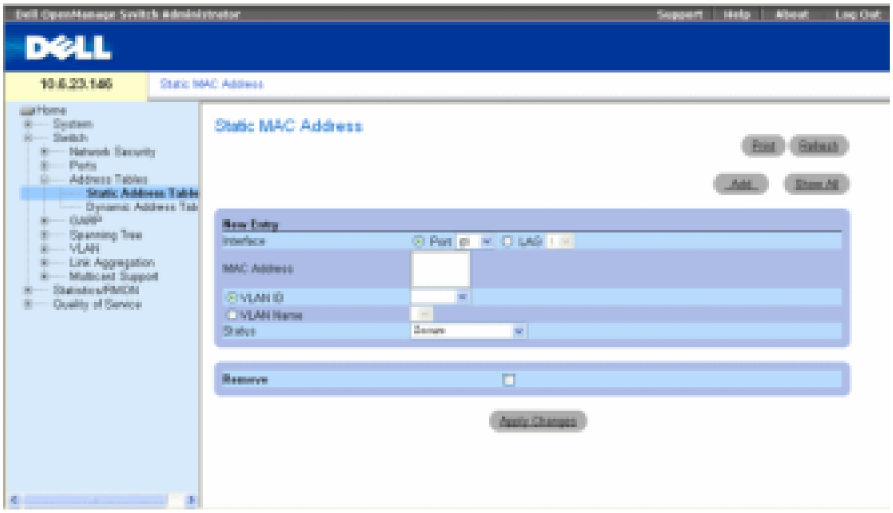
Configuring Address Tables

MAC addresses are stored in either the Static Address or the Dynamic Address databases. A packet addressed to a destination stored in one of the databases is forwarded immediately to the port. The Static and Dynamic Address Tables can be sorted by interface, VLAN, and interface type. MAC addresses are dynamically learned as packets from sources arrive at the device. Addresses are associated with ports by learning the ports from the frame's source address. Frames addressed to a destination MAC address that is not associated with any port are flooded to all ports of the relevant VLAN. Static addresses are manually configured. In order to prevent the bridging table from overflowing, dynamic MAC addresses, from which no traffic is seen for a certain period, are erased. To open the **Address Tables** page, click **Switch→Address Table** in the tree view.

Defining Static Addresses

The **Static MAC Address** page contains a list of static MAC addresses. Static Address can be added and removed from the **Static MAC Address** page. In addition, several MAC Addresses can be defined for a single port. To open the **Static MAC Address** page, click **Switch→Address Table→ Static Address** in the tree view.

Figure 7-95. Static MAC Address



Interface — The specific port or LAG to which the static MAC address is applied.

MAC Address — The MAC address listed in the current static address list.

VLAN ID — The VLAN ID attached to the MAC Address.

VLAN Name — User-defined VLAN name.

Status — MAC address status. Possible values are:

> **Secure** — Guarantees that a locked port MAC address is not deleted.
>
> **Permanent** — The MAC address is permanent.
>
> **Delete on Reset** — The MAC address is deleted when the device is reset.
>
> **Delete on Timeout** — The MAC address is deleted when a timeout occurs.

Remove — When selected, removes the the MAC address from the MAC Address Table.

Adding a Static MAC Address

1. Open the **Static MAC Address** page.
2. Click **Add**.

   The **Add Static MAC Address** page opens.
3. Complete the fields.
4. Click **Apply Changes**.

   The new static address is added to the **Static MAC Address Table**, and the device is updated.

Modifying a Static Address in the Static MAC Address Table

1. Open the **Static MAC Address** page.
2. Modify the fields.
3. Click **Apply Changes**.

   The static MAC address is modified, and the device is updated.

Removing a Static Address from the Static Address Table

1. Open the **Static MAC Address** page.
2. Click **Show All**.

   The **Static MAC Address Table** opens.
3. Select a table entry.
4. Select the **Remove** check box.
5. Click **Apply Changes**.

   The selected static address is deleted, and the device is updated.

Configuring Static Address Parameters Using CLI Commands

The following table summarizes the equivalent CLI commands for configuring static address parameters as displayed in the **Static MAC Address** page.

Table 7-57. Static Address CLI Commands

CLI Command	Description
bridge address *mac-address* {**ethernet** *interface* | *port-channel port-channel-number*} [**permanent** | **delete-on-reset** | **delete-on-timeout** | **secure**]]	Adds a static MAC-layer station source address to the bridge table.
show bridge address-table [**vlan** *vlan*] [**ethernet** *interface* | **port-channel** *port-channel-number*]	Displays entries in the bridge-forwarding database.

The following is an example of the CLI commands:.

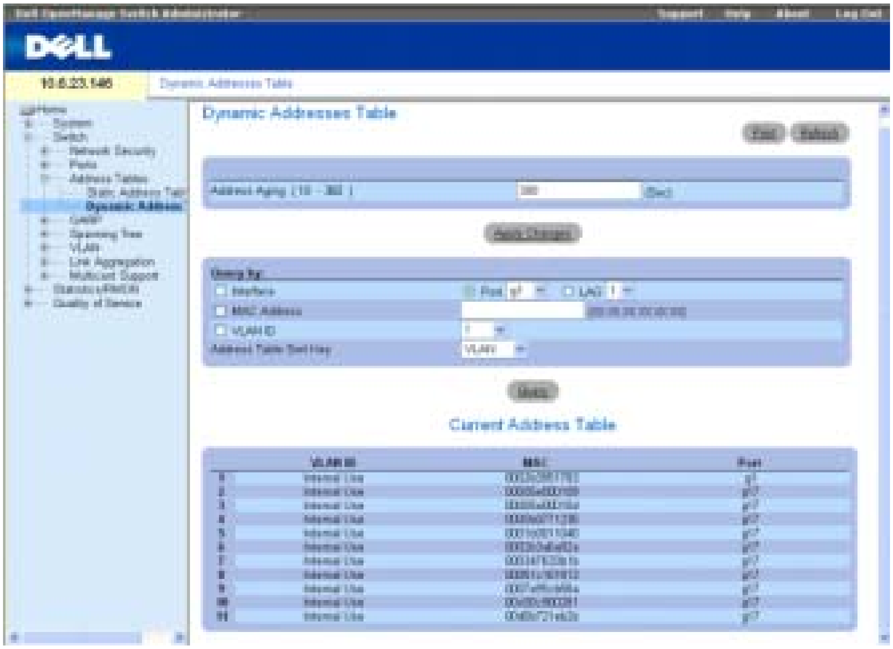
```
Console# show bridge address-table
Aging time is 300 sec

vlan    mac address          port    type
----    ------------         ----    --------
1       00:60:70:4C:73:FF    g8      dynamic
1       00:60:70:8C:73:FF    g8      dynamic
200     00:10:0D:48:37:FF    g9      static
g8      00:10:0D:98:37:88    g8      dynamic
```

Viewing Dynamic Addresses

The **Dynamic Address Table** contains fields for querying information in the dynamic address table, including the interface type, MAC addresses, VLAN, and table sorting. Packets forwarded to an address stored in the address table are forwarded directly to those ports. The **Dynamic Address Table** also contains information about the aging time before a dynamic MAC address is erased, and includes parameters for querying and viewing the Dynamic Address list. The Current Address Table contains dynamic address parameters by which packets are directly forwarded to the ports.

To open the **Dynamic Address Table**, click **Switch→Address Table→Dynamic Addresses Table** in the tree view.

Figure 7-96. Dynamic Address Table



Dynamic Addresses Table

Address Aging (10 - 360) 300 (Sec)

Query By:

□ Interface ● Port g? □ LAG 1

□ MAC Address (00:00:00:00:00:00)

□ VLAN ID 1

Address Table Sort Key VLAN

Current Address Table

	VLAN ID	MAC	Port
1	Internal Use	[illegible]	[illegible]
2	Internal Use	[illegible]	[illegible]
3	Internal Use	[illegible]	[illegible]
4	Internal Use	[illegible]	[illegible]
5	Internal Use	[illegible]	[illegible]
6	Internal Use	[illegible]	[illegible]
7	Internal Use	[illegible]	[illegible]
8	Internal Use	[illegible]	[illegible]
9	Internal Use	[illegible]	[illegible]
10	Internal Use	[illegible]	[illegible]
11	Internal Use	[illegible]	[illegible]

Address Aging (10-360) — Specifies the amount of time the MAC Address remains in the **Dynamic Address Table** before it is timed out if no traffic from the source is detected. The default value is 300 seconds.

Interface — Specifies the interface for which the table is queried. There are two interface types from which to select.

- **Port** — Specifies the port numbers for which the table is queried.
- **LAG** — Specifies the LAG for which the table is queried.

MAC Address — Specifies the MAC address for which the table is queried.

VLAN ID — The VLAN ID for which the table is queried.

Address Table Sort Key — Specifies the means by which the Dynamic Address Table is sorted.

Redefining the Aging Time

1. Open the **Dynamic Address Table**.
2. Define the **Aging Time** field.
3. Click Apply Changes.

   The aging time is modified, and the device is updated.

Querying the Dynamic Address Table

1. Open the **Dynamic Address Table**.
2. Define the parameter by which to query the **Dynamic Address Table**.

   Entries can be queried by **Port**, **MAC Address**, or **VLAN ID**.
3. Click **Query**.

   The **Dynamic Address Table** is queried.

Sorting the Dynamic Address Table

1. Open the **Dynamic Address Table**.
2. From the **Address Table Sort Key** drop-down menu, select whether to sort addresses by address, VLAN ID, or interface.
3. Click **Query**.

   The **Dynamic Address Table** is sorted.

Querying and Sorting Dynamic Addresses Using CLI Commands

The following table summarizes the equivalent CLI commands for querying and sorting dynamic addresses as displayed in the **Dynamic Address Table**.

Table 7-58. Query and Sort CLI Commands

CLI Command	Description
bridge aging-time *seconds*	Sets the address table aging time.
show bridge address-table [**vlan** *vlan*] [**ethernet** *interface* | **port-channel** *port-channel-number*]	Displays classes of dynamically created entries in the bridge-forwarding database.

The following is an example of the CLI commands:

```
Console (config)# bridge aging-time 250
Console (config)# exit
Console# show bridge address-table


Aging time is 250 sec


vlan      mac address         port     type
----      -----------         ----     ----
1         00:60:70:4C:73:FF   g8       dynamic
1         00:60:70:8C:73:FF   g8       dynamic
200       00:10:0D:48:37:FF   g8       static
```

Configuring GARP

Generic Attribute Registration Protocol (GARP) is a general-purpose protocol that registers any network connectivity or membership-style information. GARP defines a set of devices interested in a given network attribute, such as VLAN or Multicast address.

When configuring GARP, ensure the following:

- The leave time must be greater than or equal to three times the join time.
- The leave all time must be greater than the leave time.

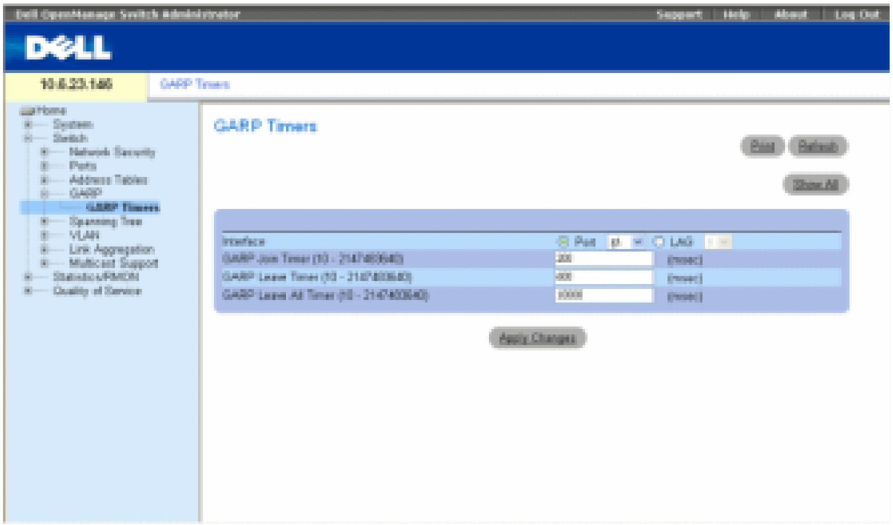
Set the same GARP timer values on all Layer 2-connected devices. If the GARP timers are set differently on the Layer 2-connected devices, GARP application does not operate successfully.

To open the **GARP** page, click **Switch→GARP** in the tree view.

Defining GARP Timers

The **GARP Timers** page contains fields for enabling GARP on the device. To open the **GARP Timers** page, click **Switch→GARP →GARP Timers** in the tree view.

Figure 7-97. GARP Timers



GARP Timers

Interface	● Port g1 ○ LAG 1	
GARP Join Timer (10 - 2147483640)	200	(msec)
GARP Leave Timer (10 - 2147483640)	600	(msec)
GARP Leave All Timer (10 - 2147483640)	10000	(msec)

Interface — Determines if enabled on a port or on a LAG.

GARP Join Timer (10 - 2147483640) — Time, in milliseconds, that PDUs are transmitted. The possible field value is 10-2147483640. The default value is 200 msec.

GARP Leave Timer (10 - 2147483640) — Time lapse, in milliseconds, that the device waits before leaving its GARP state. Leave time is activated by a Leave All Time message sent/received, and cancelled by the Join message received. Leave time must be greater than or equal to three times the join time. The possible field value is 0-2147483640. The default value is 600 msec.

GARP Leave All Timer (10 - 2147483640) — Time lapse, in milliseconds, that all devices wait before leaving the GARP state. The leave all time must be greater than the leave time. The possible field value is 0-2147483640. The default value is 10000 msec.

Defining GARP Timers

1. Open the **GARP Timers** page.
2. Complete the fields.
3. Click **Apply Changes**.

   The GARP parameters are saved to the device.

Copying Parameters in the GARP Timers Table

1. Open the **GARP Timers** page.
2. Click **Show All**.

   The **GARP Timers Table** opens.

3. Select the interface type in the **Copy Parameters from** field.
4. Select an interface in either the **Port** or **LAG** drop-down menu.
5. The definitions for this interface is copied to the selected interfaces. See step 6.
6. Select the **Copy to** check box to define the interfaces to which the GARP timer definitions are copied, or click **Select All** to copy the definitions to all ports or LAGs.
7. Click **Apply Changes**.

   The parameters are copied to the selected port ports or LAGs in the **GARP Timers Table**, and the device is updated.

Defining GARP Timers Using CLI Commands

This table summarizes the equivalent CLI commands for defining GARP timers as displayed in the **GARP Timers** page.

Table 7-59. GARP Timer CLI Commands

CLI Command	Description
garp timer {**join** | **leave** | **leaveall**} *timer_value*	Adjusts the GARP application join, leave, and leaveall GARP timer values.

The following is an example of the CLI commands:

```
console(config)# interface ethernet g1
console(config-if)# garp timer leave 900
console(config-if)# end
console# show gvrp configuration ethernet g1

GVRP Feature is currently Disabled on the device.
Maximum VLANs: 223


Port(s)  GVRP-     Registration  Dynamic VLAN  Timers   (milliseconds)
         Status                  Creation      Join     Leave   Leave All
-------  --------  ------------  ------------  -------  ------  ---------
g1       Disabled  Normal        Enabled       200      900     10000

console#
```

Configuring the Spanning Tree Protocol

Spanning Tree Protocol (STP) provides tree topography for any arrangement of bridges. STP also provides one path between end stations on a network, eliminating loops.

Loops occur when alternate paths exist between hosts. Loops in an extended network can cause bridges to forward traffic indefinitely, resulting in increased traffic and reducing network efficiency.

The devices support the following Spanning Tree protocols:

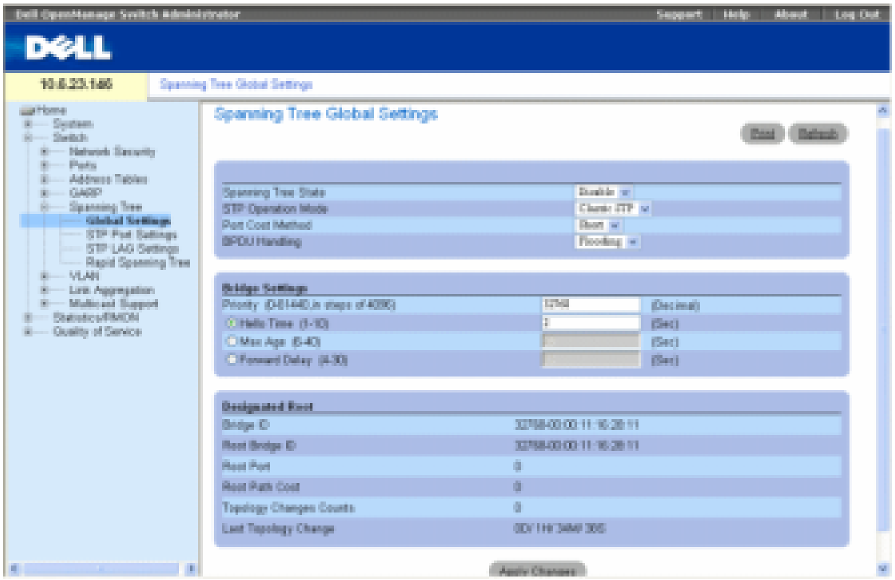
- **Classic STP** — Provides a single path between end stations, avoiding and eliminating loops. For more information on configuring Classic STP, see "Defining STP Global Settings".
- **Rapid STP** — Detects and uses of network topologies that provide faster spanning tree convergence, without creating forwarding loops. For more information on configuring Rapid STP, see "Configuring Rapid Spanning Tree".

To open the **Spanning Tree** page, click **Switch→Spanning Tree** in the tree view.

Defining STP Global Settings

The **STP Global Settings** page contains parameters for enabling and configuring STP operation on the device. To open the **STP Global Settings** page, click **Switch→Spanning Tree→Global Settings** in the tree view.

Figure 7-98. STP Global Settings



Spanning Tree Global Settings

Spanning Tree State	Enable
STP Operation Mode	Classic STP
Port Cost Method	Short
BPDU Handling	Flooding

Bridge Settings

Priority (0-61440, in steps of 4096)	32768	(Decimal)
● Hello Time (1-10)	2	(Sec)
○ Max Age (6-40)		(Sec)
○ Forward Delay (4-30)		(Sec)

Designated Root

Bridge ID	32768-00:00:11:16:28:11
Root Bridge ID	32768-00:00:11:16:28:11
Root Port	0
Root Path Cost	0
Topology Changes Counts	0
Last Topology Change	0D/1H/34M/30S

Spanning Tree State — Enables or disables Spanning Tree on the device. The possible field values are:

- **Enable** — Enables Spanning Tree
- **Disable** — Disables Spanning Tree

STP Operation Mode — The STP mode by which STP is enabled on the device. The possible field values are:

Classic STP — Enables Classic STP on the device. This is the default value.

Rapid STP — Enables Rapid STP on the device.

Port Cost Method — Determines the Spanning Tree default path cost method. The possible field values are:

Short — Specifies 1 through 65535 range for port path costs. This is the default value.

Long — Specifies 1 through 200000000 range for port path costs.

BPDU Handling — Determines how BPDU packets are managed when STP is disabled on the port/ device. BPDUs are used to transmit spanning tree information. The possible field values are:

Filtering — Filters BPDU packets when spanning tree is disabled on an interface.

Flooding — Floods BPDU packets when spanning tree is disabled on an interface. This is the default value.

Priority (0-) — Specifies the bridge priority value. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the switch with the lowest priority value becomes the Root Bridge. The default value is 32768. The bridge priority value is provided in increments of 4096 (4K increments). For example, 0, 4096, 8192, etc.

Hello Time (1-10) — Specifies the device Hello Time. The Hello Time indicates the amount of time in seconds a root bridge waits between configuration messages. The default is 2 seconds.

Max Age (6-40) — Specifies the device Maximum Age Time. The Maximum Age Time indicates the amount of time in seconds a bridge waits before sending configuration messages. The default max age is 20 seconds.

Forward Delay (4-30) — Specifies the device forward delay time. The Forward Delay Time indicates the amount of time in seconds a bridge remains in a listening and learning state before forwarding packets. The default is seconds.

Bridge ID — Identifies the Bridge priority and MAC address.

Root Bridge ID — Identifies the Root Bridge priority and MAC address.

Root Port — The port number that offers the lowest cost path from this bridge to the Root Bridge. It is significant when the Bridge is not the Root. The default is zero.

Root Path Cost — The cost of the path from this bridge to the root.

Topology Changes Counts — Specifies the total amount of STP state changes that have occurred since the last reboot.

Last Topology Change — The amount of time that has elapsed since the bridge was initialized or reset, and the last topographic change occurred. The time is displayed in a day hour minute second format, for example, hour minutes and seconds.

Defining STP Global Parameters

1. Open the **STP Global Settings** page.
2. Select the port that needs to be enabled from the **Select a Port** drop-down menu.
3. Select **Enable** in the **Spanning Tree State** field.
4. Select the **STP** mode in the **STP Operation Mode** field, and define the bridge settings.
5. Click **Apply Changes**.

   STP is enabled on the device.

Modifying STP Global Parameters

1. Open the **STP Global Settings** page.
2. Define the fields in the dialog.
3. Click **Apply Changes**.

   The STP parameters are modified, and the device is updated.

Defining STP Global Parameters Using CLI Commands

The following table summarizes the equivalent CLI commands for defining STP global parameters as displayed in the **STP Global Settings** page.

Table 7-60. STP Global Parameter CLI Commands

CLI Command	Description
spanning-tree	Enables spanning tree functionality.
spanning-tree mode {stp | rstp}	Configures the spanning tree protocol.
spanning-tree priority *priority*	Configures the spanning tree priority.
spanning-tree hello-time *seconds*	Configures the spanning tree bridge Hello Time, which is how often the device broadcasts Hello messages to other switches.
spanning-tree max-age *seconds*	Configures the spanning tree bridge maximum age.
spanning-tree forward-time *seconds*	Configures the spanning tree bridge forward time, which is the amount of time a port remains in the listening and learning states before entering the forwarding state.

Table 7-60. STP Global Parameter CLI Commands

CLI Command	Description
show spanning-tree [**ethernet** *interface* | **port-channel** *port-channel-number*]	Displays spanning tree configuration identifier.
show spanning-tree [**detail**] [**active** | **blockedports**]	Displays spanning tree configuration information - detailed information or active ports or blocked ports.

The following is an example of the CLI commands:

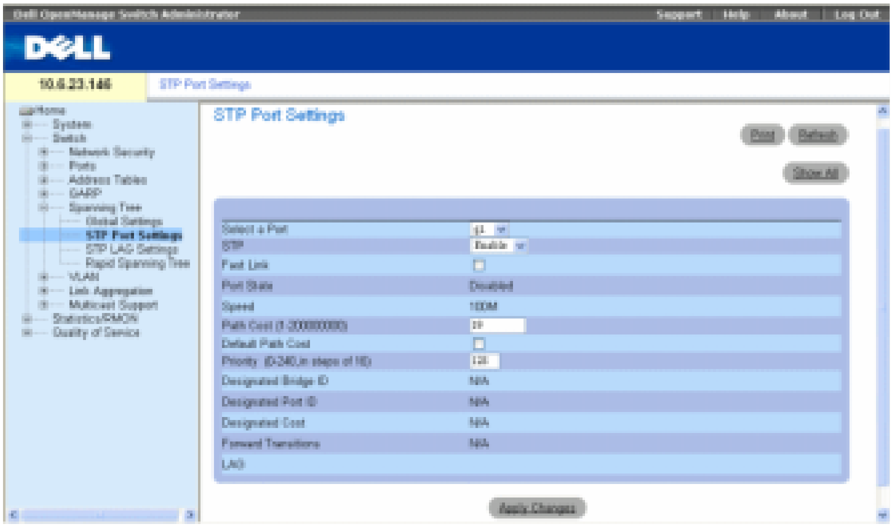
```
console(config)# spanning-tree
console(config)# spanning-tree mode rstp
console(config)# spanning-tree priority 12288
console(config)# spanning-tree hello-time 5
console(config)# spanning-tree max-age 15
console(config)# spanning-tree forward-time 25
console(config)# exit
console# show spanning-tree

Spanning tree enabled mode RSTP
Default port cost method: short

Root ID         Priority      12288
                Address       00:e8:00:b4:c0:00
                This switch is the root
                Hello Time  5 sec  Max Age 15 sec  Forward Delay 25 sec

Number of topology changes 5 last change occurred 00:05:28 ago
  Times:  hold 1, topology change 40, notification 5
          hello 5, max age 15, forward delay 25
```

```
Interfaces
Name    State     Prio.    Cost  Sts      Role     PortFast    Type
                  Nbr
-----   ------    -----    ----  ------   ------   ---------   ------
g1      enabled   128.1    100   DSBL     Dsbl     No          P2p (STP)
g2      enabled   128.2    100   DSBL     Dsbl     No          P2p (STP)
g3      enabled   128.3    100   DSBL     Dsbl     No          P2p (STP)
```

Defining STP Port Settings

The **STP Port Settings** page contains fields for assigning STP properties to individual ports. To open the **STP Port Settings** page, click **Switch→Spanning Tree→Port Settings** in the tree view.

Figure 7-99. STP Port Settings



STP Port Settings

Select a Port	g1
STP	Enable
Fast Link	□
Port State	Disabled
Speed	100M
Path Cost (1-200000000)	19
Default Path Cost	□
Priority (0-240,in steps of 16)	128
Designated Bridge ID	N/A
Designated Port ID	N/A
Designated Cost	N/A
Forward Transitions	N/A
LAG	

Select a Port — Port on which STP is enabled.

STP — Enables or disables STP on the port.

Fast Link — When selected, enables Fast Link mode for the port. If Fast Link mode is enabled for a port, the **Port State** is automatically placed in the **Forwarding** state when the port link is up. Fast Link mode optimizes the time it takes for the STP protocol to converge. STP convergence can take 30-60 seconds in large networks.

Port State — The current port STP state. If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are:

> **Disabled** — The port link is currently down.
>
> **Blocking** — The port is currently blocked and cannot be used to forward traffic or learn MAC addresses. Blocking is displayed when Classic STP is enabled.
>
> **Listening** — The port is currently in the listening mode. The port cannot forward traffic nor can it learn MAC addresses.
>
> **Learning** — The port is currently in the learning mode. The port cannot forward traffic however it can learn new MAC addresses.
>
> **Forwarding** — The port is currently in the forwarding mode. The port can forward traffic and learn new MAC addresses.

Speed — Speed at which the port is operating.

Path Cost (1-200000000) — The port contribution to the root path cost. The path cost is adjusted to a higher or lower value, and is used to forward traffic when a path being rerouted.

Default Path Cost — The default path cost of the port is automatically set by the port speed and the default path cost method.

The default values for long path costs are:

> **Ethernet** - 2000000
>
> **Fast Ethernet** - 200000
>
> **Gigabit Ethernet** - 20000

The default values for short path costs (short path costs are the default) are:

> **Ethernet** - 100
>
> **Fast Ethernet** - 19
>
> **Gigabit Ethernet** - 4

Priority (0-240, in steps of 16) — The priority value of the port. The priority value influences the port choice when a bridge has two ports connected in a loop. The priority value is between 0-240. The priority value is provided in increments of 16.

Designated Bridge ID — The bridge priority and the MAC Address of the designated bridge.

Designated Port ID— The selected port's priority and interface.

Designated Cost — The cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.

Forward Transitions — The number of times the port has changed from the **Blocking** state to the **Forwarding** state.

LAG — The LAG to which the port is attached.

Enabling STP on a Port

1. Open the **STP Port Settings** page.
2. Select **Enabled** in the **STP Port Status** field.
3. Define the **Fast Link**, **Path Cost**, and the **Priority** fields.
4. Click **Apply Changes**.

   STP is enabled on the port.

Modifying STP Port Properties

1. Open the **STP Port Settings** page.
2. Modify the **Priority**, **Fast Link**, **Path Cost**, and the **Fast Link** fields.
3. Click **Apply Changes**.

   The STP port parameters are modified, and the device is updated.

Displaying the STP Port Table

1. Open the **STP Port Settings** page.
2. Click **Show All**.

   The **STP Port Table** opens.

Defining STP Port Settings Using CLI Commands

The following table summarizes the equivalent CLI commands for defining STP port parameters as displayed in the **STP Port Settings** page.

Table 7-61. STP Port Settings CLI Commands

CLI Command	Description
spanning-tree disable	Disables spanning tree on a specific port.
spanning-tree cost *cost*	Configures the spanning tree cost contribution of a port.
spanning-tree port-priority *priority*	Configures port priority.
spanning-tree portfast	Enables PortFast mode.
show spanning-tree [**ethernet** *interface* | **port-channel** *port-channel-number*]	Displays spanning tree configuration.

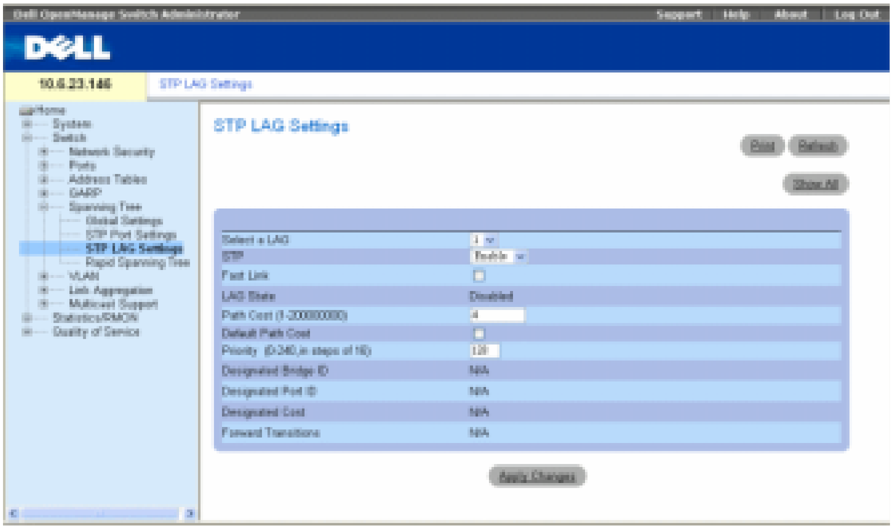
The following is an example of the CLI commands:

```
console(config)# interface ethernet g5
console(config-if)# spanning-tree disable
console(config-if)# spanning-tree cost 35000
console(config-if)# spanning-tree port-priority 96
console(config-if)# exit
console(config)# exit
console# show spanning-tree ethernet g5

Port g5 disabled
State: disabled                              Role: disabled
Port id:   96.5                              Port cost: 35000
Type: P2p    (configured: Auto)   STP        Port Fast: No (configured: No)
Designated bridge Priority : 32768           Address: 00:e8:00:b4:c0:00
Designated port id: 96.5                     Designated path cost: 19
Number of transitions to forwarding state: 0
BPDU: sent 0, received 0

console#
```

Defining STP LAG Settings

The **STP LAG Settings** page contains fields for assigning STP aggregating port parameters. To open the **STP LAG Settings** page, click **Switch→Spanning Tree→LAG Settings** in the tree view.

Figure 7-100. STP LAG Settings



STP LAG Settings

Select a LAG	1
STP	Enable
Fast Link	□
LAG State	Disabled
Path Cost (1-200000000)	4
Default Path Cost	□
Priority (0-240, in steps of 16)	128
Designated Bridge ID	N/A
Designated Port ID	N/A
Designated Cost	N/A
Forward Transitions	N/A

Select a LAG — The user-defined LAG. For more information, see "Defining LAG Membership".

STP — Enables or disables STP on the LAG.

Fast Link — Enables Fast Link mode for the LAG. If Fast Link mode is enabled for a LAG, the **LAG State** is automatically placed in the **Forwarding** state when the LAG is up. Fast Link mode optimizes the time it takes for the STP protocol to converge. STP convergence can take 30-60 seconds in large networks.

LAG State — Current STP state of a LAG. If enabled, the LAG state determines what forwarding action is taken on traffic. If the bridge discovers a malfunctioning LAG, the LAG is placed in the **Broken** state. Possible LAG states are:

> **Disabled** — The LAG link is currently down.
>
> **Blocking** — The LAG is blocked and cannot be used to forward traffic or learn MAC addresses.
>
> **Listening** — The LAG is in the listening mode and cannot forward traffic or learn MAC addresses.
>
> **Learning** — The LAG is in the learning mode and cannot forward traffic, but it can learn new MAC addresses.

Forwarding — The LAG is currently in the forwarding mode, and it can forward traffic and learn new MAC addresses.

Broken — The LAG is currently malfunctioning and cannot be used for forwarding traffic.

Path Cost (1-200000000) — Amount the LAG contributes to the root path cost. The path cost is adjusted to a higher or lower value, and is used to forward traffic when a path being rerouted. The path cost has a value of 1 to 200000000. If the path cost method is short, the LAG cost default value is 4. If the path cost method is long, the LAG cost default value is 20000.

Default Path Cost — When selected, the LAG path cost returns to its default value.

Priority (0-240, in steps of 16) — The priority value of the LAG. The priority value influences the LAG choice when a bridge has two looped ports. The priority value is between 0-240, in increments of 16.

Designated Bridge ID — The bridge priority and the MAC Address of the designated bridge.

Designated Port ID — The port priority and interface number of the designated port.

Designated Cost — The cost of the designated bridge.

Forward Transitions — The number of times the **LAG State** has changed from the **Blocking** state to a **Forwarding** state.

Modifying the LAG STP Parameters

1. Open the **STP LAG Settings** page.
2. Select a LAG from the **Select a LAG** drop-down menu.
3. Modify the fields as desired.
4. Click **Apply Changes**.

   The STP LAG parameters are modified, and the device is updated.

Defining STP LAG Settings Using CLI Commands

The following table summarizes the equivalent CLI commands for defining STP LAG settings.

Table 7-62. STP LAG Settings CLI Commands

CLI Command	Description
spanning-tree	Enables spanning tree.
spanning-tree disable	Disables spanning tree on a specific LAG.
spanning-tree cost *cost*	Configures the spanning tree cost contribution of a LAG.
spanning-tree port-priority *priority*	Configures port priority.

Table 7-62. STP LAG Settings CLI Commands

CLI Command	Description
show spanning-tree [**ethernet** *interface* | **port-channel** *port-channel-number*]	Displays spanning tree configuration.
show spanning-tree [**detail**] [**active** | **blockedports**]	Displays detailed spanning tree information on active or blocked ports

The following is an example of the CLI commands:

```
console(config)# interface port-channel 1
console(config-if)# spanning-tree port-priority 16
```

Configuring Rapid Spanning Tree

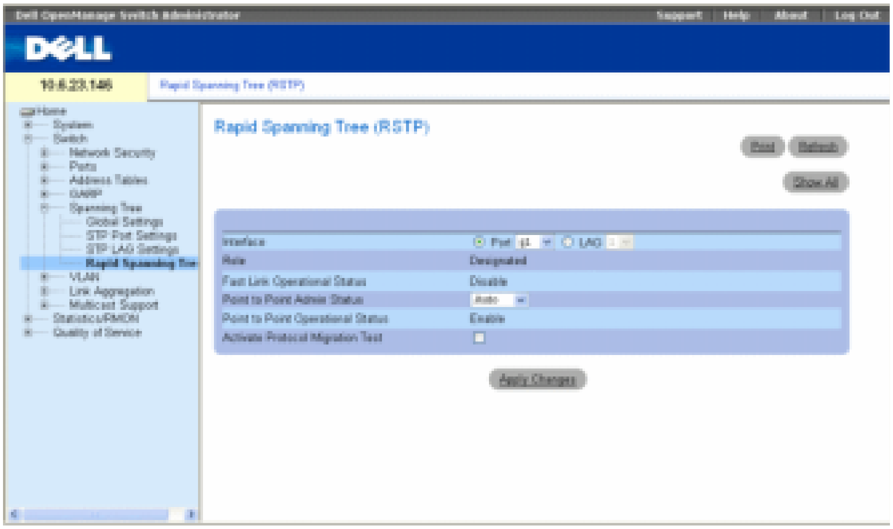
While Classic Spanning Tree guarantees preventing L2 forwarding loops in a general network topology, convergence can take up to 30-60 seconds. The convergence time is considered too long for many applications. When network topology allows, faster convergence may be possible. The Rapid Spanning Tree Protocol (RSTP) detects and uses of network topologies that provide faster convergence of the spanning tree, without creating forwarding loops.

RSTP has the following different port states:

- Disabled
- Learning
- Discarding
- Forwarding

Rapid Spanning Tree is enabled on the **STP Global Settings** page. To open the **Rapid Spanning Tree (RSTP)** page, click **Switch→Spanning Tree→Rapid Spanning Tree** in the tree view.

Figure 7-101. Rapid Spanning Tree (RSTP)



Rapid Spanning Tree (RSTP)

Interface	● Port g1 ○ LAG 1
Role	Designated
Fast Link Operational Status	Disable
Point to Point Admin Status	Auto
Point to Point Operational Status	Enable
Activate Protocol Migration Test	□

Interface — Port or LAG on which Rapid STP is enabled.

Role — The port role assigned by the STP algorithm in order to provide to STP paths. The possible field values are:

Root — Provides the lowest cost path to forward packets to root device.

Designated — The port or LAG via which the designated device is attached to the LAN.

Alternate — Provides an alternate path to the root device from the root interface.

Backup — Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop. Backup ports also occur when a LAN has two or more connections connected to a shared segment.

Disabled — The port is not participating in the Spanning Tree (the port's link is down).

Fast Link Operational Status — Indicates if Fast Link is enabled or disabled for the port or LAG. If Fast Link is enabled for a port, the port is automatically placed in the forwarding state.

Point-to-Point Admin Status — Enables or disables the device to establish a point-to-point link, or specifies for the device to automatically establish a point-to-point link.

To establish communications over a point-to-point link, the originating PPP first sends Link Control Protocol (LCP) packets to configure and test the data link. After a link is established and optional facilities are negotiated as needed by the LCP, the originating PPP sends Network Control Protocols (NCP) packets to select and configure one or more network layer protocols. When each of the chosen network layer protocols has been configured, packets from each network layer protocol can be sent over the link. The link remains configured for communications until explicit LCP or NCP packets close the link, or until some external event occurs. This is the actual device port link type. It may differ from the administrative state.

Point-to-Point Operational Status — The Point-to-Point operating state.

Activate Protocol Migrational Test — When selected, enables PPP sending Link Control Protocol (LCP) packets to configure and test the data link.

Enabling RSTP

1. Open the **Rapid Spanning Tree (RSTP)** page.
2. Define the **Point-to-Point Admin**, **Point-to-Point Oper**, and the **Activate Protocol Migration** fields.
3. Click **Apply Changes**.

   Rapid STP is enabled, and the device is updated.

Defining Rapid STP Parameters Using CLI Commands

The following table summarizes the equivalent CLI commands for defining Rapid STP parameters as displayed in the **Rapid Spanning Tree (RSTP)** page.

Table 7-63. RSTP Settings CLI Command

CLI Command	Description
spanning-tree link-type {**point-to-point** | **shared**}	Overrides the default link-type setting.
spanning tree mode {**stp** | **rstp**}	Configure the spanning tree protocol currently running.
clear spanning-tree detected-protocols [**ethernet** *interface* | **port-channel** *port-channel-number*]	Restarts the protocol migration process.
show spanning-tree [**ethernet** *interface* | **port-channel** *port-channel-number*]	Displays spanning tree configuration.

The following is an example of the CLI commands:

```
Console(config)# interface ethernet g5
Console(config-if)# spanning-tree link-type shared
```

Configuring VLANs

VLANs are logical subgroups of a Local Area Network (LAN) created via software rather than defining a hardware solution. VLANs combine user stations and network devices into a single domain regardless of the physical LAN segment to which they are attached. VLANs allow network traffic to flow more efficiently within subgroups. VLANs managed through software reduces the amount of time in which network changes are implemented.

VLANs have no minimum number of ports, and can be created per device or any other logical connection combination, as VLANs are software based and not defined by physical attributes.

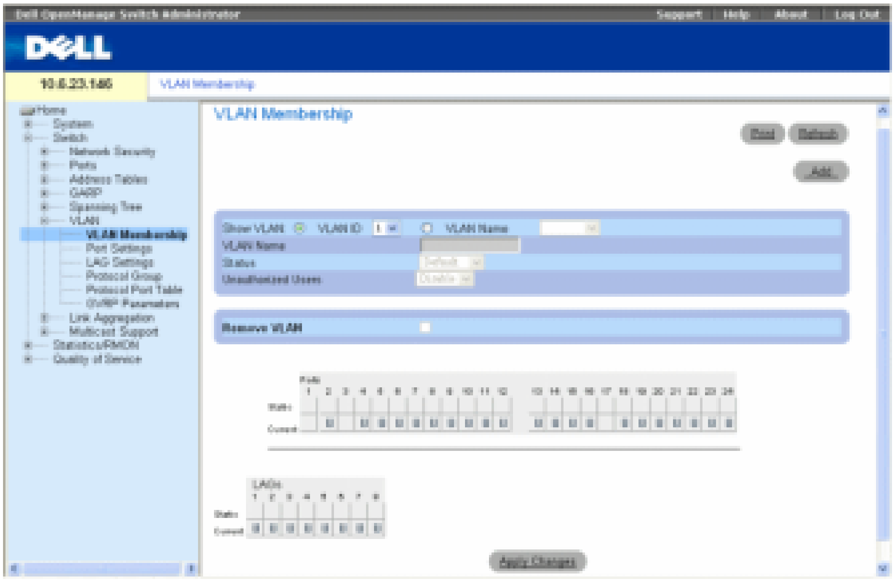
VLANs function at Layer 2. Since VLANs isolate traffic within the VLAN, a Layer 3 router functioning router is needed to allows traffic flow between VLANs. Layer 3 routers identify segments and coordinate with VLANs. VLANs are broadcast and Multicast domains. Broadcast and Multicast traffic is transmitted only in the VLAN in which the traffic is generated.

VLAN tagging provides a method of transferring VLAN information between VLAN groups. VLAN tagging attaches a tag to packet headers. The VLAN tag indicates to which VLAN the packet belongs. VLAN tags are attached to the packet by either the end station or by the network device. VLAN tags also contains VLAN network priority information. Combining VLANs and GVRP enables the automatic dispersal of VLAN information. To open the **VLAN** page, click **Switch→ VLAN** in the tree view.

Defining VLAN Members

The **VLAN Membership** page contains fields for defining VLAN groups. The device supports the mapping of 4094 VLAN IDs to 256 VLANs. All ports must have a defined PVID. If no other value is configured the default VLAN PVID is used. VLAN number 1 is the default VLAN, and cannot be deleted from the system. To open the **VLAN Membership** page, click **Switch→VLAN→VLAN Membership** in the tree view.

Figure 7-102. VLAN Membership Page



VLAN Membership

Show VLAN ● VLAN ID 1 ○ VLAN Name

VLAN Name

Status Default

Unauthorized Users Disable

Remove VLAN □

Ports 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

Static

Current

LAGs 1 2 3 4 5 6 7 8

Static

Current

Show VLAN — Lists and displays specific VLAN information according to VLAN ID or VLAN name.

VLAN Name — The user-defined VLAN name.

Status — The VLAN type. Possible values are:

- **Dynamic** — The VLAN was dynamically created through GVRP.
- **Static** — The VLAN is user-defined.
- **Default** — The VLAN is the default VLAN.

Unauthorized Users — Enables or disables unauthorized users from accessing a VLAN.

Remove VLAN — When selected, removes the VLAN from the VLAN Membership Table.

Adding New VLANs

1 Open the **VLAN Membership** page.

2 Click **Add**.

The **Create New VLAN** page opens.

3 Enter the VLAN ID and name.

4 Click **Apply Changes**.

The new VLAN is added, and the device is updated.

Modifying VLAN Membership Groups

1 Open the **VLAN Membership** page.

2 Select a VLAN from the **Show VLAN** drop-down menu.

3 Modify the fields as desired.

4 Click **Apply Changes**.

The VLAN membership information is modified, and the device is updated.

Deleting VLAN Membership Groups

1 Open the **VLAN Membership** page.

2 Select a VLAN in the **Show VLAN** field.

3 Select the **Remove VLAN** check box.

4 Click **Apply Changes**.

The selected VLAN is deleted, and the device is updated.

Defining VLAN Membership Groups Using CLI Commands

The following table summarizes the equivalent CLI commands for defining VLAN membership groups as displayed in the **VLAN Membership** page.

Table 7-64. VLAN Membership Group CLI Commands

CLI Command	Description
`vlan database`	Enters the interface configuration (VLAN) mode.
`vlan {`*`vlan-range`*`}`	Creates a VLAN.
name *`string`*	Adds a name to a VLAN.

The following is an example of the CLI commands:

```
console(config)# vlan database
console(config-vlan)# vlan 1972
console(config-vlan)# exit
console(config)# interface vlan 1972
console(config-if)# name Marketing
console(config-if)# exit
console(config)#
```

VLAN Port Membership Table

The **VLAN Port Membership Table** contains a Port Table for assigning ports to VLANs. Ports are assigned VLAN membership by toggling through the Port Control settings. Ports can have the following values:

Table 7-65. VLAN Port Membership Table

Port Control	Definition
`T`	The interface is a member of a VLAN. All packets forwarded by the interface are tagged. The packets contain VLAN information.
`U`	The interface is a VLAN member. Packets forwarded by the interface are untagged.
`F`	The interface is denied membership to a VLAN.
`Blank`	The interface is not a VLAN member. Packets associated with the interface are not forwarded.

NOTE: Ports which are LAG members are not displayed in the VLAN Port Membership Table.

The **VLAN Port Membership Table** displays the ports and the ports states, as well as LAGs.

Assigning Ports to a VLAN Group

1. Open the **VLAN Membership** page.
2. Click the **VLAN ID** or **VLAN Name** option button and select a VLAN from the drop-down menu.
3. Select a port in the **Port Membership Table**, and assign the port a value.
4. Click **Apply Changes**.

   The port is assigned to the VLAN group, and the device is updated.

Deleting a VLAN

1. Open the **VLAN Membership** page.
2. Click the **VLAN ID** or **VLAN Name** option button and select a VLAN from the drop-down menu.
3. Select the **Remove VLAN** check box.
4. Click **Apply Changes**.

   The selected VLAN is deleted, and the device is updated.

Assigning Ports to VLAN Groups Using CLI Commands

The following table summarizes the equivalent CLI commands for assigning ports to VLAN groups.

Table 7-66. Port-to-VLAN Group Assignments CLI Commands

CLI Command	Description
switchport general acceptable-frame-types tagged-only	Discards untagged frames at ingress.
switchport forbidden vlan {add *vlan-list* | **remove** *vlan-list*}	Forbids adding specific VLANs to the port.
switchport mode {**access** | **trunk** | **general**}	Configures the VLAN membership mode of a port.
switchport access vlan *vlan-id*	Configures the VLAN ID when the interface is in access mode.
switchport trunk allowed vlan {**add** *vlan-list* | **remove** *vlan-list*}	Adds or removes VLANs from a trunk port.
switchport trunk native vlan *vlan-id*	Defines the port as a member of the specified VLAN, and the VLAN ID as the "port default VLAN ID (PVID)".

Table 7-66. Port-to-VLAN Group Assignments CLI Commands

CLI Command	Description
switchport general allowed vlan add *vlan-list* [**tagged** | **untagged**]	Adds or removes VLANs from a general port.
switchport general pvid vlan-id	Configures the PVID when the interface is in general mode.

The following is an example of the CLI commands:

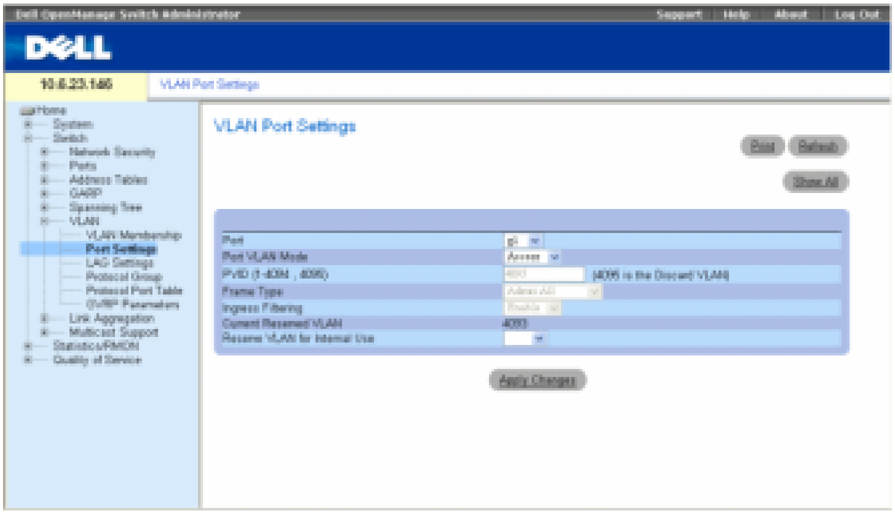
```
Console (config)# vlan database
Console (config-vlan)# vlan 23-25
Console (config-vlan)# exit
Console (config)# interface vlan 23
Console (config-if)# name Marketing
Console (config-if)# exit
Console (config)# interface ethernet g8
Console (config-if)# switchport mode access
Console (config-if)# switchport access vlan 23

Console (config-if)# exit
Console (config)# interface ethernet g9
Console (config-if)# switchport mode trunk
Console (config-if)# swithport mode trunk allowed
vlan add 23-25

Console (config-if)# exit
Console (config)# interface ethernet g10
Console (config-if)# switchport mode general
Console (config-if)# switchport general allowed vlan
add 23,25 tagged
Console (config-if)# switchport general pvid 25
```

Defining VLAN Ports Settings

The **VLAN Port Settings** page contains fields for managing ports that are part of a VLAN. The port default VLAN ID (PVID) is configured on the **VLAN Port Settings** page. All untagged packets arriving to the device are tagged by the ports PVID.

To open the **VLAN Port Settings** page, click **Switch→VLAN→Port Settings** in the tree view.

Figure 7-103. VLAN Port Settings



VLAN Port Settings

Port	g1
Port VLAN Mode	Access
PVID (1-4094 , 4095)	[illegible] (4095 is the Discard VLAN)
Frame Type	Admit All
Ingress Filtering	[illegible]
Current Reserved VLAN	4093
Reserve VLAN for Internal Use	

Port — The port number included in the VLAN.

Port VLAN Mode — The port mode. Possible values are:

General — The port belongs to VLANs, and each VLAN is user-defined as tagged or untagged (full 802.1Q mode).

Access — The port belongs to a single untagged VLAN. When a port is in Access mode, the packet types which are accepted on the port cannot be designated. Ingress filtering cannot be enabled/disabled on an access port.

Trunk — The port belongs to VLANs in which all ports are tagged (except for one port that can be untagged).

PVID — Assigns a VLAN ID to untagged packets. The possible values are 1-4094. VLAN 4095 is defined as per standard and industry practice as the discard VLAN. Packets classified to the Discard VLAN are dropped.

Frame Type — Packet type accepted on the port. Possible values are:

Admit Tag Only — Only tagged packets are accepted on the port.

Admit All — Both tagged and untagged packets are accepted on the port.

Ingress Filtering — Enables or disables Ingress filtering on the port. Ingress filtering discards packets that are destined to VLANs of which the specific LAG is not a member.

Current Reserve VLAN — The VLAN currently designated by the system as the reserved VLAN.

Reserve VLAN for Internal Use — The VLAN selected by the user to be the reserved VLAN if not in use by the system.

Assigning Port Settings

1. Open the **VLAN Port Settings** page.
2. Select the port to which settings need to be assigned from the **Port** drop-down menu.
3. Complete the remaining fields on the page
4. Click **Apply Changes**.

   The VLAN port settings are defined, and the device is updated.

Displaying the VLAN Port Table

1. Open the **VLAN Port Settings** page.
2. Click **Show All.**

   The **VLAN Port Table** opens.

Assigning Ports to VLAN Groups Using CLI Commands

The following table summarizes the equivalent CLI commands for assigning ports to VLAN groups.

Table 7-67. VLAN Port CLI Commands

CLI Command	Description
switchport mode {access | trunk | general}	Configures a port VLAN membership mode.
switchport trunk native vlan *vlan-id*	Defines the port as a member of the specified VLAN, and the VLAN ID as the "port default VLAN ID (PVID)".
switchport general pvid *vlan-id*	Configure the Port VLAN ID (PVID) when the interface is in general mode.
switchport general allowed vlan add *vlan-list* **[tagged | untagged]**	Adds or removes VLANs from a general port.
switchport general acceptable-frame-types tagged-only	Discards untagged packets at ingress.
switchport general ingress-filtering disable	Disables port ingress filtering.

Table 7-67. VLAN Port CLI Commands

CLI Command	Description
shutdown	Disables interfaces.
set interface active {**ethernet** *interface* | **port-channel** *port-channel-number* }	Reactivates an interface that is shutdown due to security reasons.

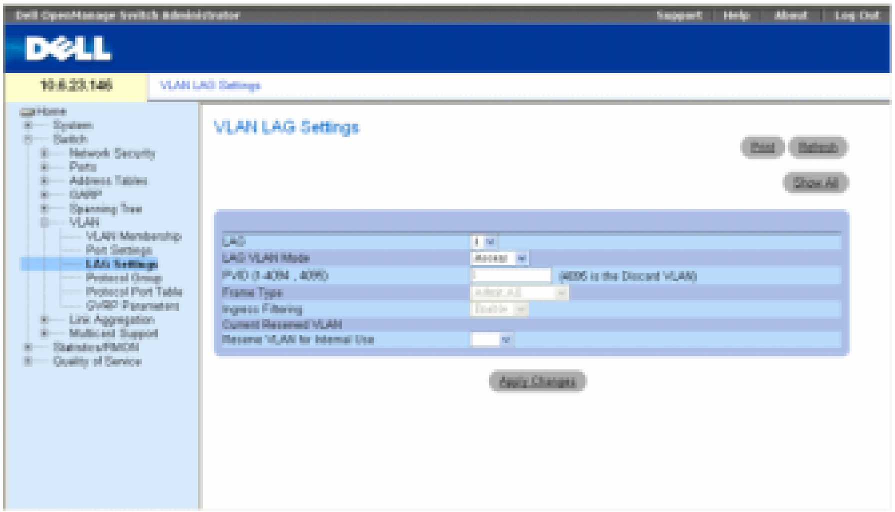
The following is an example of the CLI commands:

```
Console (config)# interface range ethernet g18-20

Console (config-if)# switchport mode access

Console (config-if)# switchport general pvid 234

Console (config-if)# switchport general allowed vlan add
1,2,5,6 tagged

Console (config-if)# switchport general ingress-filtering
disable
```

Defining VLAN LAG Settings

The **VLAN LAG Setting** page provides parameters for managing LAGs that are part of a VLAN. VLANs can either be composed of individual ports or of LAGs. Untagged packets entering the device are tagged with the LAGs ID specified by the PVID. To open the **VLAN LAG Setting** page, click **Switch→VLAN→LAG Settings** in the tree view.

Figure 7-104. VLAN LAG Setting



VLAN LAG Settings

LAG	1
LAG VLAN Mode	Access
PVID (1-4094 , 4095)	1 (4095 is the Discard VLAN)
Frame Type	Admit All
Ingress Filtering	Disable
Current Reserved VLAN	
Reserve VLAN for Internal Use	

LAG — The LAG number included in the VLAN.

LAG VLAN Mode — The LAG VLAN mode. Possible values are:

General — The LAG belongs to VLANs, and each VLAN is user-defined as tagged or untagged (full 802.1Q mode).

Access — The LAG belongs to a single, untagged VLAN.

Trunk — The LAG belongs to VLANs in which all ports are tagged (except for an optional single native VLAN).

PVID — Assigns a VLAN ID to untagged packets. The possible field values are 1-4095. VLAN 4095 is defined as per standard and industry practice, as the discard VLAN. Packets classified to this VLAN are dropped.

Frame Type — Packet type accepted by the LAG. Possible values are:

Admit Tag Only — Only tagged packets are accepted by the LAG.

Admit All — Tagged and untagged packets are both accepted by the LAG.

Ingress Filtering — Enables or disables Ingress filtering by the LAG. Ingress filtering discards packets that are destined to VLANs of which the specific port is not a member.

Current Reserve VLAN — The VLAN currently designated as the reserved VLAN.

Reserve VLAN for Internal Use — The VLAN that is designated as the reserved VLAN after the device is reset.

Assigning VLAN LAG Settings:

1 Open the **VLAN LAG Setting** page.

2 Select a LAG from the **LAG** drop-down menu and complete the fields on the page.

3 Click **Apply Changes**.

The VLAN LAG parameters are defined, and the device is updated.

Displaying the VLAN LAG Table

1 Open the **VLAN LAG Setting** page.

2 Click **Show All**.

The **VLAN LAG Table** opens.

Assigning LAGs to VLAN Groups Using CLI Commands

The following table summarizes the equivalent CLI commands for assigning LAGs to VLAN groups as displayed in the **VLAN LAG Setting** page.

Table 7-68. LAG VLAN Assignments CLI Commands

CLI Command	Description
switchport mode {access | trunk | general}	Configures a port VLAN membership mode.
switchport trunk native vlan *vlan-id*	Defines the port as a member of the specified VLAN, and the VLAN ID as the port default VLAN ID (PVID).
switchport general pvid *vlan-id*	Configure the Port VLAN ID (PVID) when the interface is in general mode.
switchport general allowed vlan add *vlan-list* **[tagged | untagged]**	Adds or removes VLANs from a general port.
switchport general acceptable-frame-type tagged-only	Discards untagged packets at ingress.
switchport general ingress-filtering disable	Disables port ingress filtering.

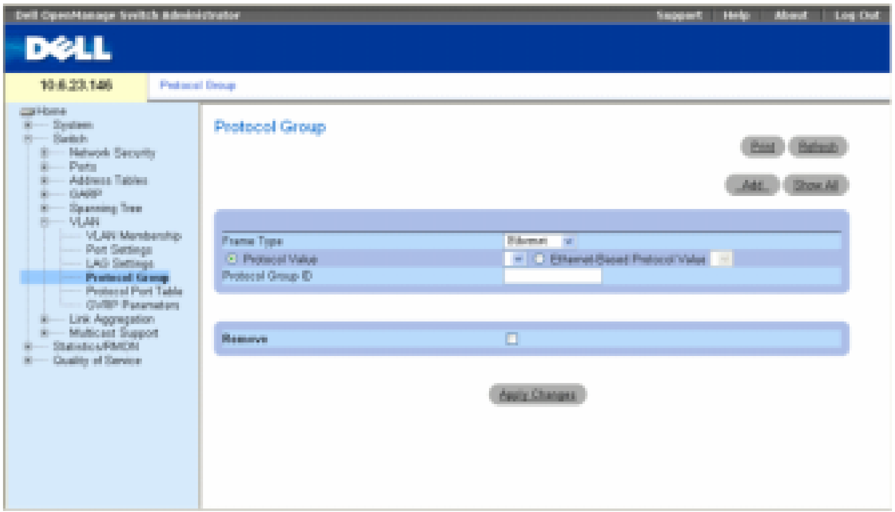
The following is an example of the CLI commands:

```
console(config)# interface port-channel 1
console(config-if)# switchport mode access
console(config-if)# switchport access vlan 2
console(config-if)# exit

console(config)# interface port-channel 2
console(config-if)# switchport mode general
console(config-if)# switchport general allowed vlan add 2-3
tagged
console(config-if)# switchport general pvid 2
console(config-if)# switchport general acceptable-frame-type
tagged-only
console(config-if)# switchport general ingress-filtering
disable
console(config-if)# exit

console(config)# interface port-channel 3
console(config-if)# switchport mode trunk
console(config-if)# switchport trunk native vlan 3
console(config-if)# switchport trunk allowed vlan add 2
console(config-if)# exit
```

Defining VLAN Protocol Groups

The **Protocol Group** page provides parameters for configuring frame types to specific protocol groups. To open the **Protocol Group** page, click **Switch→VLAN→Protocol Group** in the tree view.

Figure 7-105. Protocol Group



Frame Type: Ethernet

● Protocol Value ○ Ethernet-Based Protocol Value

Protocol Group ID

Remove □

Frame Type — The packet type. Possible field values are **Ethernet**, **RFC1042**, and **LLC Other**.

Protocol Value — User-defined protocol name.

Ethernet-Based Protocol Value — The Ethernet protocol group type. The possible field values are **IP**, **IPX** and **IPV6**..

Protocol Group ID — The VLAN Group ID number.

Remove —

Adding a Protocol Group

1. Open the **Protocol Group** page.
2. Click **Add.**

   The **Add Protocol to Group** page opens.
3. Complete the fields on the page.
4. Click **Apply Changes**.

   The protocol group is assigned, and the device is updated.

Assigning VLAN Protocol Group Settings

1. Open the **Protocol Group** page.
2. Complete the fields on the page.
3. Click **Apply Changes**.

   The VLAN protocol group parameters are defined, and the device is updated.

Removing Protocols From the Protocol Group Table

1. Open the **Protocol Group** page.
2. Click **Show All**.

   The **Protocol Group Table** opens.

3. Select **Remove** for the protocol groups that need to be removed.
4. Click **Apply Changes**.

   The protocol is removed, and the device is updated.

Defining VLAN Protocol Groups Using CLI Commands

The following table summarizes the equivalent CLI commands for configuring Protocol Groups.

Table 7-69. VLAN Protocol Groups CLI Commands

CLI Command	Description
map protocol *protocol [encapsulation]* **protocols-group** *group*	

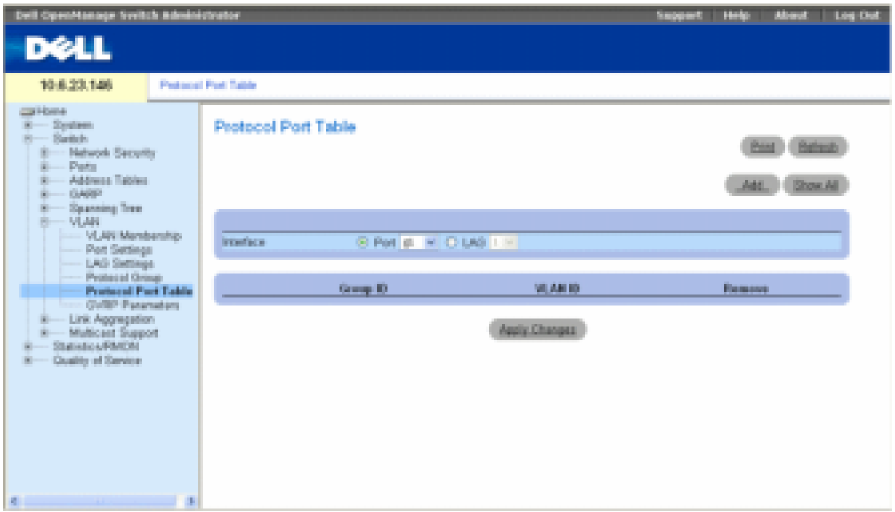
The following example maps ip-arp protocol to group "213":

```
Console (config)# vlan database
Console (config-vlan)# map protocol ip-arp protocols-group 213
```

Adding Protocol Ports

The **Protocol Port** page adds interfaces to Protocol groups. To open the **Protocol Port** page, click **Switch→VLAN→Protocol Port** in the tree view.

Figure 7-106. Protocol Port



Interface — Port or LAG number added to a protocol group.

Group ID — Protocol group ID to which the interface is added. Protocol group IDs are defined in the Protocol Group Table.

VLAN ID (1-4095) — Attaches the interface to a user-defined VLAN ID. The VLAN ID is defined on the **Create a New VLAN** page. Protocol ports can either be attached to a VLAN ID or a VLAN name.

NOTE: VLAN 4095 is the discard VLAN.

Adding a New Protocol Port

NOTE: Protocol ports can be defined only on ports that are defined as **General** in the **VLAN Port Settings** page.

1. Open the **Protocol Port** page.
2. Click **Add**.

   The **Add Protocol Port** page opens.
3. Complete the fields in the dialog.
4. Click **Apply Changes**.

   The new VLAN protocol group is added to the **Protocol Port Table**, and the device is updated.

Defining Protocol Ports Using CLI Commands

The following table summarizes the equivalent CLI command for for defining Protocol Ports.

Table 7-70. Protocol Port CLI Commands

CLI Command	Description
switchport general map protocols-group *group* **vlan** *vlan-id*	Sets a protocol-based classification rule.

The following example sets a protocol-based classification rule of protocol group 1 to VLAN 8:

```
Console (config-if)# switchport general map protocols-group 1
vlan 8
```

Configuring GVRP

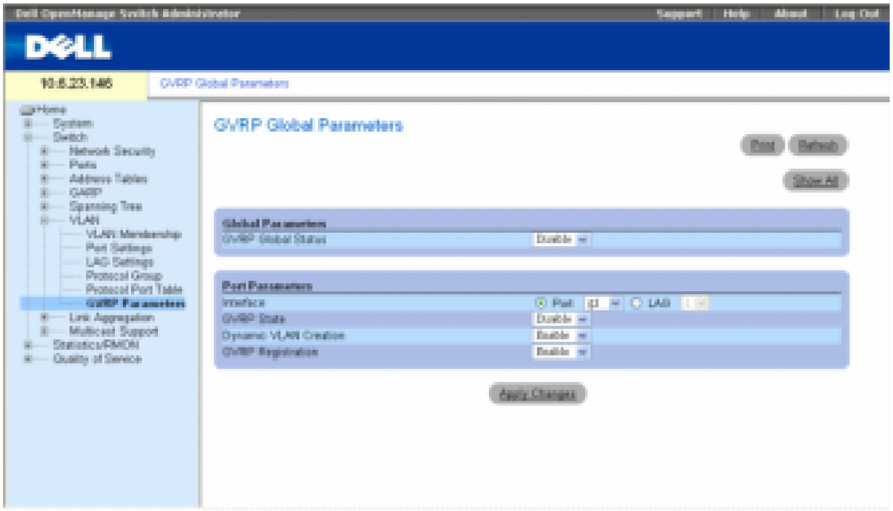
GARP VLAN Registration Protocol (GVRP) is specifically provided for automatic distribution of VLAN membership information among VLAN-aware bridges. GVRP allows VLAN-aware bridges to automatically learn VLANs to bridge ports mapping, without having to individually configure each bridge and register VLAN membership.

To ensure the correct operation of the GVRP protocol, it is advised to set the maximum number of GVRP VLANs equal to a value which significantly exceeds the sum of:

- The number of all static VLANs both currently configured and expected to be configured.
- The number of all dynamic VLANs participating in GVRP, both currently configured (initial number of dynamic GVRP VLANs is 128) and expected to be configured.

The **GVRP Global Parameters** page enables GVRP globally. GVRP can also be enabled on a per-interface basis. To open the **GVRP Parameters** page, click **Switch→VLAN→GVRP Parameters** in the tree view.

Figure 7-107. GVRP Parameters



GVRP Global Parameters

Global Parameters

GVRP Global Status: Disable

Port Parameters

Interface: ● Port g1 ○ LAG 1

GVRP State: Disable

Dynamic VLAN Creation: Enable

GVRP Registration: Enable

GVRP Global Status — Enables or disables GVRP on the device. GVRP is disabled by default.

Interface — The port or LAG for which GVRP is enabled.

GVRP State — Enables or disables GVRP on an interface.

Dynamic VLAN Creation — Enables or disables VLAN creation through GVRP.

GVRP Registration — The GVRP Registration status.

Enabling GVRP on the Device

1. Open the **GVRP Global Parameters** page.
2. Select **Enable** in the **GVRP Global Status** field.
3. Click **Apply Changes**.

   GVRP is enabled on the device.

Enabling VLAN Registration Through GVRP

1. Open the **GVRP Global Parameters** page.
2. Select **Enable** in the **GVRP Global Status** field for the desired interface.
3. Select **Enable** in the **GVRP Registration** field.
4. Click **Apply Changes**.

GVRP VLAN Registration is enabled on the port, and the device is updated.

Configuring GVRP Using CLI Commands

The following table summarizes the equivalent CLI commands for configuring GVRP as displayed in the **GVRP Global Parameters** page.

Table 7-71. GVRP Global Parameters CLI Commands

CLI Command	Description
gvrp enable (global)	Enables GVRP globally.
gvrp enable (interface)	Enables GVRP on an interface.
gvrp vlan-creation-forbid	Enables or disables dynamic VLAN creation.
gvrp registration-forbid	De-registers all dynamic VLANs, and prevents dynamic VLAN registration on the port.
show gvrp configuration [**ethernet** *interface* | **port-channel** *port-channel-number*]	Displays GVRP configuration information, including timer values, whether GVRP and dynamic VLAN creation is enabled, and which ports are running GVRP.
show gvrp error-statistics [**ethernet** *interface* | **port-channel** *port-channel-number*]	Displays GVRP error statistics.
show gvrp statistics [**ethernet** *interface* | **port-channel** *port-channel-number*]	Displays GVRP statistics.
clear gvrp statistics [**ethernet** *interface* | **port-channel** *port-channel-number*]	Clears all the GVRP statistics information.

The following is an example of the CLI commands:

```
console(config)# gvrp enable
console(config)# interface ethernet g1
console(config-if)# gvrp enable
console(config-if)# gvrp vlan-creation-forbid
console(config-if)# gvrp registration-forbid
console(config-if)# end
console# show gvrp configuration


GVRP Feature is currently Enabled on the device.
Maximum VLANs: 223


Port(s)  GVRP-     Registration  Dynamic    Timers         Leave    Leave
         Status                  VLAN       (milliseconds)          All
                                 Creation   Join
-------  ------    ------------  --------   -------------- -----    -----
g1       Enabled   Forbidden     Disabled   200            900      10000
g2       Disabled  Normal        Enabled    200            600      10000
```

Aggregating Ports

Port Aggregation optimizes port usage by linking a group of ports together to form a single Link Aggregated Groups (LAGs). Port Aggregation multiplies the bandwidth between the devices, increases port flexibility, and provides link redundancy. The device supports up to eight LAGs per system, and eight ports per LAG per device.

Each LAG is composed of ports of the same speed, set to full-duplex operations. Ports in a LAG, can be of different media types (UTP/Fiber, or different fiber types), provided they operate at the same speed.

Aggregated Links can be assigned manually or automatically by enabling Link Aggregation Control Protocol (LACP) on the relevant links. The device provides LAG Load Balancing based on both source MAC addresses and destination MAC addresses.

Aggregated Links are treated by the system as a single logical port. Specifically, the Aggregated Link has similar port attributes to a non-aggregated port, including auto-negotiation, speed, Duplex setting, etc.

The device supports both static LAGs and Link Aggregation Control Protocol (LACP) LAGs. LACP LAG negotiate Aggregated Port links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establish a LAG between them.

The following guidelines should be followed when adding ports to a LAG:

- There is no Layer 3 interface defined on the port.
- The port does not belong to any VLAN.
- The port does not belong to any other LAG.
- The port is not a mirrored port.
- The port's 802.1p priority is equal to LAGs 802.1p priority.
- QoS Trust is not disabled on the port.
- GVRP is not enabled.

NOTE: Ports can be configured as LACP ports only if the ports are not part of a previously configured LAG.

The device uses a hash function to determine which frames are carried on which aggregated-link member. The hash function statistically load-balances the aggregated link members. The device considers an Aggregated Link as a single logical port.

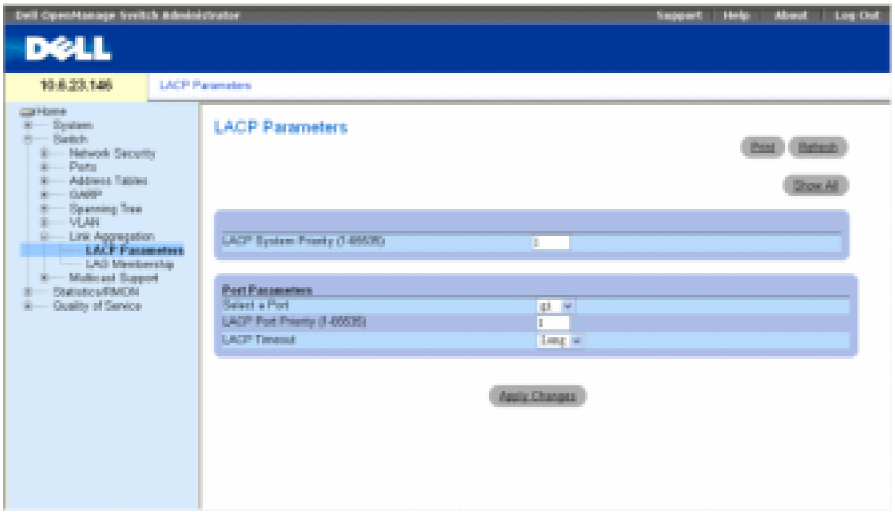
Each Aggregated Link has an Aggregated Link Port Type, including Gigabit Ethernet ports. Ports can be added to an Aggregated Link only if they are the same port type. When ports are removed from an Aggregated Links, the ports revert to the original port settings. To open the **Link Aggregation** page, click **Switch→Link Aggregation** in the tree view.

Defining LACP Parameters

The **LACP Parameters** page contains fields for configuring LACP LAGs. Aggregate ports can be linked into link-aggregation port-groups. Each group is comprised of ports with the same speed.

Aggregated Links can be manually setup or automatically established by enabling Link Aggregation Control Protocol (LACP) on the relevant links. To open the **LACP Parameters** page, click **Switch→ Link Aggregation→LACP Parameters** in the tree view.

Figure 7-108. LACP Parameters



LACP Parameters

LACP System Priority (1-65535) 1

Port Parameters

Select a Port g1

LACP Port Priority (1-65535) 1

LACP Timeout Long

LACP System Priority (1-65535) — The LACP priority value for global settings. The possible range is 1- 65535. The default value is 1.

Select a Port — The port number to which timeout and priority values are assigned.

LACP Port Priority (1-65535) — LACP priority value for the port.

LACP Timeout — Administrative LACP timeout. The possible field values are:

- **Short** — Specifies a short timeout value.
- **Long** — Specifies a long timeout value.

Defining Link Aggregation Global Parameters

1 Open the **LACP Parameters** page.

2 Complete the **LACP System Priority** field.

3 Click **Apply Changes**.

The parameters are defined, and the device is updated.

Defining Link Aggregation Port Parameters

1 Open the **LACP Parameters** page.

2 Complete the fields in the **Port Parameters** area.

3 Click **Apply Changes**.

The parameters are defined, and the device is updated.

Displaying the LACP Parameters Table

1 Open the **LACP Parameters** page.

2 Click **Show All**.

The **LACP Parameters Table** opens.

Configuring LACP Parameters Using CLI Commands

The following table summarizes the equivalent CLI commands for configuring LACP parameters as displayed in the **LACP Parameters** page.

Table 7-72. LACP Parameters CLI Commands

CLI Command	Description
lacp system-priority *value*	Configures the system priority.
lacp port-priority *value*	Configures the priority value for physical ports.
lacp timeout {long | short}	Assigns an administrative LACP timeout.
show lacp ethernet *interface* **[parameters | statistics | protocol-state]**	Displays LACP information for ethernet ports.

The following is an example of the CLI commands:

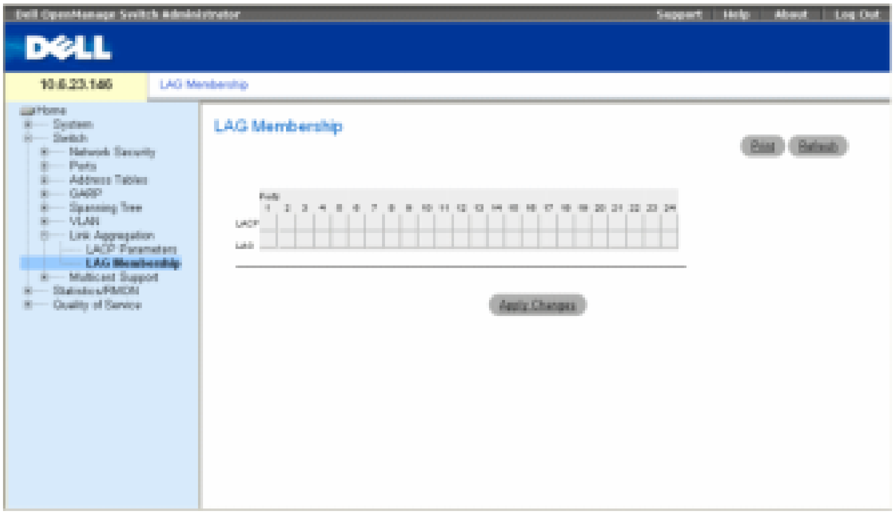
```
Console (config)# lacp system-priority 120
Console (config)# interface ethernet g1
Console (config-if)# lacp port-priority 247
Console (config-if)# lacp timeout long
Console (config-if)# end
Console# show lacp ethernet g1 statistics
Port g1 LACP Statistics:
LACP PDUs sent:2
LACP PDUs received:2
```

Defining LAG Membership

The **LAG Membership** page contains fields for assigning ports to LAGs. LAGs can include up to 8 ports.When a port is added to a LAG, the port acquires the LAG's properties.

The **LAG Membership** page contains fields for assigning ports to LAGs. To open the **LAG Membership** page, click **Switch→Link Aggregation→LAG Membership** in the tree view.

Figure 7-109. LAG Membership



LACP — Aggregates the port to a LAG, using LACP.

LAG — Adds a port to a LAG, and indicates the specific LAG to which the port belongs.

Configuring a Port to a LAG or LACP

1. Open the **LAG Membership** page.
2. In the LAG row (the second row), toggle the button to a specific number to aggregate or remove the port to that LAG number.
3. In the LACP row (the first row), toggle the button under the port number to assign either the LACP or the static LAG.
4. Click **Apply Changes**.

   The port is added to the LAG or LACP, and the device is updated.

Assigning Ports to LAGs Using CLI Commands

The following table summarizes the equivalent CLI commands for assigning ports to LAGs as displayed in the **LAG Membership** page.

Table 7-73. LAG Membership CLI Commands

CLI Command	Description
interface port-channel *port-channel-number*	Enters the interface configuration mode of a specific port-channel.
channel-group *port-channel-number* **mode** {**on** | **auto**}	Associates a port with a port-channel. Use the no form of this command to remove the channel-group configuration from the interface.
show interfaces port-channel [*port-channel-number*]	Displays port-channel information.

The following is an example of the CLI commands:

```
console# config
console(config)# interface ethernet g1
console(config-if)# channel-group 1 mode on
console(config-if)# 01-Jan-2000 01:47:18 %LINK-W-Down: ch1

console(config-if)#
```

Multicast Forwarding Support

Multicast forwarding allows a single packet to be forwarded to multiple destinations. L2 Multicast service is based on L2 switch receiving a single packet addressed to a specific Multicast address. Multicast forwarding creates copies of the packet, and transmits the packets to the relevant ports.

The device supports:

- **Forwarding L2 Multicast Packets** — Enabled by default, and not configurable.

NOTE: The system supports Multicast filtering for 63 Multicast groups.

- **Filtering L2 Multicast Packets** — Enables forwarding of Layer 2 packets to interfaces. If Multicast filtering is disabled, Multicast packets are flooded to all relevant ports.

To open the **Multicast Support** page, click **Switch→Multicast Support** in the tree view.

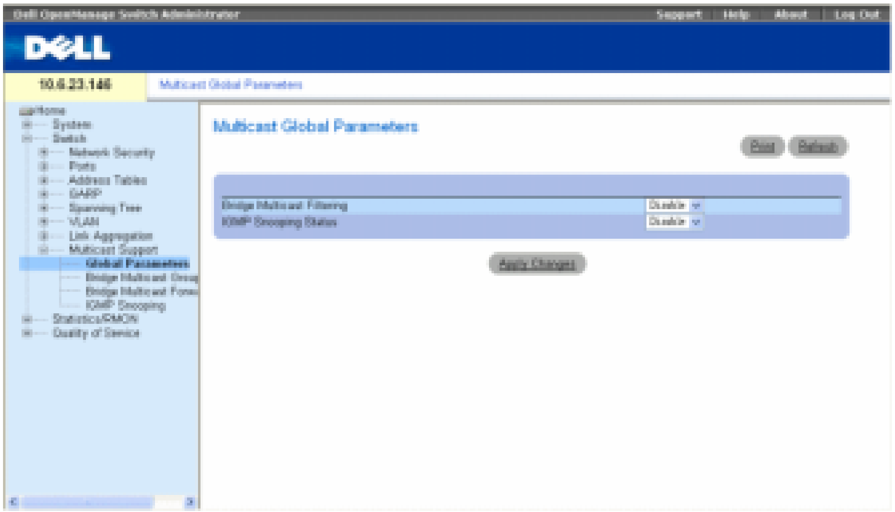
Defining Multicast Global Parameters

Layer 2 switching forwards Multicast packets to all relevant VLAN ports by default, treating the packet as a Multicast transmission. While this is functional, in the sense that all relevant ports/nodes receive a copy of the frame, it is potentially wasteful as ports/nodes may receive irrelevant frames only needed by a subset of the ports of that VLAN. Multicast forwarding filters enable forwarding of Layer 2 packets to port subsets, defined in the Multicast filter database.

When IGMP snooping is enabled globally, the switching ASIC is programmed to forward all IGMP packets to the CPU. The CPU analyzes the incoming packets and determines which ports are to join which Multicast groups, which ports have Multicast routers generating IGMP queries, and what routing protocols are forwarding packets and Multicast traffic. Ports requesting to join a specific Multicast group issues an IGMP report specifying that Multicast group. This results in the creation of the Multicast filtering database.

The **Multicast Global Parameters** page contains fields for enabling IGMP Snooping on the device. To open the **Multicast Global Parameters** page, click **Switch→Multicast Support→Global Parameters** in the tree view.

Figure 7-110. Multicast Global Parameters



Bridge Multicast Filtering Disable

IGMP Snooping Status Disable

Bridge Multicast Filtering — Enables or disables bridge Multicast filtering. Disabled is the default value.

IGMP Snooping Status — Enables or disables IGMP Snooping on the device. Disabled is the default value.

Enabling Bridge Multicast Filtering on the Device

1. Open the **Multicast Global Parameters** page.
2. Select **Enable** in the **Bridge Multicast Filtering** field.
3. Click **Apply Changes**.

Bridge Multicast is enabled on the device.

Enabling IGMP Snooping on the Device

1. Open the **Multicast Global Parameters** page.
2. Select **Enable** in the **IGMP Snooping Status** field.
3. Click **Apply Changes**.

   IGMP Snooping is enabled on the device.

Enabling Multicast Forwarding and IGMP Snooping Using CLI Commands

The following table summarizes the equivalent CLI commands for enabling Multicast forwarding and IGMP Snooping as displayed on the **Multicast Global Parameters** page.

Table 7-74. Multicast Forwarding and Snooping CLI Commands

CLI Command	Description
bridge multicast filtering	Enables filtering of Multicast addresses.
ip igmp snooping	Enables Internet Group Membership Protocol (IGMP) snooping.

The following is an example of the CLI commands:

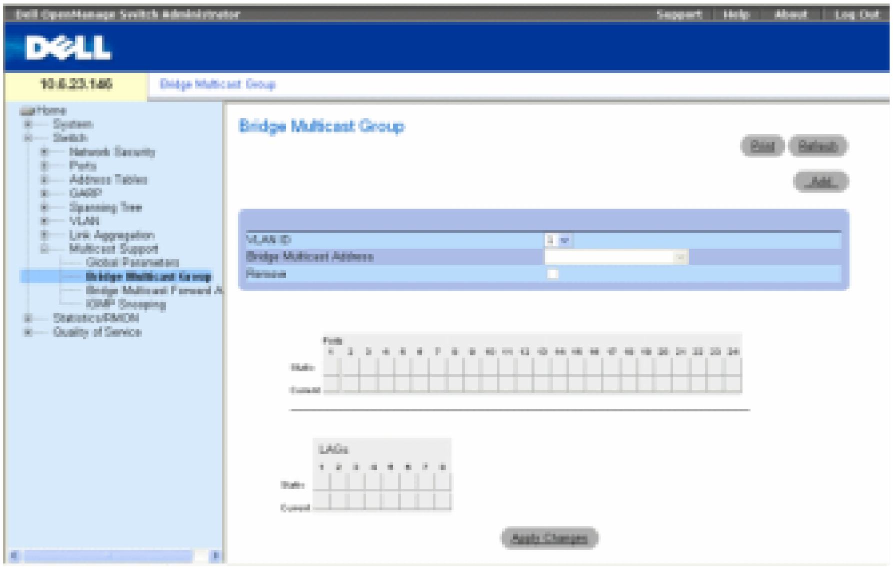
```
Console (config)# bridge multicast filtering
Console (config)# ip igmp snooping
```

Adding Bridge Multicast Address Members

The **Bridge Multicast Group** page displays the ports and LAGs attached to the Multicast service group in the **Ports** and **LAGs** tables. The Port and LAG tables also reflect the manner in which the port or LAGs joined the Multicast group. Ports can be added either to existing groups or to new Multicast service groups. The **Bridge Multicast Group** page permits new Multicast service groups to be created. The **Bridge Multicast Group** page also assigns ports to a specific Multicast service address group.

To open the **Bridge Multicast Group** page, click **Switch→Multicast Support→Bridge Multicast Address** in the tree view.

Figure 7-111. Bridge Multicast Group



Bridge Multicast Group

VLAN ID	1
Bridge Multicast Address	
Remove	□

Ports

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Static																								
Current																								

LAGs

	1	2	3	4	5	6	7	8
Static								
Current								

VLAN ID — Identifies a VLAN and contains information about the Multicast group address.

Bridge Multicast Address — Identifies the Multicast group MAC address/IP address.

Remove — When selected, removes a Bridge Multicast address.

Ports — Port that can be added to a Multicast service.

LAGs — LAGs that can be added to a Multicast service.

The following table contains the IGMP port and LAG members management settings:

Table 7-75. IGMP Port/LAG Members Table Control Settings

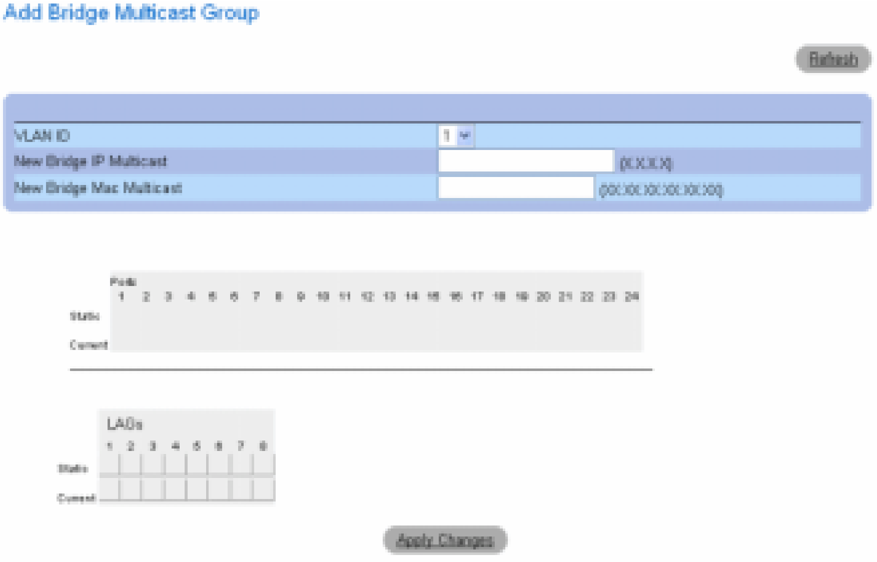
Port Control	Definition
D	The port/LAG has joined the Multicast group dynamically in the Current Row.
S	Attaches the port to the Multicast group as static member in the Static Row. The port/LAG has joined the Multicast group statically in the Current Row.
F	Forbidden.
Blank	The port is not attached to a Multicast group.

Adding Bridge Multicast Addresses

1. Open the **Bridge Multicast Group** page.
2. Click **Add**.

   The **Add Bridge Multicast Group** page opens:

Figure 7-112. Add Bridge Multicast Group



Add Bridge Multicast Group

VLAN ID: 1

New Bridge IP Multicast: (X.X.X.X)

New Bridge Mac Multicast: (XX:XX:XX:XX:XX:XX)

3. Define the **VLAN ID** and **New Bridge Multicast Address** fields.
4. Toggle a port to **S** to join the port to the selected Multicast group.
5. Toggle a port to **F** to forbid adding specific Multicast addresses to a specific port.

6 Click **Apply Changes**.

The bridge Multicast address is assigned to the Multicast group, and the device is updated.

Defining Ports to Receive Multicast Service

1 Open the **Bridge Multicast Group** page.

2 Define the **VLAN ID** and the **Bridge Multicast Address** fields.

3 Toggle a port to **S** to join the port to the selected Multicast group.

4 Toggle a port to **F** to forbid adding specific Multicast addresses to a specific port.

5 Click **Apply Changes**.

The port is assigned to the Multicast group, and the device is updated.

Assigning LAGs to Receive Multicast Service

1 Open the **Bridge Multicast Group** page.

2 Define the **VLAN ID** and the **Bridge Multicast Address** fields.

3 Toggle the LAG to **S** to join the LAG to the selected Multicast group.

4 Toggle the LAG to **F** to forbid adding specific Multicast addresses to a specific LAG.

5 Click **Apply Changes**.

The LAG is assigned to the Multicast group, and the device is updated.

Managing Multicast Service Members Using CLI Commands

The following table summarizes the equivalent CLI commands for managing Multicast service members as displayed in the **Bridge Multicast Group** page.

Table 7-76. Multicast Service Member CLI Commands

CLI Command	Description
bridge multicast address {*mac-multicast-address* | *ip-multicast-address*}	Registers MAC-layer Multicast addresses to the bridge table, and adds static ports to the group.
bridge multicast forbidden address {*mac-multicast-address* | *ip-multicast-address*}[**add** | **remove**] {**ethernet** *interface-list* | **port-channel** *port-channel-number-list*}	Forbids adding a specific Multicast address to specific ports. Use the no form of this command to return to default
show bridge multicast address-table [**vlan** *vlan-id*] [**address** *mac-multicast-address* | *ip-multicast-address*] [**format ip** | **mac**]	Displays Multicast MAC address table information.

The following is an example of the CLI commands:

```
Console> enable
Console# config
console(config)#vlan database
console(config-if)#vlan 8
console(config-if)#exit
console(config)#interface range ethernet g1-9
console(config-if)# switchport mode general
console(config-if)# switchport general allow vlan add 8
console(config)#interface vlan 8
console (config-if)# exit
Console(config-if)# bridge multicast address 0100.5e02.0203
add ethernet g1,g2
Console(config-if)# exit
Console(config)# exit
Console # show bridge multicast address-table

Vlan     MAC Address            Type              Ports
----     -----------            -----             ----------
1        0100.5e02.0203         static            g1, g2
19       0100.5e02.0208         static            g1-8
19       0100.5e02.0208         dynamic           g9-11

Forbidden ports for multicast addresses:

Vlan     MAC Address            Ports
----     -----------            ----------
1        0100.5e02.0203         g8
19       0100.5e02.0208         g8
```

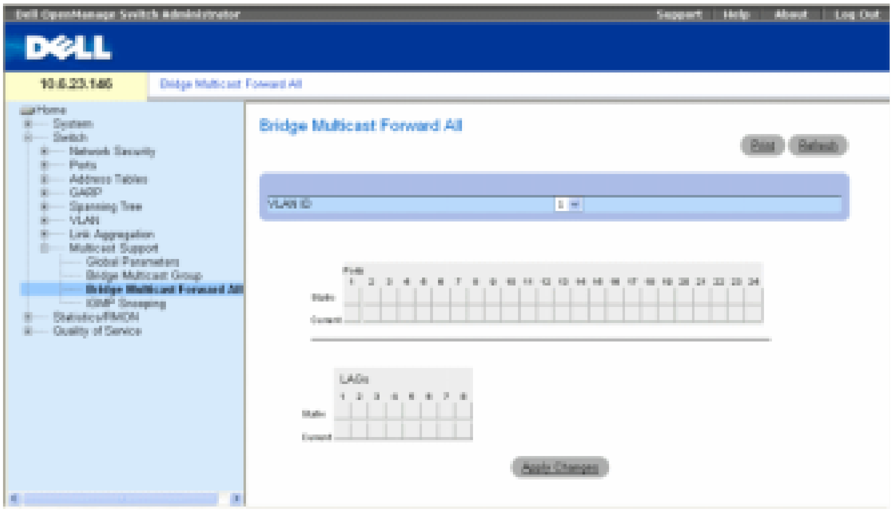
```
Console # show bridge multicast address-table format ip

Vlan     IP Address            Type              Ports
----     -----------           -----             ----------
1        224-239.130|2.2.3     static            g1, g2
19       224-239.130|2.2.8     static            g1-8
19       224-239.130|2.2.8     dynamic           g9-11

Forbidden ports for multicast addresses:

Vlan     IP Address            Ports
----     -----------           ----------
1        224-239.130|2.2.3     g8
19       224-239.130|2.2.8     g8
```

Assigning Multicast Forward All Parameters

The **Bridge Multicast Forward All** page contains fields for attaching ports or LAGs to a device that is attached to a neighboring Multicast router/switch. Once IGMP Snooping is enabled, Multicast packets are forwarded to the appropriate port or VLAN.

To open the **Bridge Multicast Forward All** page, click **Switch→Multicast Support→Bridge Multicast→Bridge Multicast Forward All** page in the tree view.

Figure 7-113. Bridge Multicast Forward All



VLAN ID 1

Ports	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Static																								
Current																								

LAGs	1	2	3	4	5	6	7	8
Static								
Current								

VLAN ID — Identifies a VLAN.

Ports — Ports that can be added to a Multicast service.

LAGs — LAGs that can be added to a Multicast service.

The **Bridge Multicast Forward All Router/Port Control Settings Table** contains the settings for managing router and port settings.

Table 7-77. Bridge Multicast Forward All Router/Port Control Settings Table

Port Control	Definition
D	Attaches the port to the Multicast router or switch as a dynamic port.
S	Attaches the port to the Multicast router or switch as a static port.
F	Forbidden.
Blank	The port is not attached to a Multicast router or switch.

Attaching a Port to a Multicast Router or Switch

1. Open **Bridge Multicast Forward All** page.
2. Define the **VLAN ID** field.
3. Select a port in the **Ports** table, and assign the port a value.
4. Click **Apply Changes**.

   The port is attached to the Multicast router or switch.

Attaching a LAG to a Multicast Router or Switch

1. Open **Bridge Multicast Forward All** page.
2. Define the **VLAN ID** field.
3. Select a port in the **LAGs** table, and assign the LAG a value.
4. Click **Apply Changes**.

   The LAG is attached to the Multicast router or switch.

Managing LAGs and Ports Attached to Multicast Routers Using CLI Commands

The following table summarizes the equivalent CLI commands for managing LAGs and ports attached to Multicast routers as displayed on the **Bridge Multicast Forward All** page.

Table 7-78. CLI Commands for Managing LAGs and Ports Attached to Multicast Routers

CLI Command	Description
show bridge multicast filtering *vlan-id*	Displays the Multicast filtering configuration.
no bridge multicast forbidden forward-all	Disables forwarding Multicast packets on a port.
bridge multicast forward-all {add | remove} {ethernet *interface-list* **| port-channel** *port-channel-number-list***}**	Enables forwarding of all Multicast packets on a port. Use the no form of this command to return to default.

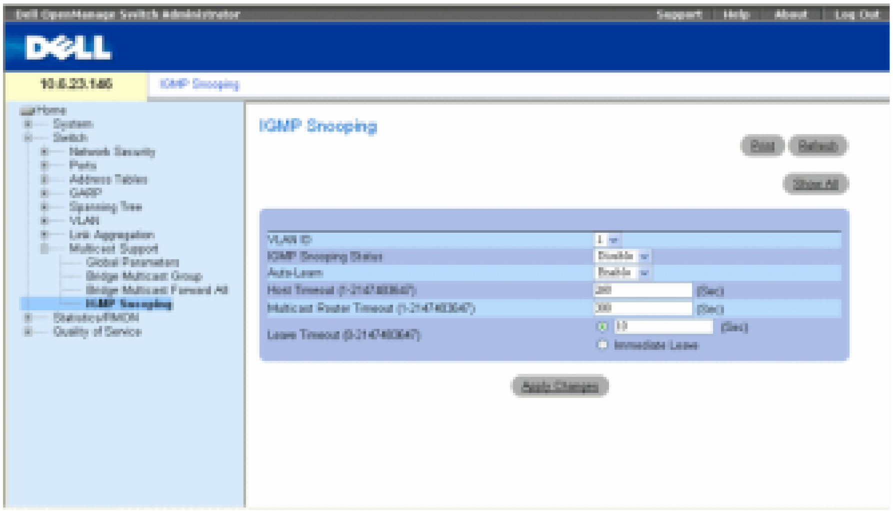
The following is an example of the CLI commands:

```
console(config)#vlan database
console(config-if)#vlan 8
console(config-vlan)#exit
console(config)#interface range ethernet g1-9
console(config-if)# switchport mode general
console(config-if)# switchport general allow vlan add 8
Console(config-if)# exit
console(config)#interface vlan 8
Console(config-if)# bridge multicast address 0100.5e02.0203
add ethernet g1-9
Console(config-if)# exit
Console (config)# interface VLAN 1
Console (config-if)# bridge multicast forward-all add ethernet
g8
Console(config-if)# end
Console # show bridge multicast filtering 1
Filtering: Enabled
VLAN:           Forward-All


Port            Static                  Status
-------         -----------------       -----------
g1              Forbidden               Filter
g2              Forward                 Forward(s)
g3              -                       Forward(d)
```

IGMP Snooping

The **IGMP Snooping** page contains fields for adding IGMP members. To open the **IGMP Snooping** page, click **Switch→Multicast Support→IGMP Snooping** in the tree view.

Figure 7-114. IGMP Snooping



VLAN ID	1	
IGMP Snooping Status	Disable	
Auto-Learn	Enable	
Host Timeout (1-2147483647)	260	(Sec)
Multicast Router Timeout (1-2147483647)	300	(Sec)
Leave Timeout (0-2147483647)	● 10 ○ Immediate Leave	(Sec)

VLAN ID — Specifies the VLAN ID.

IGMP Snooping Status — Enables or disables IGMP snooping on the VLAN.

Auto Learn — Enables or disables Auto Learn on the device.

Host Timeout (1-2147483647) — Time before an IGMP snooping entry is aged out. The default time is 260 seconds.

Multicast Router Timeout (1-2147483647) — Time before aging out a Multicast router entry. The default value is 300 seconds.

Leave Timeout (0-2147483647) — Time, in seconds, after a port leave message is received before the entry is aged out. **User-defined** enables a user-definable timeout period, and **Immediate Leave** specifies an immediate timeout period. The default timeout is 10 seconds.

Enabling IGMP Snooping on the Device

1. Open the **IGMP Snooping** page.
2. Select the VLAN ID for the device on which IGMP snooping needs to be enabled.
3. Select **Enable** in the **IGMP Snooping Status** field.
4. Complete the fields on the page.
5. Click **Apply Changes**.

IGMP snooping is enabled on the device.

Displaying the IGMP Snooping Table

1 Open the **IGMP Snooping**.

2 Click **Show All**.

The **IGMP Snooping Table** opens.

Configuring IGMP Snooping with CLI Commands

The following table summarizes the equivalent CLI commands for configuring IGMP Snooping on the device:

Table 7-79. IGMP Snooping CLI Commands

CLI Command	Description
ip igmp snooping	Enables Internet Group Membership Protocol (IGMP) snooping.
ip igmp snooping mrouter learn-pim-dvmrp	Enables automatic learning of Multicast router ports in the context of a specific VLAN.
ip igmp snooping host-time-out *time-out*	Configures the host-time-out.
ip igmp snooping mrouter-time-out *time-out*	Configures the mrouter-time-out.
ip igmp snooping leave-time-out {*time-out* | *immediate-leave*}	Configures the leave-time-out.
show ip igmp snooping groups [**vlan** *vlan-id*] [**address** *ip-multicast-address*]	Displays the Multicast groups learned by IGMP snooping.
show ip igmp snooping interface *vlan-id*	Displays IGMP snooping configuration.
show ip igmp snooping mrouter [**interface** *vlan-id*]	Displays information about dynamically learned Multicast router interfaces.

The following is an example of the CLI commands:

```
Console> enable
Console# config
Console (config)# ip igmp snooping
Console (config)# interface vlan 1
Console (config-if)# ip igmp snooping mrouter learn-pim-dvmrp
Console (config-if)# ip igmp snooping host-time-out 300
Console (config-if)# ip igmp snooping mrouter-time-out 200
Console (config-if)# exit
Console (config)# interface vlan 1
Console (config-if)# ip igmp snooping leave-time-out 60
Console (config-if)# exit
Console (config)# exit
Console # show ip igmp snooping groups

Vlan            IP Address           Querier     Ports
-----          ------------------   --------     -----
1              224-239.130|2.2.3      Yes        g1, g2
19             224-239.130|2.2.8      Yes        g9-11

Console # show ip igmp snooping interface 1
IGMP Snooping is globally enabled
IGMP Snooping is enabled on VLAN 1
IGMP host timeout is 300 sec
IGMP Immediate leave is disabled. IGMP leave timeout is 60 sec
IGMP mrouter timeout is 200 sec
Automatic learning of multicast router ports is enabled

Console # show ip igmp snooping mrouter
```

```
VLAN            Ports
----            ------
1               g1
```

8

Viewing Statistics

The **Statistic** pages contains device information for interface, GVRP, etherlike, RMON, and device utilization. To open the **Statistics** page, click **Statistics** in the tree view.

NOTE: CLI commands are not available for all the Statistics pages.

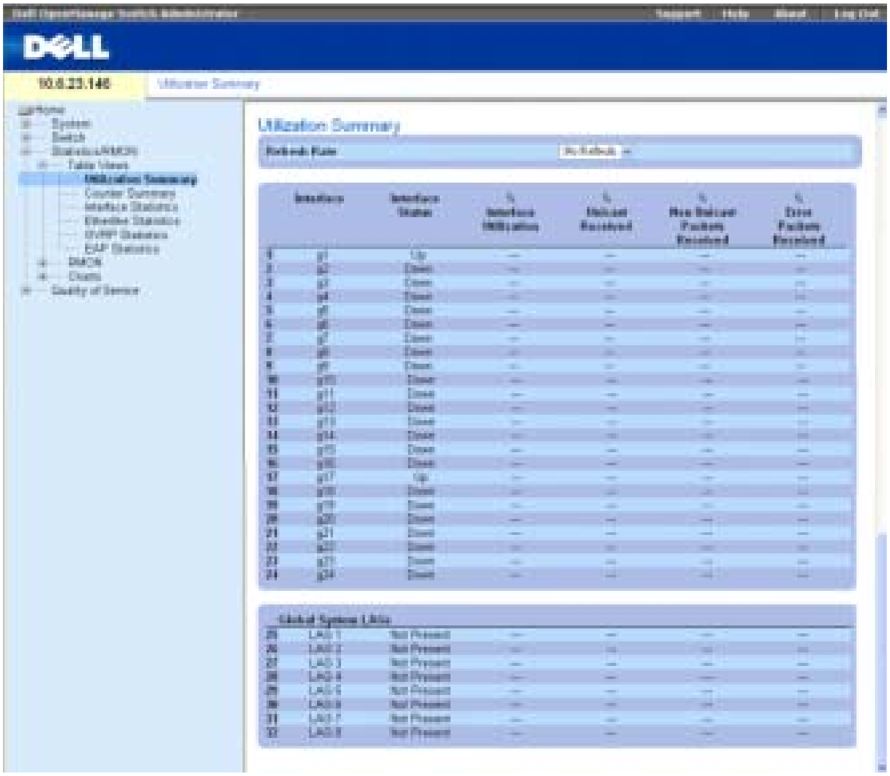
Viewing Tables

The **Table Views** page contains links for displaying statistics in a chart form. To open the page, click **Statistics→Table** in the tree view.

Viewing Utilization Summary

The **Utilization Summary** page contains statistics for interface utilization. To open the page, click **Statistics→Table Views→Utilization Summary** in the tree view.

Figure 8-115. Utilization Summary



Utilization Summary

Refresh Rate: No Refresh

	Interface	Interface Status	% Interface Utilization	% Unicast Received	% Non Unicast Packets Received	% Error Packets Received
1	g1	Up	—	—	—	—
2	g2	Down	—	—	—	—
3	g3	Down	—	—	—	—
4	g4	Down	—	—	—	—
5	g5	Down	—	—	—	—
6	g6	Down	—	—	—	—
7	g7	Down	—	—	—	—
8	g8	Down	—	—	—	—
9	g9	Down	—	—	—	—
10	g10	Down	—	—	—	—
11	g11	Down	—	—	—	—
12	g12	Down	—	—	—	—
13	g13	Down	—	—	—	—
14	g14	Down	—	—	—	—
15	g15	Down	—	—	—	—
16	g16	Down	—	—	—	—
17	g17	Up	—	—	—	—
18	g18	Down	—	—	—	—
19	g19	Down	—	—	—	—
20	g20	Down	—	—	—	—
21	g21	Down	—	—	—	—
22	g22	Down	—	—	—	—
23	g23	Down	—	—	—	—
24	g24	Down	—	—	—	—

Global System LAGs						
25	LAG 1	Not Present	—	—	—	—
26	LAG 2	Not Present	—	—	—	—
27	LAG 3	Not Present	—	—	—	—
28	LAG 4	Not Present	—	—	—	—
29	LAG 5	Not Present	—	—	—	—
30	LAG 6	Not Present	—	—	—	—
31	LAG 7	Not Present	—	—	—	—
32	LAG 8	Not Present	—	—	—	—

Refresh Rate — The amount of time that passes before the interface statistics are refreshed.

Interface — The interface number.

Interface Status — Status of the interface.

% Interface Utilization — Network interface utilization percentage based on the duplex mode of the interface. The range of this reading is from 0 to 200%. The maximum reading of 200% for a full duplex connection indicates that 100% of bandwidth of incoming and outgoing connections is used by the traffic travelling through the interface. The maximum reading for a half duplex connection is 100%.

% Unicast Received — Percentage of Unicast packets received on the interface.

% Non Unicast Packets Received — Percentage of non-Unicast packets received on the interface.

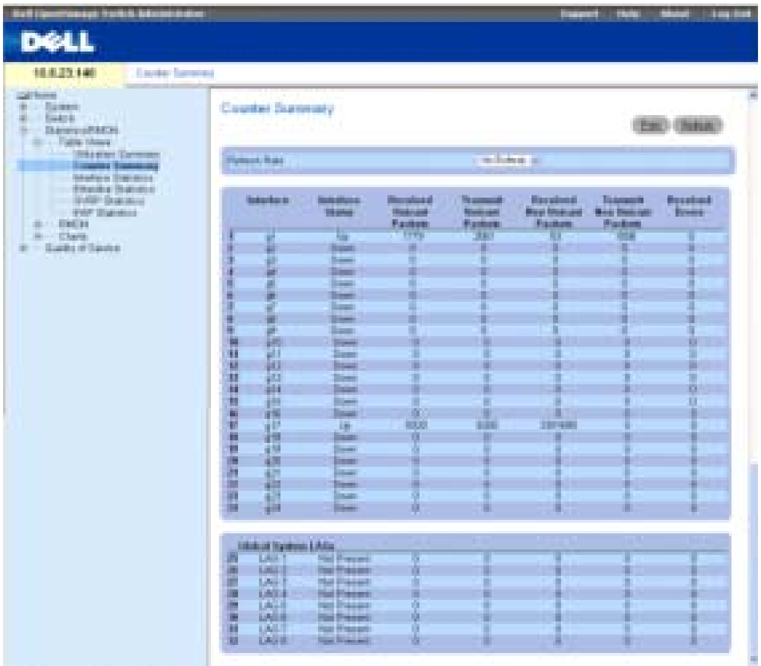
% Error Packets Received — Number packets with errors received on the interface.

Global System LAG — Current LAG/trunk performance.

Viewing Counter Summary

The **Counter Summary** page contains statistics for port utilization in numeric sums as opposed to percentages. To open the **Counter Summary** page, click **Statistics/RMON→Table Views→Counter Summary** in the tree view.

Figure 8-116. Counter Summary



Refresh Rate — The amount of time that passes before the interface statistics are refreshed.

Interface — The interface number.

Interface Status — The interface status.

Received Unicast Packets — Number of received Unicast packets on the interface.

Received Non Unicast Packets — Number of received non-Unicast packets on the interface.

Transmit Unicast Packets — Number of transmitted Unicast packets from the interface.

Transmit Non Unicast Packets — Number of transmitted non-Unicast packets from the interface.

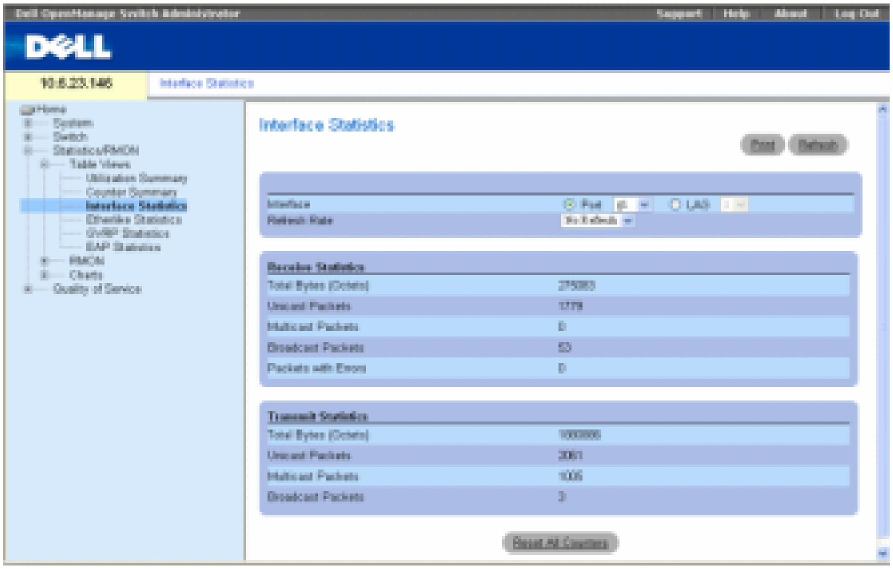
Received Errors —

Global System LAG — Current LAG/trunk performance.

Viewing Interface Statistics

The **Interface Statistics** page contains statistics for both received and transmitted packets. The fields for both received and transmitted packets are identical. To open the **Interface Statistics** page, click **Statistics/RMON→Table Views→Interface Statistics** in the tree view.

Figure 8-117. Interface Statistics



Interface	● Port g1 ○ LAG 1
Refresh Rate	No Refresh

Receive Statistics	
Total Bytes (Octets)	275083
Unicast Packets	1779
Multicast Packets	0
Broadcast Packets	53
Packets with Errors	0

Transmit Statistics	
Total Bytes (Octets)	1000895
Unicast Packets	2061
Multicast Packets	1006
Broadcast Packets	3

Interface — Specifies whether statistics are displayed for a port or LAG.

Refresh Rate — Amount of time that passes before the interface statistics are refreshed.

Receive Statistics

Total Bytes (Octets) — of octets received on the selected interface.

Unicast Packets — of Unicast packets received on the selected interface.

Multicast Packets — of Multicast packets received on the selected interface.

Broadcast Packets — of Broadcast packets received on the selected interface.

Packets with Errors — of error from the selected interface.

Transmit Statistics

Total Bytes (Octets) — of octets transmitted on the selected interface.

Unicast Packets — of Unicast packets transmitted on the selected interface.

Multicast Packets — of Multicast packets transmitted on the selected interface.

Broadcast Packets — of Broadcast packets transmitted on the selected interface.

Packets with Errors — of error transmitted from the selected interface.

Displaying Interface Statistics

1. Open the **Interface Statistics** page.
2. Select an interface in the **Interface** field.

   The interface statistics are displayed.

Resetting Interface Statistics Counters

1. Open the **Interface Statistics** page.
2. Click **Reset All Counters**.

   The interface statistics counters are reset.

Viewing Interface Statistics Using the CLI Commands

The following table summarizes the equivalent CLI commands for viewing interface statistics.

Table 8-80. Interface Statistics CLI Commands

CLI Command	Description
show interfaces counters [**ethernet** *interface* | **port-channel** *port-channel-number*]	Displays traffic seen by the physical interface.

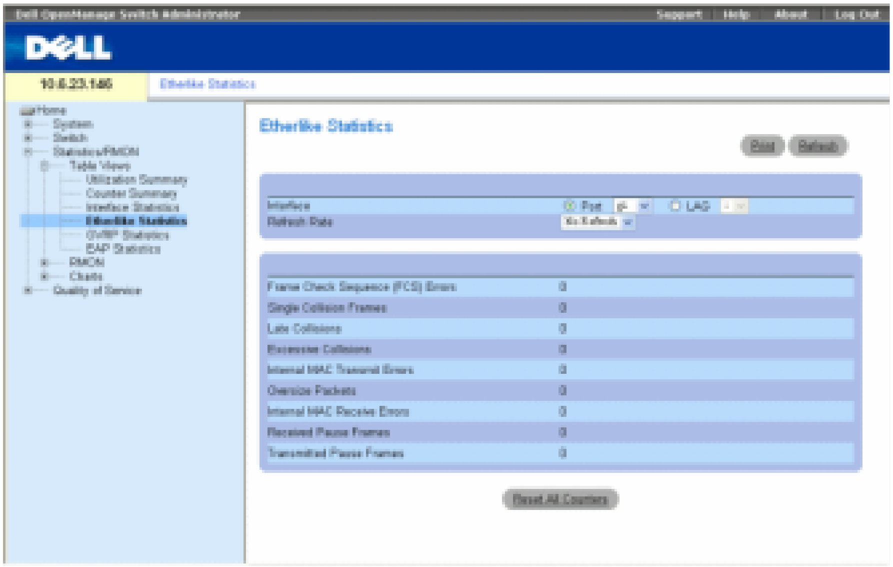
The following is an example of the CLI commands.

```
Console> enable

Console# show interfaces counters

Port     InOctets       InUcastPkts       InMcastPkts       InBcastPkts
-------  -------------  ----------------  ----------------  ------------
g1       183892         1289              987               8
g2       0              0                 0                 0
g3       123899         1788              373               19

Port     OutOctets      OutUcastPkts      OutMcastPkts      OutBcastPkts
-------  -------------  ----------------  ----------------  ------------
g4       9188           9                 8                 0
g5       0              0                 0                 0
g6       8789           27                8                 0


Ch       InOctets       InUcastPkts       InMcastPkts       InBcastPkts
-------  -------------  ----------------  ----------------  ------------
1        27889          928               0                 78

Ch       OutOctets      OutUcastPkts      OutMcastPkts      OutBcastPkts
-------  -------------  ----------------  ----------------  ------------
1        23739          882               0                 122
```

Viewing Etherlike Statistics

The **Etherlike Statistics** page contains interface statistics. To open the **Etherlike Statistics** page, click **Statistics/RMON→Table Views→Etherlike Statistics** in the tree view.

Figure 8-118. Etherlike Statistics



Etherlike Statistics

Interface	● Port g1 ○ LAG
Refresh Rate	No Refresh

Frame Check Sequence (FCS) Errors	0
Single Collision Frames	0
Late Collisions	0
Excessive Collisions	0
Internal MAC Transmit Errors	0
Oversize Packets	0
Internal MAC Receive Errors	0
Received Pause Frames	0
Transmitted Pause Frames	0

Interface — Specifies whether statistics are displayed for a port or LAG.

Refresh Rate — Amount of time that passes before the interface statistics are refreshed.

Frame Check Sequence (FCS) Errors — Number of FCS errors received on the selected interface.

Single Collision Frames — Number of single collision frames received on the selected interface.

Multiple Collision Frames — Number of multiple collisions frames received on the selected interface.

Single Quality Error (SQE) Test Errors — Number of SQE test errors received on the selected interface.

Deferred Transmissions — Number of deferred transmissions on the selected interface.

Late Collisions — **Excessive Collisions** — Number of excessive collisions received on the selected interface.

Internal MAC Transmit Errors — Number of internal MAC transmit errors on the selected interface.

Carrier Sense Errors — Number of carrier sense errors on the selected interface.

Oversize Packets — Number of oversized packet errors on the selected interface.

Internal MAC Receive Errors — Number of internal MAC received errors on the selected interface.

Single Quality Errors (SQE) Test Errors — The amount of SQE test errors received on the selected interface.

Receive Pause Frames — Number of received paused frames on the selected interface.

Transmitted Paused Frames —

Displaying Etherlike Statistics for an Interface

1 Open the **Etherlike Statistics** page.

2 Select an interface in the **Interface** field.

The interface's Etherlike statistics are displayed.

Resetting Etherlike Statistics

1 Open the **Etherlike Statistics** page.

2 Click **Reset All Counters**.

The Ethernetlike statistics are reset.

Viewing Etherlike Statistics Using the CLI Commands

The following table summarizes the equivalent CLI commands for viewing etherlike statistics.

Table 8-81. Etherlike Statistics CLI Commands

CLI Command	Description
show interfaces counters [**ethernet** interface | **port-channel** *port-channel-number*]	Displays traffic seen by the physical interface.

The following is an example of the CLI commands.

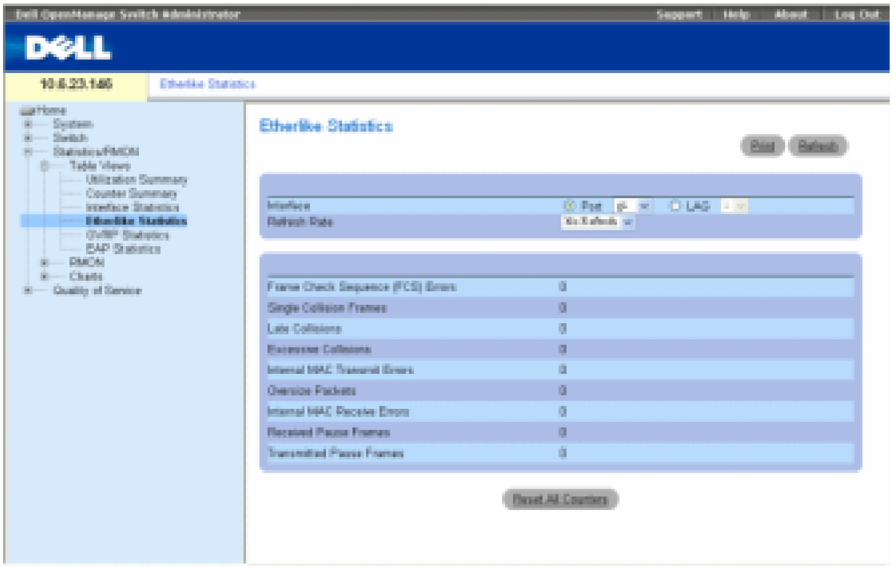
```
Console> enable
Console# show interfaces counters ethernet g1

Port    InOctets      InUCastPkts      InMcastPkts      InBcastPkts
------- ------------  ---------------  ---------------  -----------
```

```
g1       183892         1289              987               8

Port     OutOctets      OutUcastPkts      OutMcastPkts      OutBcastPkts
-------  -------------  ----------------  ----------------  ------------
g1       9188           9                 8                 0

FCS Errors: 8
Single Collision Frames: 0
Multiple Collision Frames: 0
SQE Test Errors: 0
Deferred Transmissions: 0
Late Collisions: 0
Excessive Collisions: 0
Internal MAC Tx Errors: 0
Carrier Sense Errors: 0
Oversize Packets: 0
Internal MAC Rx Errors: 0
Received Pause Frames: 0
Transmitted Pause Frames: 0
```

Viewing GVRP Statistics

The **GVRP Statistics** page contains device statistics for GVRP. To open the page, click **Statistics/RMON→Table Views→GVRP Statistics** in the tree view.

Figure 8-119. GVRP Statistics



Etherlike Statistics

Interface ● Port g4 ○ LAG

Refresh Rate No Refresh

Frame Check Sequence (FCS) Errors	0
Single Collision Frames	0
Late Collisions	0
Excessive Collisions	0
Internal MAC Transmit Errors	0
Oversize Packets	0
Internal MAC Receive Errors	0
Received Pause Frames	0
Transmitted Pause Frames	0

Interface — Specifies whether statistics are displayed for a port or LAG.

Refresh Rate — Amount of time that passes before the interface statistics are refreshed.

Join Empty — Device GVRP Join Empty statistics.

Empty — Device GVRP Empty statistics.

Leave Empty — Device GVRP Leave Empty statistics.

Join In — Device GVRP Join In statistics.

Leave In — Device GVRP Leave In statistics.

Leave All — Device GVRP Leave all statistics.

Invalid Protocol ID — Device GVRP Invalid Protocol ID statistics.

Invalid Attribute Type — Device GVRP Invalid Attribute ID statistics.

Invalid Attribute Value — Device GVRP Invalid Attribute Value statistics.

Invalid Attribute Length — Device GVRP Invalid Attribute Length statistics.

Invalid Events — Device GVRP Invalid Events statistics.

Displaying GVRP Statistics for a Port

1. Open the **GVRP Statistics** page.
2. Select an interface in the **Interface** field.

   The interface's GVRP statistics are displayed.

Resetting GVRP Statistics

1. Open the **GVRP Statistics** page.
2. Click **Reset All Counters**.

   The GVRP counters are reset.

Viewing GVRP Statistics Using the CLI Commands

The following table summarizes the equivalent CLI commands for viewing GVRP statistics.

Table 8-82. GVRP Statistics CLI Commands

CLI Command	Description
show gvrp statistics [**ethernet** *interface* | **port-channel** *port-channel-number*]	Displays GVRP statistics.
show gvrp error-statistics [**ethernet** *interface* | **port-channel** *port-channel-number*]	Displays GVRP error statistics.

The following is an example of the CLI commands:

:

```
Console# show gvrp statistics

GVRP statistics:
----------------
rJE  : Join Empty Received          rJIn : Join In Received
rEmp : Empty Received               rLIn : Leave In Received
rLE  : Leave Empty Received         rLA  : Leave All Received
sJE  : Join Empty Sent              sJIn : Join In Sent
sEmp : Empty Sent                   sLIn : Leave In Sent
sLE  : Leave Empty Sent             sLA  : Leave All Sent

Port rJE    rJIn  rEmp  rLIn  rLE   rLA   sJE   sJIn  sEmp  sLIn sLE   sLA
---- ---    ----  ----  ----  ---   ---   ---   ----  ----  ---- ---   ---
g1   0      0     0     0     0     0     0     0     0     0    0     0
g2   0      0     0     0     0     0     0     0     0     0    0     0
g3   0      0     0     0     0     0     0     0     0     0    0     0
g4   0      0     0     0     0     0     0     0     0     0    0     0
g5   0      0     0     0     0     0     0     0     0     0    0     0
g6   0      0     0     0     0     0     0     0     0     0    0     0
g7   0      0     0     0     0     0     0     0     0     0    0     0
g8   0      0     0     0     0     0     0     0     0     0    0     0
```

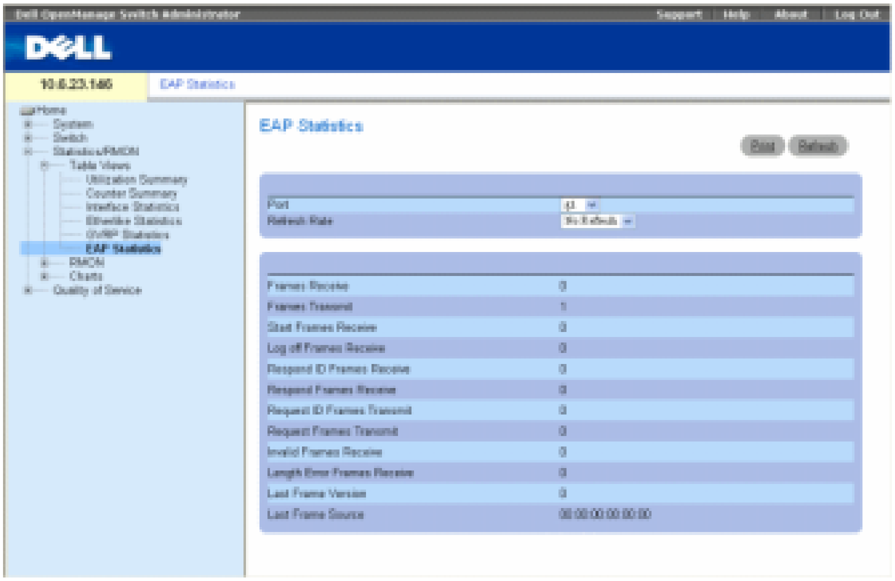
```
Console# show gvrp error-statistics

GVRP error statistics:
----------------------
Legend:
INVPROT  : Invalid Protocol Id      INVPLEN  : Invalid PDU Length
INVATYP  : Invalid Attribute Type   INVALEN  : Invalid Attribute Length
```

```
INVAVAL  : Invalid Attribute Value  INVEVENT : Invalid Event
Port     INVPROT       INVATYP    INVAVAL      INVALEN    INVEVENT
----     -------       -------    -------      -------    --------
g1       0             0          0            0          0
g2       0             0          0            0          0
g3       0             0          0            0          0
g4       0             0          0            0          0
g5       0             0          0            0          0
g6       0             0          0            0          0
g7       0             0          0            0          0
g8       0             0          0            0          0
```

Viewing EAP Statistics

The **EAP Statistics** page contains information about EAP packets received on a specific port. For more information about EAP, see "Port Based Authentication (802.1x)" . To open the **EAP Statistics** page, click **Statistics/RMON > Table Views > EAP Statistics** in the tree view.

Figure 8-120. EAP Statistics



EAP Statistics

Port	g1
Refresh Rate	No Refresh

Frames Receive	0
Frames Transmit	1
Start Frames Receive	0
Log off Frames Receive	0
Respond ID Frames Receive	0
Respond Frames Receive	0
Request ID Frames Transmit	0
Request Frames Transmit	0
Invalid Frames Receive	0
Length Error Frames Receive	0
Last Frame Version	0
Last Frame Source	00:00:00:00:00:00

Port — The port which is polled for statistics.

Refresh Rate — Amount of time that passes before the interface statistics are refreshed.

Frames Receive — The number of valid EAPOL frames received on the port.

Frames Transmit — The number of EAPOL frames transmitted via the port.

Start Frames Receive — The number of EAPOL Start frames received on the port.

Log off Frames Receive — The number of EAPOL Logoff frames that have been received on the port.

Respond ID Frames Receive — The number of EAP Resp/Id frames that have been received on the port.

Respond Frames Receive — The number of valid EAP Response frames received on the port.

Request ID Frames Transmit — The number of EAP Requested ID frames transmitted via the port.

Request Frames Transmit — The number of EAP Request frames transmitted via the port.

Invalid Frames Receive — The number of unrecognized EAPOL frames received on this port.

Length Error Frames Receive — The number of EAPOL frames with an invalid Packet Body Length received on this port.

Last Frame Version — The protocol version number attached to the most recently received EAPOL frame.

Last Frame Source — The source MAC address attached to the most recently received EAPOL frame.

Displaying EAP statistics for a Port

1. Open the **EAP Statistics** page.
2. Select an interface in the **Interface** field.

   The interface EAP statistics are displayed.

Resetting the EAP Statistics

1. Open the **EAP Statistics** page.
2. Click **Reset All Counters** to reset the counter.

   The EAP statistics are reset.

Viewing EAP Statistics Using the CLI Commands

The following table summarizes the CLI commands for viewing EAP statistics.

Table 8-83. GVRP Statistics CLI Commands

CLI Command	Description
show dot1x statistics ethernet *interface*	Displays 802.1X statistics for the specified interface.

The following is an example of the CLI commands:

```
Switch# show dot1x statistics ethernet g1
EapolFramesRx: 11
EapolFramesTx: 12
EapolStartFramesRx: 1
EapolLogoffFramesRx: 1
EapolRespIdFramesRx: 3
EapolRespFramesRx: 6
EapolReqIdFramesTx: 3
EapolReqFramesTx: 6
InvalidEapolFramesRx: 0
EapLengthErrorFramesRx: 0
LastEapolFrameVersion: 1
LastEapolFrameSource: 0008.3b79.8787
```

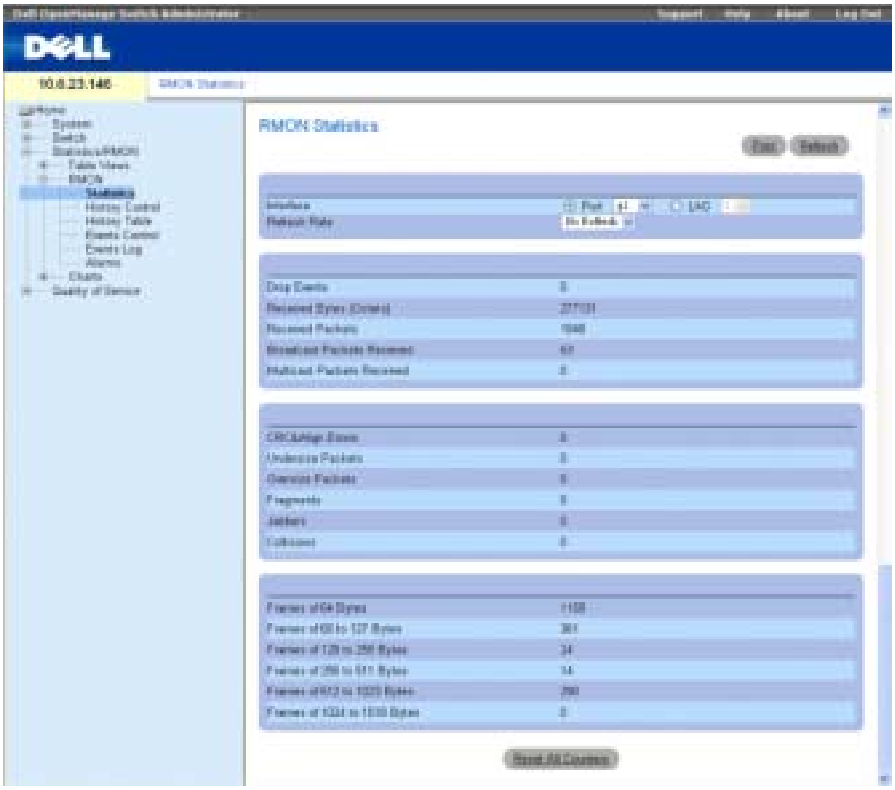
Viewing RMON Statistics

Remote Monitoring (RMON) contins links for viewing network information from a remote location. To open the **RMON** page, click **Statistics/RMON→RMON** in the tree view.

Viewing RMON Statistics Group

The **RMON Statistics** page contains fields for viewing information about device utilization and errors that occurred on the device. To open the **RMON Statistics** page, click **Statistics/RMON→ RMON→Statistics** in the tree view.

Figure 8-121. RMON Statistics



RMON Statistics

Interface	○ Port g1 ○ LAG 1
Refresh Rate	No Refresh

Drop Events	0
Received Bytes (Octets)	277131
Received Packets	1946
Broadcast Packets Received	67
Multicast Packets Received	0

CRC&Align Errors	0
Undersize Packets	0
Oversize Packets	0
Fragments	0
Jabbers	0
Collisions	0

Frames of 64 Bytes	1158
Frames of 65 to 127 Bytes	361
Frames of 128 to 255 Bytes	34
Frames of 256 to 511 Bytes	14
Frames of 512 to 1023 Bytes	290
Frames of 1024 to 1518 Bytes	0

Interface — Specifies the port or LAG for which statistics are displayed.

Refresh Rate — Amount of time that passes before the statistics are refreshed.

Drop Events — Number of dropped events that have occurred on the interface since the device was last refreshed.

Received Bytes (Octets) — Number of octets received on the interface since the device was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.

Received Packets — Number of packets received on the interface, including bad packets, Multicast and broadcast packets, since the device was last refreshed.

Broadcast Packets Received — Number of good broadcast packets received on the interface since the device was last refreshed. This number does not include Multicast packets.

Multicast Packets Received — Number of good Multicast packets received on the interface since the device was last refreshed.

CRC & Align Errors — Number of CRC and Align errors that have occurred on the interface since the device was last refreshed.

Undersize Packets — Number of undersized packets (less than 64 octets) received on the interface since the device was last refreshed.

Oversize Packets — Number of oversized packets (over 1518 octets) received on the interface since the device was last refreshed.

Fragments — Number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received on the interface since the device was last refreshed.

Jabbers — Number of jabbers (packets longer than 1518 octets) received on the interface since the device was last refreshed.

Collisions — Number of collisions received on the interface since the device was last refreshed.

Frames of *xx* Bytes — Number of *xx*-byte frames received on the interface since the device was last refreshed.

Viewing Interface Statistics

1. Open the **RMON Statistics** page.
2. Select an interface type and number in the **Interface** field.

   The interface statistics are displayed.

Viewing RMON Statistics Using the CLI Commands

The following table summarizes the equivalent CLI commands for viewing RMON statistics.

Table 8-84. RMON Statistics CLI Commands

CLI Command	Description
show rmon statistics {ethernet *interface* **| port-channel** *port-channel-number***}**	Displays RMON Ethernet statistics.

The following is an example of the CLI commands:

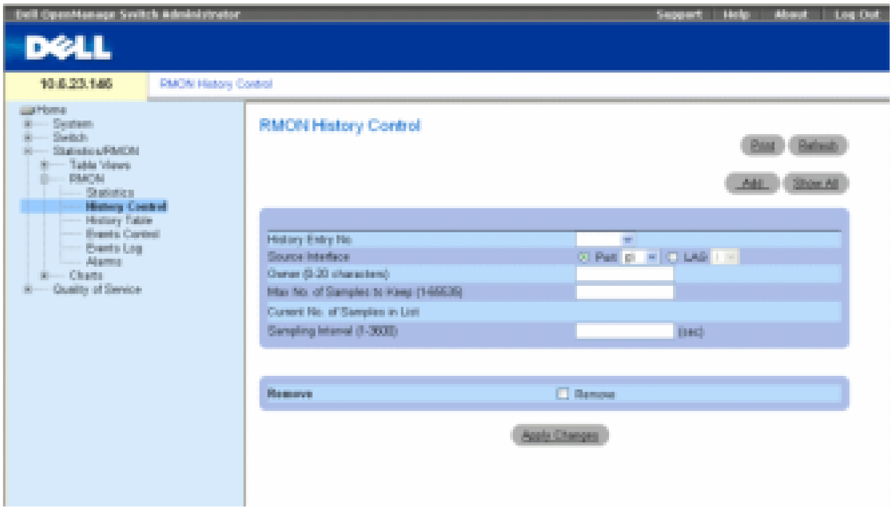
```
console> enable
```

```
console> enable
Console# show rmon statistics ethernet g1
Port g1
Dropped: 8
Octets: 878128 Packets: 978
Broadcast: 7 Multicast: 1
CRC Align Errors: 0 Collisions: 0
Undersize Pkts: 0 Oversize Pkts: 0
Fragments: 0 Jabbers: 0
64 Octets: 98 65 to 127 Octets: 0
128 to 255 Octets: 0 256 to 511 Octets: 0
512 to 1023 Octets: 491 1024 to 1518 Octets: 389
```

Viewing RMON History Control Statistics

The **RMON History Control** page contains information about samples of data taken from ports. For example, the samples may include interface definitions or polling periods. To open the **RMON History Control** page, click **Statistics/RMON→History Control** in the tree view.

Figure 8-122. RMON History Control



History Entry No.	
Source Interface	● Port g1 ○ LAG 1
Owner (0-20 characters)	
Max No. of Samples to Keep (1-65535)	
Current No. of Samples in List	
Sampling Interval (1-3600)	(sec)

Remove	□ Remove

History Entry No. — Entry number for the **History Control Table** page.

Source Interface — Port or LAG from which the history samples were taken.

Owner (0-20 characters) — RMON station or user that requested the RMON information.

Max No. of Samples to Keep (1-65535) — Number of samples to be saved. The default value is 50.

Current No. of Samples in List — The current number of samples taken.

Sampling Interval (1-3600) — Indicates in seconds the time that sampl s are taken from the ports. The possible values are 1-3600 seconds. The default is 1800 seconds (30 minutes).

Remove — When selected, removes the **History Control Table** entry.

Adding a History Control Entry

1. Open the **RMON History Control** page.
2. Click **Add**.

   The **Add History Entry** page opens.
3. Complete the fields in the dialog.
4. Click **Apply Changes**.

   The entry is added to the **History Control Table**.

Modifying a History Control Table Entry

1. Open the **RMON History Control** page.
2. Select an entry in the **History Entry No.** field.
3. Modify the fields as required.
4. Click **Apply Changes**.

   The table entry is modified, and the device is updated.

Deleting a History Control Table Entry

1. Open the **RMON History Control** page.
2. Select an entry in the **History Entry No.** field.
3. Click **Remove**.
4. Click **Apply Changes**.

   The selected table entry is deleted, and the device is updated.

Viewing RMON History Control Using the CLI Commands

The following table summarizes the equivalent CLI commands for viewing GVRP statistics.

Table 8-85. RMON History CLI Commands

CLI Command	Description
rmon collection history *index* [**owner** *ownername* | **buckets** *bucket-number*] [**interval** *seconds*]	Enables and configures RMON on an interface.
show rmon collection history [**ethernet** *interface* | **port-channel** *port-channel-number*]	Displays RMON collection history statistics.

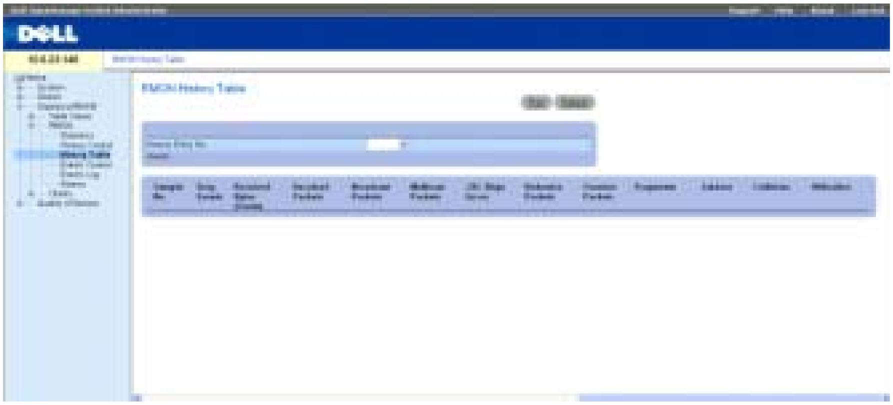
The following is an example of the CLI commands:

```
Console (config)# interface ethernet g8
Console (config-if)# rmon collection history 1 interval 2400
Console (config-if)# exit
Console (config)# exit
```

Viewing the RMON History Table

The **RMON History Table** contains interface specific statistical network samplings. Each table entry represents all counter values compiled during a single sample. To open the **RMON History Table**, click **Statistics/RMON→RMON→History Table** in the tree view.

Figure 8-123. RMON History Table



Sample No. — The specific sample the information in the table reflects.

Drop Events — The number of dropped packets due to lack of network resources during the sampling interval. This may not represent the exact number of dropped packets, but rather the number of times dropped packets were detected.

Received Bytes (Octets) — The number of data octets, including bad packets, received on the network.

Received Packets — The number of packets received during the sampling interval.

Broadcast Packets — The number of good broadcast packets received during the sampling interval.

Multicast Packets — The number of good Multicast packets received during the sampling interval.

CRC Align Errors — The number of packets received during the sampling session with a length of 64-1518 octets, a bad Check Sequence (FCS), and with an integral number of octets, or a bad FCS with a non-integral number.

Undersize Packets — The number of packets received less than 64 octets long during the sampling session.

Oversize Packets — The number of packets received more than 1518 octets long during the sampling session.

Fragments — The number of packets received less than 64 octets long and had a FCS during the sampling session.

Jabbers — The number of packets received more than 1518 octets long and had a FCS during the sampling session.

Collisions — Estimates the total number of packet collision that occurred during the sampling session. Collision are detected when repeater ports detects two or more stations transmit simultaneously.

Utilization — Estimates the main physical layer network usage on an interface during the session sampling. The value is reflected in hundredths of a percent.

Viewing Statistics for a Specific History Entry

1. Open the **RMON History Table**.
2. Select an entry in the **History Table No.** field.

   The entry statistics display in the RMON History Table.

Viewing RMON History Control Using the CLI Commands

The following table summarizes the equivalent CLI commands for viewing RMON history.

Table 8-86. RMON History Control CLI Commands

CLI Command	Description
show rmon history *index* {**throughput** | **errors** | **other**} [**period** *seconds*]	Displays RMON Ethernet statistics history.

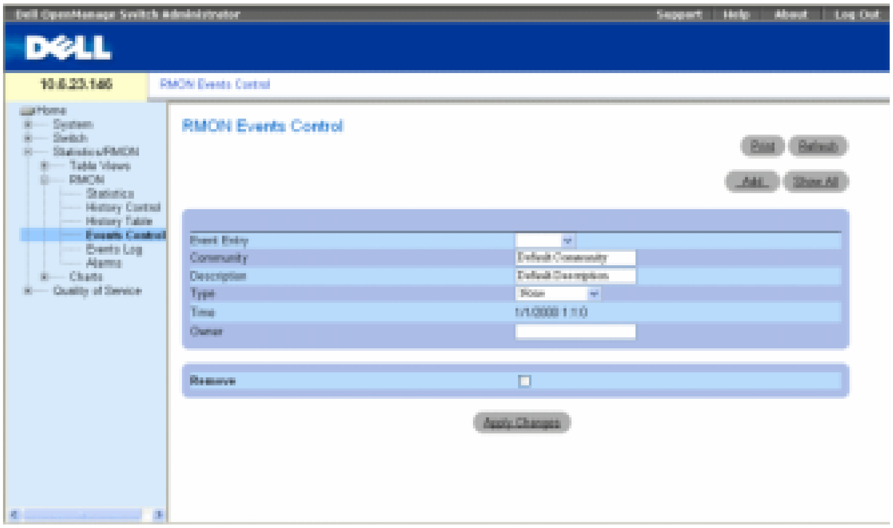
The following is an example of the CLI commands for displaying RMON ethernet statistics for throughput on index 1:.

```
console> enable
Console# show rmon history 1 throughput
Sample Set: 1                    Owner: CLI
Interface: g1                    Interval: 1800
Requested samples: 50            Granted samples: 50

Maximum table size: 500

Time                  Octets    Packets  Broadcast    Multicast    %
------------------    --------- -------  ----------   ---------    -----
Jan 18 2004 21:57:00  303595962 357568   3289         7287         19.98%
Jan 18 2004 21:57:30  287696304 275686   2789         2789         20.17%
```

Defining Device RMON Events

The **RMON Events Control** page contains fields for defining RMON events. To open the **RMON Events Control** page, click **Statistics/RMON→RMON→Events Control** in the tree view.

Figure 8-124. RMON Events Control



Event Entry	
Community	Default Community
Description	Default Description
Type	None
Time	1/1/2000 1:1:0
Owner	

Remove □

Event Entry — The event.

Community — Community to which the event belongs.

Description — User-defined event description.

Type — Describes the event type. Possible values are:

Log — Event type is a log entry.

Trap — Event type is a trap.

Log and Trap — Event type is both a log entry and a trap.

None — There is no event.

Time —

Owner — The device or user that defined the event.

Remove — When selected, removes the event from the **RMON Events Table**.

Adding an RMON Event

1. Open the **RMON Events Control** page.
2. Click **Add**.

The **Add an Event Entry** page opens.

3 Complete the information in the dialog and click **Apply Changes**.

The **Event Table** entry is added, and the device is updated.

Modifying an RMON Event

1 Open the **RMON Events Control** page

2 Select an entry in the **Event Table**.

3 Modify the fields in the dialog and click **Apply Changes**.

The **Event Table** entry is modified, and the device is updated.

Deleting RMON Event Entries

1 Open the **RMON Events Control** page.

2 Click **Show All**.

The **Events Table** page opens.

3 Select **Remove** for the event(s) that need to be deleted and then click **Apply Changes**.

The selected table entry is deleted, and the device is updated.

NOTE: A single event entry can be removed from the **RMON Events Control** page by selecting the **Remove** check box on that page.

Defining Device Events Using the CLI Commands

The following table summarizes the equivalent CLI commands for defining device events.

Table 8-87. Device Event Definition CLI Commands

CLI Command	Description
rmon event *index type* [**community** *text*] [**description** *text*] [**owner** *name*]	Configures RMON events.
show rmon events	Displays RMON event table.

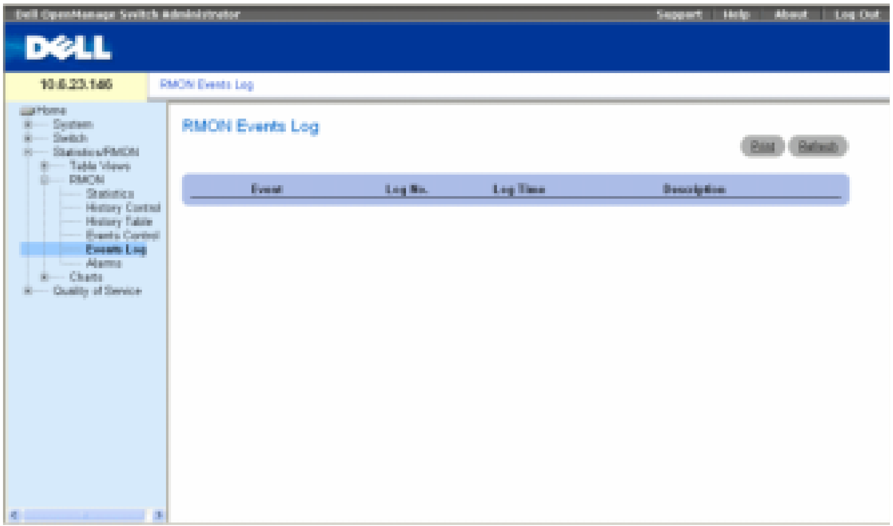
The following is an example of the CLI commands:

```
console> enable
console# config
console (config)# rmon event 1 log
console (config)# exit
Console# show rmon events

Index Description   Type      Community Owner   Last time sent
----- -----------   --------  --------- ------- --------------------
1     Errors        Log                 CLI     Jan 18 2002 23:58:17
2     High          Log-Trap  router    Manager Jan 18 2002 23:59:48
      Broadcast
```

Viewing the RMON Events Log

The **RMON Events Log** page contains a list of RMON events. To open the **RMON Events Log** page, click **Statistics/RMON→RMON→Events** in the tree view.

Figure 8-125. RMON Events Log



RMON Events Log

Event	Log No.	Log Time	Description

Event — The RMON Events Log entry number.

Log No.— The log number.

Log Time — Time when the log entry was entered.

Description — Describes the log entry.

Defining Device Events Using the CLI Commands

The following table summarizes the equivalent CLI commands for defining device events.

Table 8-88. Device Event Definition CLI Commands

CLI Command	Description
show rmon log [*event*]	Displays the RMON logging table.

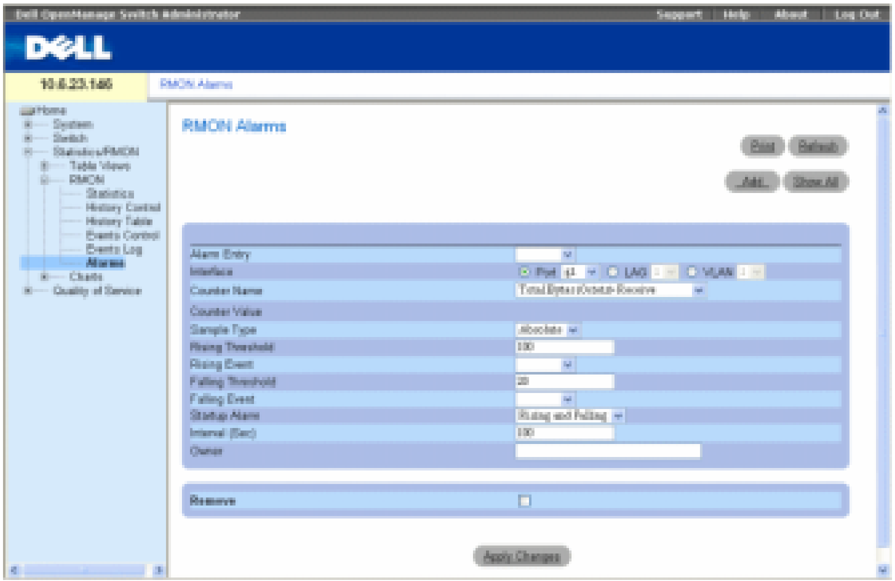
The following is an example of the CLI commands:

```
console> enable
console# config
console (config)# rmon event 1 log
console (config)# exit
Console# show rmon log

Maximum table size: 500

Event      Description       Time
-------    --------------    ---------
1          Errors            Jan 18 2002 23:48:19
1          Errors            Jan 18 2002 23:58:17
2          High Broadcast    Jan 18 2002 23:59:48

Console# show rmon log

Maximum table size: 500 (800 after reset)

Event      Description       Time
-------    --------------    ---------
1          Errors            Jan 18 2002 23:48:19
1          Errors            Jan 18 2002 23:58:17
2          High Broadcast    Jan 18 2002 23:59:48
```

Defining RMON Device Alarms

The **RMON Alarms** page contains fields for setting network alarms. Network alarms occur when a network problem, or event, is detected. Rising and falling thresholds generate events. To open the **RMON Alarms** page, click **Statistics/RMON→RMON→Alarms** in the tree view.

Figure 8-126. RMON Alarms



RMON Alarms

Alarm Entry	
Interface	● Port g1 ○ LAG 1 ○ VLAN 1
Counter Name	Total Bytes (Octets) Receive
Counter Value	
Sample Type	Absolute
Rising Threshold	100
Rising Event	
Falling Threshold	20
Falling Event	
Startup Alarm	Rising and Falling
Interval (Sec)	100
Owner	

Remove	□

Alarm Entry — Indicates a specific alarm.

Interface — The interface for which RMON statistics are displayed.

Counter Name — The selected MIB variable.

Counter Value — The value of the selected MIB variable.

Sample Type — Specifies the sampling method for the selected variable and comparing the value against the thresholds. The possible field values are:

> **Delta** — Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold.
>
> **Absolute** — Compares the values directly with the thresholds at the end of the sampling interval.

Rising Threshold — The rising counter value that triggers the rising threshold alarm. The rising threshold is presented on top of the graph bars. Each monitored variable is designated a color.

Rising /Falling Event — The mechanism in which the alarms are reported — LOG, TRAP, or a combination of both. When LOG is selected, there is no saving mechanism either in the device or in the management system. However, if the device is not being reset, it remains in the device LOG table. If TRAP is selected, an SNMP trap is generated and reported via the trap's general mechanism. The TRAP can be saved using the same mechanism.

Falling Threshold — The falling counter value that triggers the falling threshold alarm. The falling threshold is graphically presented on of the graph bars. Each monitored variable is designated a color.

Startup Alarm — The trigger that activates the alarm generation. Rising is defined by crossing the threshold from a low-value threshold to a higher-value threshold.

Interval (sec) — Alarm interval time.

Owner — Device or user that defined the alarm.

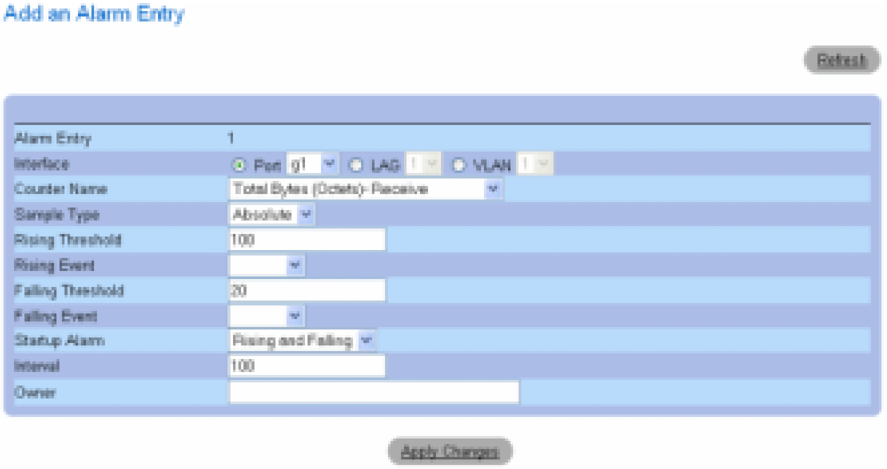
Remove — When selected, removes an RMON Alarm.

Adding an Alarm Table Entry

1. Open the **RMON Alarms** page.
2. Click **Add**.

   The **Add an Alarm Entry** page opens:

Figure 8-127. Add an Alarm Entry Page



Add an Alarm Entry

Alarm Entry	1
Interface	● Port g1 ○ LAG 1 ○ VLAN 1
Counter Name	Total Bytes (Octets)- Receive
Sample Type	Absolute
Rising Threshold	100
Rising Event	
Falling Threshold	20
Falling Event	
Startup Alarm	Rising and Falling
Interval	100
Owner	

3. Select an interface.
4. Complete the fields in the dialog.

5 Click **Apply Changes**.

The RMON alarm is added, and the device is updated.

Modifying an Alarm Table Entry

1 Open the **RMON Alarms** page.

2 Select an entry in the **Alarm Entry** drop-down menu.

3 Modify the fields in the dialog as required.

4 Click **Apply Changes**.

The entry is modified, and the device is updated.

Displaying the Alarm Table

1 Open the **RMON Alarms** page.

2 Click **Show All**.

The **Alarms Table** page opens.

Deleting an Alarm Table Entry

1 Open the **RMON Alarms** page.

2 Select an entry in the **Alarm Entry** drop-down menu.

3 Select the **Remove** check box.

4 Click **Apply Changes**.

The selected entry is deleted, and the device is updated.

Defining Device Alarms Using the CLI Commands

The following table summarizes the equivalent CLI commands for defining device alarms.

Table 8-89. Device Alarm CLI Commands

CLI Command	Description
rmon alarm *index variable interval rthreshold fthreshold revent fevent* [**type** *type*] [**startup** *direction*] [**owner** *name*]	Configures RMON alarm conditions.
show rmon alarm-table	Displays summary of the alarm table.
show rmon alarm	Displays RMON alarm configuration.

The following is an example of the CLI commands:

```
console> enable

console# config

Console (config)# rmon alarm 1000 dell 360000 1000000 1000000
10 20

Console# show rmon alarm-table


Index   OID                 Owner
------  ------------------- --------------
1       1.3.6.1.2.1.2.2.1.1 CLI
        0.1
2       1.3.6.1.2.1.2.2.1.1 Manager
        0.1
3       1.3.6.1.2.1.2.2.1.1 CLI
        0.9
```

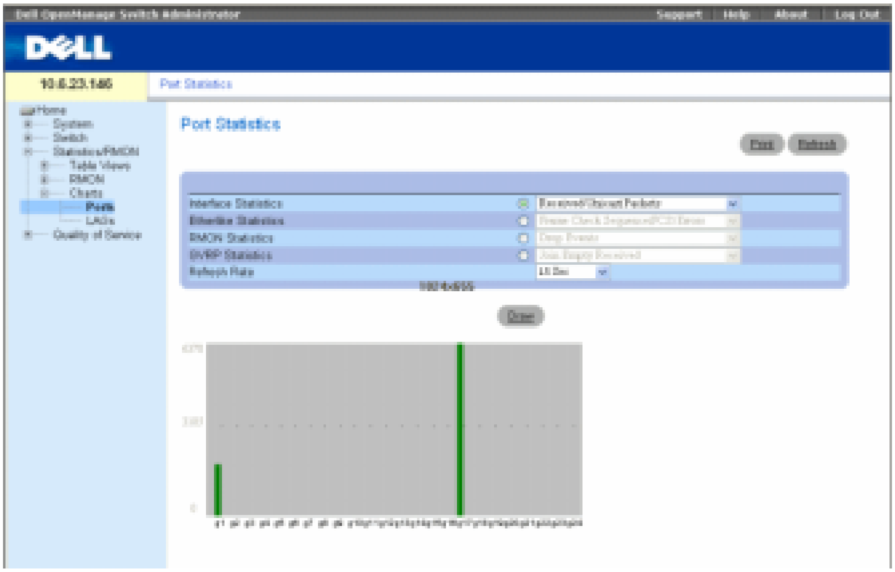
Viewing Charts

The **Chart** page contains links for displaying statistics in a chart form. To open the page, click **Statistics→Charts** in the tree view.

Viewing Port Statistics

The **Port Statistics** page contains fields for opening statistics in a chart form for port elements. To open the **Port Statistics** page, click **Statistics→Charts→Ports** in the tree view.

Figure 8-128. Port Statistics



Interface Statistics ● Received Unicast Packets

Etherlike Statistics ○ Frame Check Sequence(FCS) Errors

RMON Statistics ○ Drop Events

GVRP Statistics ○ Join Empty Received

Refresh Rate 15 Sec

Interface Statistics — Selects the type of interface statistics to open.

Etherlike Statistics — Selects the type of Etherlike statistics to open.

RMON Statistics — Selects the type of RMON statistics to open.

GVRP Statistics — Selects the GVRP statistics type to open.

Refresh Rate — Amount of time that passes before the statistics are refreshed.

Displaying Port Statistics

1. Open the **Port Statistics** page.
2. Select the statistic type to open.
3. Select the desired refresh rate from the **Refresh Rate** drop-down menu.
4. Click **Draw**.

The graph for the selected statistic is displayed.

Viewing Port Statistics Using the CLI Commands

The following table summarizes the equivalent CLI commands for viewing port statistics.

Table 8-90. Port Statistic CLI Commands

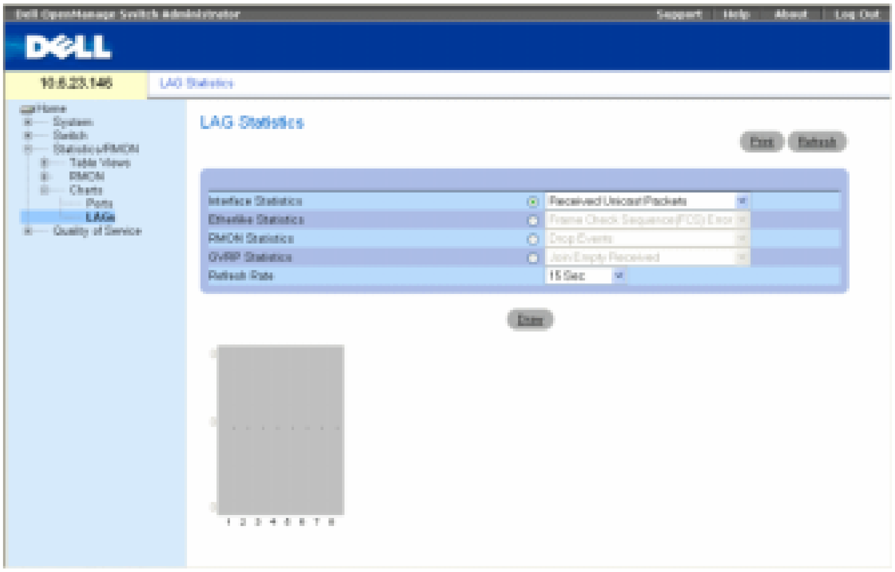
CLI Command	Description
show interfaces counters [**ethernet** interface | **port-channel** *port-channel-number*]	Displays traffic seen by the physical interface.
show rmon statistics {**ethernet** *interface* | **port-channel** *port-channel-number*}	Displays RMON Ethernet statistics.
show gvrp statistics {**ethernet** *interface* | **port-channel** *port-channel-number*}	Displays GVRP statistics.
show gvrp error-statistics {**ethernet** *interface* | **port-channel** *port-channel-number*}	Displays GVRP error statistics.

```
Console# show interfaces description ethernet g1

Port          Description
----          ------------------
g1            Management_port
g2            R&D_port
g3            Finance_port

Ch            Description
----          ------------------
1             Output
```

Viewing LAG Statistics

The **LAG Statistics** page contains fields for opening statistics in a chart form for LAGs. To open the **LAG Statistics** page, click **Statistics→Charts→LAGs** in the tree view.

Figure 8-129. LAG Statistics



LAG Statistics

Interface Statistics	●	Received Unicast Packets
Etherlike Statistics	○	Frame Check Sequence(FCS) Error
RMON Statistics	○	Drop Events
GVRP Statistics	○	Join Empty Received
Refresh Rate		15 Sec

Interface Statistics — Selects the type of interface statistics to open.

Etherlike Statistics — Selects the type of Etherlike statistics to open.

RMON Statistics — Selects the type of RMON statistics to open.

GVRP Statistics — Selects the type of GVRP statistics to open.

Refresh Rate — Amount of time that passes before the statistics are refreshed.

Displaying LAG Statistics

1 Open the **LAG Statistics** page.

2 Select the statistic type to open.

3 Select the desired refresh rate from the **Refresh Rate** drop-down menu.

4 Click **Draw**.

The graph for the selected statistic is displayed.

Viewing LAG Statistics Using the CLI Commands

The following table summarizes the equivalent CLI commands for viewing LAG statistics.

Table 8-91. LAG Statistic CLI Commands

CLI Command	Description
show interfaces counters [**ethernet** *interface* | **port-channel** *port-channel-number*]	Displays traffic seen by the physical interface.
show rmon statistics {**ethernet** *interface* | **port-channel** *port-channel-number*}	Displays RMON Ethernet statistics.
show gvrp statistics {**ethernet** *interface* | **port-channel** *port-channel-number*}	Displays GVRP statistics.
show gvrp error-statistics {**ethernet** *interface* | **port-channel** *port-channel-number*}	Displays GVRP error statistics.

```
Console# show gvrp statistics

GVRP statistics:
----------------
rJE  : Join Empty Received          rJIn : Join In Received
rEmp : Empty Received               rLIn : Leave In Received
rLE  : Leave Empty Received         rLA  : Leave All Received
sJE  : Join Empty Sent              sJIn : Join In Sent
sEmp : Empty Sent                   sLIn : Leave In Sent
sLE  : Leave Empty Sent             sLA  : Leave All Sent

Port rJE   rJIn  rEmp  rLIn  rLE   rLA  sJE   sJIn  sEmp  sLIn sLE  sLA
---- ---   ----  ----  ----  ---   ---  ---   ----  ----  ---- ---  ---
g1   0     0     0     0     0     0    0     0     0     0    0    0
```

```
g2   0     0     0     0     0    0    0     0    0    0    0    0
g3   0     0     0     0     0    0    0     0    0    0    0    0
g4   0     0     0     0     0    0    0     0    0    0    0    0
g5   0     0     0     0     0    0    0     0    0    0    0    0
g6   0     0     0     0     0    0    0     0    0    0    0    0
g7   0     0     0     0     0    0    0     0    0    0    0    0
g8   0     0     0     0     0    0    0     0    0    0    0    0
```

9

Configuring Quality of Service

This section provides information for defining and configuring Quality of Service (QoS) parameters. To open the Click **Quality of Service** in the tree view.

Quality of Service (QoS) Overview

Quality of Service (QoS) provides the ability to implement QoS and priority queuing within a network. QoS improves network traffic flow based on policies, frame counters and context.

An implementation example that requires QoS include certain types of traffic such as Voice, Video and real-time traffic which can be assigned a high priority queue, while other traffic can be assigned a lower priority queue. The result is an improved traffic flow for traffic with high demand.

QoS is defined by:

- **Classification** — Specifies which packet fields are matched to specific values. All packets matching the user-defined specifications are classified together.
- **Action** — Defines traffic management where packets being forwarded are based on packet information, and packet field values such as VLAN priority (VPT) and DSCP (DiffServ Code Point).

VPT Tag Classification Information

VLAN Priority Tags are used to classify the packets by mapping packets to one of the output queues. VLAN Priority Tag to queue assignments are also user-definable. The table below details the VPT to queue default settings:

Table 9-92. CoS to Queue Mapping Table Default values

CoS Value	Forwarding Queue Values
0	q2
1	q1 (Lowest Priority = Best Effort)
2	q1 (Lowest Priority = Best Effort)
3	q2
4	q3
5	q3
6	q4 (Highest Priority)
7	q4 (Highest Priority)

Packets arriving untagged are assigned a default VPT that is set on a per port basis. The assigned VPT is used to map the packet to the output queue and as the egress VPT.

DSCP values can be mapped to priority queues. The following table contains the default DSCP mapping to forwarding queue values:

Table 9-93. DSCP to Queue Mapping Table Default Values

DSCP Value	Forwarding Queue Values
0-7	q2 (Lowest Priority)
8-15	q1
16-23	q1
24-31	q2
32-39	q3
40-47	q3
48-55	q4
55-63	q4 (Highest Priority)

DSCP mapping is enabled on a per-system basis.

CoS Services

After packets are assigned to a specific queue, CoS services can be assigned to the queue(s). Output queues are configured with a scheduling scheme by one of the following methods:

- **Strict Priority** — Ensures that time-sensitive applications are always forwarded through an expedited path. Strict Priority allows the prioritization of mission-critical, time-sensitive traffic over less time-sensitive applications.
  For example, under Strict Priority, voice over IP traffic is forwarded before FTP or e-mail (SMTP) traffic.
  The strict priority queue is emptied before the traffic in the remaining queues in forwarded.
- **Weighted Round Robin** — Ensures that a single application does not dominate the device forwarding capacity. Weighted Round Robin (WRR) forwards entire queues in a Round Robin order. Queue priorities are defined by the queue length. The longer the queue length, the higher the queue's forwarding priority.
  For example, if four queues have queue weights of 1, 2, 3 and 4, packets with the highest forwarding priority are assigned to queue 4, and packets with the lowest forwarding priority assigned to queue 1.
  By providing highest forwarding priority to length 4 queues, weighted round robin processes higher priority traffic, and ensure that low-priority traffic is forwarded satisfactorily.

The scheduling scheme is enabled system-wide. Queues assigned to the strict priority policy are automatically assigned to the highest priority queue By default all values are set as Strict Priority.

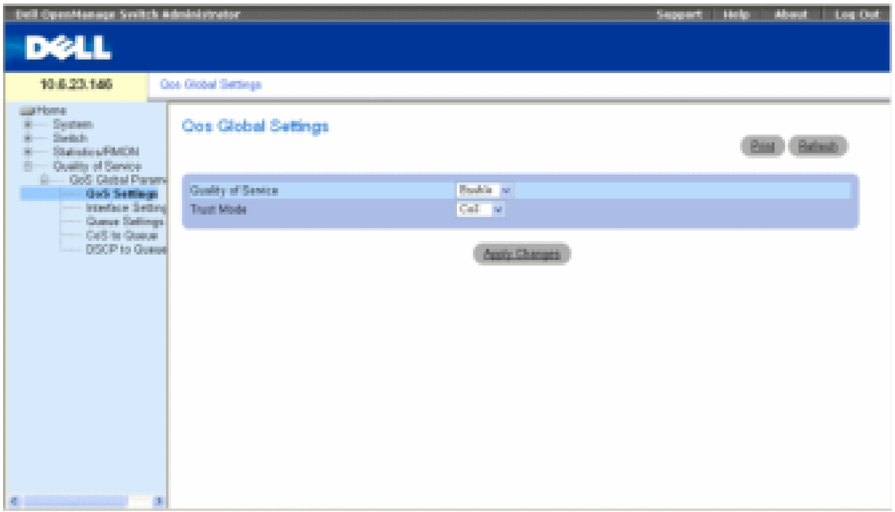
When changing to WRR mode the default weight value is one. Queue weight values can be assigned in any order using WRR. WRR values can be assigned system-wide. Best effort traffic is always assigned to the first queue. WRR values must be assigned so that Queue 1 remains best effort.

Defining CoS Global Parameters

Class of Service global parameters are set from the **CoS Global Parameter** pages.

To open the **QoS Settings** page, click **Quality of Service→CoS Global Parameters →CoS Settings** in the tree view.

Figure 9-130. QoS Settings



Quality of Service: Enable
Trust Mode: CoS

Quality of Service — Enables or disables managing network traffic using Quality of Service.

Trust Mode — Determines which packet fields to use for classifying packets entering the device. When no rules are defined the traffic containing the predefined packet field (CoS or DSCP) is mapped according to the relevant trust modes table. Traffic not containing a predefined packet field is mapped to best effort. The possible Trust Mode field values are:

> **CoS** — The output queue assignment is determined by the IEEE802.1p VLAN priority tag (VPT) or by the default VPT assigned to a port.
>
> **DSCP** — The output queue assignment is determined by the DSCP field.

Enabling Quality of Service:

1. Open the **QoS Settings** page.
2. Select **Enable** in the **CoS Mode** field.

3 Click Apply Changes.

Class of Service is enabled on the device.

Enabling Trust:

1 Open the **QoS Settings** page.

2 Select **Trust** in the **Trust Mode** field.

3 Click Apply Changes.

Trust is enabled on the device.

Enabling Trust Using the CLI Commands

The following table summarizes the equivalent CLI commands for configuring fields in the **QoS Settings** page.

Table 9-94. CoS Setting CLI Commands

CLI Command	Description
qos trust [cos | dscp]	Configures the system to basic mode and the "trust" state.
no cos trust	Returns to the non-trusted state.

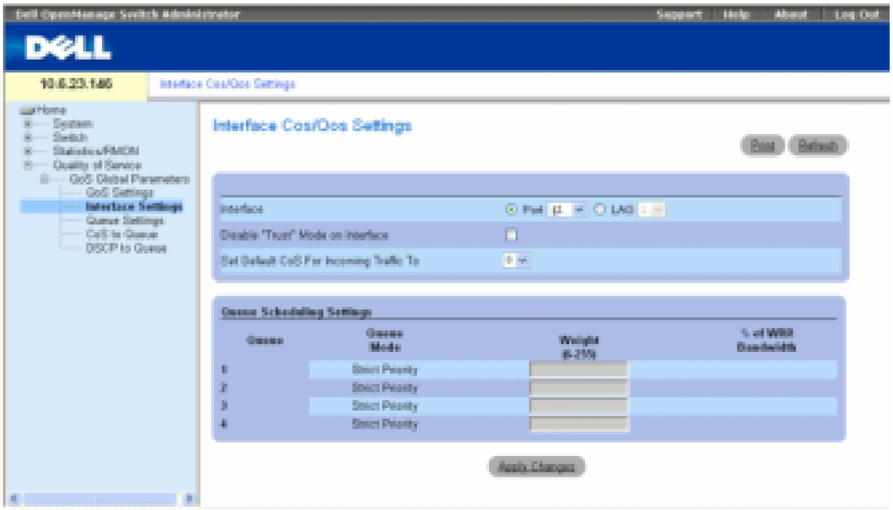
The following is an example of the CLI commands:

```
Console (config)# cos trust dscp
```

Defining QoS Interface Settings

The **Interface Cos/QoS Settings** page contains fields for defining, per interface, if the selected Trust mode is to be activated. The default priority for incoming untagged packets is also selected in the **Interface Cos/QoS Settings** page, click **Quality of Service →CoS Global Parameters→ Interface Settings** in the tree view.

Figure 9-131. Interface Cos/QoS Settings



Interface Cos/Qos Settings

Interface ● Port 1 ○ LAG 1

Disable "Trust" Mode on Interface □

Set Default CoS For Incoming Traffic To 0

Queue Scheduling Settings

Queue	Queue Mode	Weight (6-255)	% of WRR Bandwidth
1	Strict Priority		
2	Strict Priority		
3	Strict Priority		
4	Strict Priority		

Interface — The specific port or LAG to configure:

Disable "Trust" Mode on Interface —

Set Default CoS For Incoming Traffic To — Sets the default CoS tag value untagged packets. The CoS tag values are 0-7. The default value is 0.

Queue — The queue number.

Queue Mode — Indicates whether the queue is Strict Priority or WRR. This is defined in the **Queue Settings** screen.

Weight (6-255) — Assigns WRR weights to queues. This field is enabled only for queues in WRR queue mode.

% of WRR Bandwidth — The percentage translation of the weight defined in the **Weight (6-255)** field.

Assigning QoS/CoS settings for an interface:

1. Open the **Interface Cos/QoS Settings** page.
2. Select an interface in the **Interface** field.
3. Define the fields.
4. Click **Apply Changes**.

   The CoS settings are assigned to the interface.

Assigning CoS Interfaces Using the CLI Commands

The following table summarizes the equivalent CLI commands for configuring fields in the **Interface Cos/QoS Settings** page.

Table 9-95. CoS Interface CLI Commands

CLI Command	Description
qos trust	Enables trust state for each.
qos cos *default-cos*	Configures the default port CoS value.
no qos trust	Disables Trust state on each port.

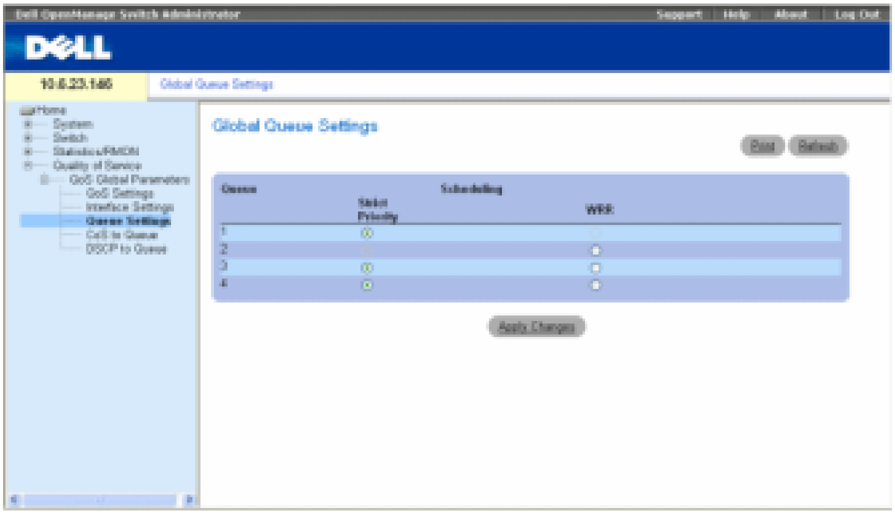
The following is an example of the CLI commands:

```
Console (config)# interface ethernet g5
Console (config-if)# qos trust
Console (config-if)# qos cos 3
```

Defining Queue Settings

The **Global Queue Setting** page contains fields for configuring the scheduling method by which the queues are maintained. To open the **Global Queue Setting** page click **Quality of Service→CoS Global Parameters→Queue Settings** in the tree view.

Figure 9-132. Global Queue Setting



Global Queue Settings

Queue	Scheduling	
	Strict Priority	WRR
1	●	○
2	○	○
3	●	○
4	●	○

Queues — The Queue number.

Strict Priority — Specifies if traffic scheduling is based strictly on the queue priority. The default is enabled.

WRR — Specifies if traffic scheduling is based on the Weighted Round Robin (WRR) weights to egress queues.

Defining the Queue Settings

1. Open the **Global Queue Setting** page.
2. Define the fields.
3. Click **Apply Changes**.

   The queue settings are defined, and the device is updated.

Assigning Queue Setting Using the CLI Commands

The following table summarizes the equivalent CLI commands for configuring fields in the **Global Queue Setting** page.

Table 9-96. Queue Settings CLI Commands

CLI Command	Description
wrr-queue bandwidth *weight1 weight2* . *weight_n*	Assigns Weighted Round Robin (WRR) weights to egress queues.
show qos interface [**ethernet** *interface-number*] [**queuing**]	Displays interface QoS data.

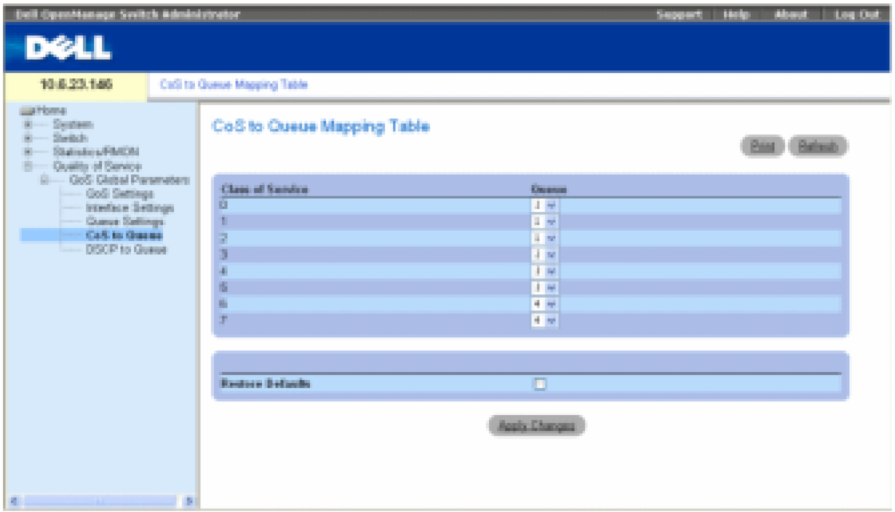
The following is an example of the CLI commands:

```
Console (config)# wrr-queue bandwidth 10 20 30 40
Console (config)# exit
Console # exit
Console> show qos interface ethernet g1 queueing
Ethernet g1
wrr bandwidth weights and EF priority:
    Console (config)# wrr-queue bandwidth 10 20 30 40
    Console (config)# exit
    Console # exit
    Console> show qos interface ethernet g1 queueing
    Ethernet g1
    wrr bandwidth weights and EF priority:

qid         weights            Ef            Priority
-----       --------           -----         ----------
1           125                Disable       N/A
2           125                Disable       N/A
3           125                Disable       N/A
4           125                Disable       N/A
    Cos queue map:
    Cos qid
    0   2
    1   1
    2   1
    3   2
    4   3
    5   3
    6   4
    7   4
```

Mapping CoS Values to Queues

The **CoS to Queue Mapping Table** page contains fields for classifying CoS settings to traffic queues. To open the **CoS to Queue Mapping Table** page, click **Quality of Service→CoS Global Parameters→CoS to Queue** in the tree view.

Figure 9-133. CoS to Queue Mapping Table



CoS to Queue Mapping Table

Class of Service	Queue
0	2
1	1
2	1
3	2
4	3
5	3
6	4
7	4

Restore Defaults ☐

Class of Service — Specifies the CoS priority tag values, where zero is the lowest and 7 is the highest.

Queue — The traffic forwarding queue to which the CoS priority is mapped. Four traffic priority queues are supported.

Restore Defaults — Restores the device factory defaults for mapping CoS values to a forwarding queue.

Mapping a CoS value to a Queue

1. Open the **CoS to Queue Mapping Table** page.
2. Select a CoS entry.
3. Define the queue number in the **Queue** field.
4. Click **Apply Changes**.

   The CoS value is mapped to a queue, and the device is updated.

Assigning CoS Values to Queues Using the CLI Commands

The following table summarizes the equivalent CLI commands for configuring fields in the **CoS to Queue Mapping Table** page.

Table 9-97. CoS to Queue Settings CLI Commands

CLI Command	Description
wrr-queue cos-map *queue-id cos1..cos*8	Maps assigned CoS values to the egress queues.

The following is an example of the CLI commands:

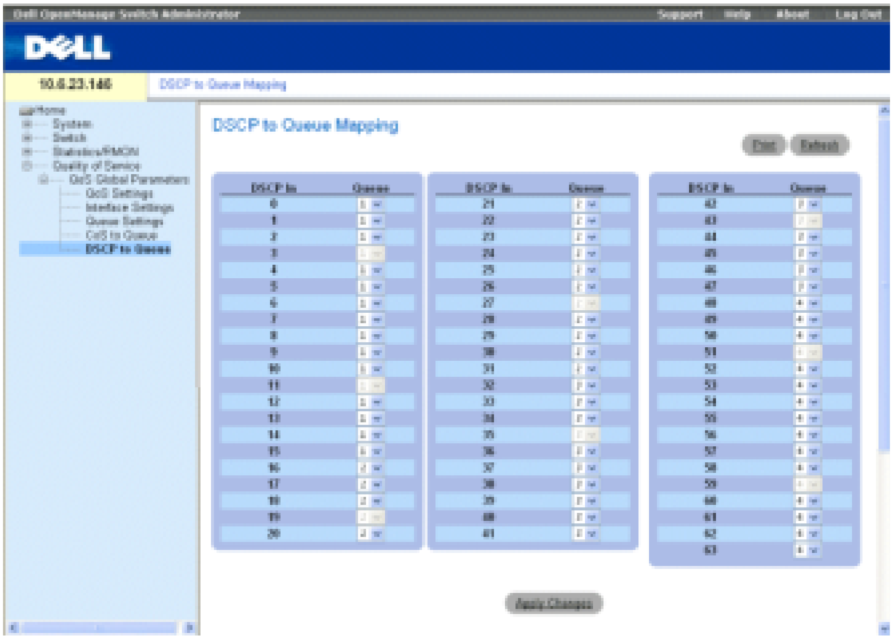
```
Console (config)# wrr-queue cos-map 4 7
```

Mapping DSCP Values to Queues

The **DSCP Mapping** page provides fields for defining output queue to specific DSCP fields. To open the **DSCP Mapping** page, click **Quality of Service→CoS Global Parameters→DSCP Mapping** in the tree view.

NOTE: For the list of the DSCP default queue settings, see "DSCP to Queue Mapping Table Default Values".

Figure 9-134. DSCP Mapping



DSCP to Queue Mapping

DSCP In	Queue	DSCP In	Queue	DSCP In	Queue
0	1	21	2	42	3
1	1	22	2	43	3
2	1	23	2	44	3
3	1	24	2	45	3
4	1	25	2	46	3
5	1	26	2	47	3
6	1	27	2	48	4
7	1	28	2	49	4
8	1	29	2	50	4
9	1	30	2	51	4
10	1	31	2	52	4
11	1	32	3	53	4
12	1	33	3	54	4
13	1	34	3	55	4
14	1	35	3	56	4
15	1	36	3	57	4
16	2	37	3	58	4
17	2	38	3	59	4
18	2	39	3	60	4
19	2	40	3	61	4
20	2	41	3	62	4
				63	4

DSCP In — The values of the DSCP field within the incoming packet.

Queue — The queue to which packets with the specific DSCP value is assigned. The values are 1-4, where one is the lowest value and four is the highest.

Mapping a DSCP value and assigning priority queue:

1. Open the **DSCP Mapping** page.
2. Select a value in the **DSCP In** column.
3. Define the **Queue** fields.
4. Click **Apply Changes**.

   The DSCP is overwritten, and the value is assigned a forwarding queue.

Assigning DSCP Values Using the CLI Commands

The following table summarizes the equivalent CLI commands for configuring fields in the **DSCP Mapping** page.

Table 9-98. DSCP Value to Queue CLI Commands

CLI Command	Description
qos map dscp-queue *dscp-list* **to** *queue-id*	Modifies the DSCP to queue mapping.

The following is an example of the CLI commands:

```
Console (config)# qos map dscp-queue 33 40 41 to 1
```

10

Device Specifications

This appendix includes the information needed for running the device.

Port and Cable Specifications

This section describes the port specifications.

Port Specifications

The following table describes the device port types, as well as, a description of the port types.

Table 10-99. Port Specifications

Device	Specification
PowerConnect 5324	• 24 GE ports • 4 SFP ports • RS-232 Console port
Port Types	
RJ-45	• 10 Base-T • 100 Base-T • 1000 Base-T
SFP	Supports Standard Small Form-Factor Gigabit Plug Transceivers
Port Settings	
	• Auto-negotiation for speed, duplex mode and flow control • Back Pressure • Head of Line Blocking • Auto MDI/MDIX • Port Mirroring • Broadcast Storm Control

Operating Conditions

This section details operating conditions including operating temperatures and humidity.

Table 10-100. Operating Conditions

Feature	Specification
Operating Temperature	0 to 40 C / 32 to 104 F
Operating Humidity	10% - 90% (non-condensing)

Physical Device Specifications

This section details operating conditions including operating temperatures and humidity.

Table 10-101. Physical Device Specifications

Feature	Specification
Unit Size	• 19“ Width • 1U Height
Ventilation	Two fans per unit.

Device Memory Specifications

This section details the device memory specifications.

Table 10-102. Device Memory Specifications

Memory Type	Amount
CPU DRAM	64MB
Flash Memory	16MB
Packet Buffer Memory	2Mb

Feature Specifications

VLAN

- VLAN support for Tagging and Port Based as per IEEE 802.1Q
- Up to 4094 VLANs Supported
- Reserved VLANs for internal system use
- Dynamic VLANs with GVRP support
- Protocol based VLANs

Quality of Service

- Layer 2 Trust Mode (IEEE 802.1p tagging)
- Layer 3 Trust Mode (DSCP)
- Adjustable Weighted Round Robin (WRR)
- Adjustable Strict Queue Scheduling

Layer 2 Multicast

- Dynamic Multicast Support - upto 256 Multicast groups supported in IGMP Snooping or static Multicast

Device Security

- Switch access password protection
- Port-based MAC Address alert and lock-down
- RADIUS remote authentication for switch management access
- TACACS+
- Management access filtering via Management Access Profiles
- SSH/SSL Management Encryptions

Additional Switching Features

- Link Aggregation with support for up to 8 Aggregated Links per device and up to 8 Ports per aggregated link (IEEE 802.3ad)
- LACP Support
- Supports Jumbo Frames up to 10K
- Broadcast Storm Control
- Port Mirroring

Device Management

- Web Based Management Interface
- CLI Accessibility via Telnet
- SNMPv1 and SNMP v2 are supported
- 4 RMON Groups Supported
- TFTP Transfers of Firmware and Configuration Files
- Dual Firmware Images On-Board
- Multiple Configuration File Upload/Download Supported
- Statistics for Error Monitoring and Performance Optimization
- BootP/DHCP IP Address Management Supported
- Syslog Remote Logging Capabilities
- SNTP Support
- Layer 3 Traceroute
- Telnet Client
- DNS Client

Glossary

This glossary contains key technical words of interest.

A B C D E F G H I J L M N O P Q R S T U V W

A

Access Mode

Specifies the method by which user access is granted to the system.

Access Profiles

Allows network managers to define profiles and rules for accessing the device. Access to management functions can be limited to user groups, which are defined by the following criteria:

- Ingress interfaces
- Source IP address and/or Source IP subnets

Aggregated VLAN

Groups several VLANs into a single aggregated VLAN. Aggregating VLANs enables routers to respond to ARP requests for nodes located on different sub-VLANs belonging to the same Super VLAN. Routers respond with their MAC address.

ARP

Address Resolution Protocol. A TCP/IP protocol that converts IP addresses into physical addresses.

ASIC

Application Specific Integrated Circuit. A custom chip designed for a specific application.

Asset Tag

Specifies the user-defined device reference.

Authentication Profiles

Sets of rules which that enables login to and authentication of users and applications.

Auto-negotiation

Allows 10/100 Mpbs or 10/100/1000 Mbps Ethernet ports to establish for the following features:

- Duplex/ Half Duplex Mode
- Flow Control
- Speed

B

Back Pressure

A mechanism used with Half Duplex mode that enables a port not to receive a message.

Backplane

The main BUS that carries information in the device.

Backup Configuration Files

Contains a backup copy of the device configuration. The Backup file changes when the Running Configuration file or the Startup file is copied to the Backup file.

Bandwidth

Bandwidth specifies the amount of data that can be transmitted in a fixed amount of time. For digital devices, bandwidth is defined in Bits per Second (bps) or Bytes per Second.

Bandwidth Assignments

The amount of bandwidth assigned to a specific application, user, and/or interface.

Baud

The number of signaling elements transmitted each second.

Best Effort

Traffic is assigned to the lowest priority queue, and packet delivery is not guaranteed.

Boot Version

The boot version.

BootP

Bootstrap Protocol. Enables a workstation to discover its IP address, an IP address of a BootP server on a network, or a configuration file loaded into the boot of a device.

BPDU

Bridge Protocol Data Unit. Provide bridging information in a message format. BPDUs are sent across device information with in Spanning Tree configuration. BPDU packets contain information on ports, addresses, priorities, and forwarding costs.

Bridge

A device that connect two networks. Bridges are hardware specific, however they are protocol independent. Bridges operate at Layer 1 and Layer 2 levels.

Broadcast Domain

Devices sets that receive broadcast frames originating from any device within a designated set. Routers bind Broadcast domains, because routers do not forward broadcast frames.

Broadcasting

A method of transmitting packets to all ports on a network.

Broadcast Storm

An excessive amount of broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses are heaped onto the network, overloading network resources or causing the network to time out.

For more information about broadcast storms, see "Defining LAG Parameters".

C

CDB

Configuration Data Base. A file containing a device’s configuration information.

Class of Service

Class of Service (CoS). Class of Service is the 802.1p priority scheme. CoS provides a method for tagging packets with priority information. A CoS value between 0-7 is added to the Layer II header of packets, where zero is the lowest priority and seven is the highest.

A overlapping transmission of two or more packets that collide. The data transmitted cannot be used, and the session is restarted.

Combo Ports

A single logical port with two physical connections, including an RJ-45 connection and an SFP connection.

CLI

Command Line Interface. A set of line commands used to configure the system. For more information on using the CLI, see **Using the CLI**.

Communities

Specifies a group of users which retains the same system access rights.

CPU

Central Processing Unit. The part of a computer that processes information. CPUs are composed of a control unit and an ALU.

D

DHCP Client

An Internet host using DHCP to obtain configuration parameters, such as a network address.

DSCP

DiffServe Code Point (DSCP). DSCP provides a method of tagging IP packets with QoS priority information.

Domain

A group of computers and devices on a network that are grouped with common rules and procedures.

Duplex Mode

Permits simultaneous transmissions and reception of data. There are two different types of duplex mode:

- **Full Duplex Mode** — Permits for bisynchronous communication, for example, a telephone. Two parties can transmit information at the same time.
- **Half Duplex Mode** — Permits asynchronous communication, for example, a walkie-talkie. Only one party can transmit information at a time.

E

Egress Ports

Ports from which network traffic is transmitted.

End System

An end user device on a network.

Ethernet

Ethernet is standardized as per IEEE 802.3. Ethernet is the most common implemented LAN standard. Supports data transfer rates of Mpbs, where 10, 100 or 1000 Mbps is supported.

EWS

Embedded Web Server. Provides device management via a standard web browser. Embedded Web Servers are used in addition to or in place of a CLI or NMS.

F

FFT

Fast Forward Table. Provides information about forwarding routes. If a packet arrives to a device with a known route, the packet is forwarded via a route listed in the FFT. If there is not a known route, the CPU forwards the packet and updates the FFT.

FIFO

First In First Out. A queuing process where the first packet in the queue is the first packet out of the packet.

Flapping

Flapping occurs when an interfaces state is constantly changing. For example, an STP port constantly changes from listening to learning to forwarding. This may cause traffic loss.

Flow Control

Enables lower speed devices to communicate with higher speed devices, that is, that the higher speed device refrains from sending packets.

Fragment

Ethernet packets smaller than 576 bits.

Frame

Packets containing the header and trailer information required by the physical medium.

G

GARP

General Attributes Registration Protocol. Registers client stations into a Multicast domain.

Gigabit Ethernet

Gigabit Ethernet transmits at 1000 Mbps, and is compatible with existing 10/100 Mbps Ethernet standards.

GVRP

GARP VLAN Registration Protocol. Registers client stations into a VLANs.

H

HOL

Head of Line. Packets are queued. Packets at the head of the queue are forwarded before packets at the end of the line.

Host

A computer that acts as a source of information or services to other computers.

HTTP

HyperText Transport Protocol. Transmits HTML documents between servers and clients on the internet.

I

IC

Integrated Circuit. Integrated Circuits are small electronic devices composed from semiconductor material.

ICMP

Internet Control Message Protocol. Allows gateway or destination host to communicate with a source host, for example, to report a processing error.

IEEE

Institute of Electrical and Electronics Engineers. An Engineering organization that develops communications and networking standards.

IEEE 802.1d

Used in the Spanning Tree Protocol, IEEE 802.1d supports MAC bridging to avoid network loops.

IEEE 802.1p

Prioritizes network traffic at the data-link/MAC sublayer.

IEEE 802.1Q

Defines the operation of VLAN Bridges that permit the definition, operation, and administration of VLANs within Bridged LAN infrastructures.

Image File

System images are saved in two Flash sectors called images (Image 1 and Image 2). The active image stores the active copy; while the other image stores a second copy.

Ingress Port

Ports on which network traffic is received.

IP

Internet Protocol. Specifies the format of packets and there addressing method. IP addresses packets and forwards the packets to the correct port.

IP Address

Internet Protocol Address. A unique address assigned to a network device with two or more interconnected LANs or WANs.

IPX

Internetwork Packet Exchange. Transmits connectionless communications.

J

Jumbo Frames

Enables transporting the identical data in fewer frames. Jumbo Frames reduce overhead, lower processing time, and ensures fewer interrupts.

L

LAG

Link Aggregated Group. Aggregates ports or VLANs into a single virtual port or VLAN.

For more information on LAGs, see **Defining LAG Membership**.

LAN

Local Area Networks. A network contained within a single room, building, campus or other limited geographical area.

Layer 2

Data Link Layer or MAC Layer. Contains the physical address of a client or server station. Layer 2 processing is faster than Layer 3 processing because there is less information to process.

Layer 4

Establishes a connections and ensures that all data arrives to their destination. Packets inspected at the Layer 4 level are analyzed and forwarding decisions based on their applications.

Load Balancing

Enables the even distribution of data and/or processing packets across available network resources. For example, load balancing may distribute the incoming packets evenly to all servers, or redirect the packets to the next available server.

M

MAC Address

Media Access Control Address. The MAC Address is a hardware specific address that identifies each network node.

MAC Address Learning

MAC Address Learning characterizes a learning bridge, in which the packet's source MAC address is recorded. Packets destined for that address are forwarded only to the bridge interface on which that address is located. Packets addressed to unknown addresses are forwarded to every bridge interface. MAC Address Learning minimizes traffic on the attached LANs.

MAC Layer

A sub-layer of the *Data Link Control* (DTL) layer.

Mask

A filter that includes or excludes certain values, for example parts of an IP address.

For example, Unit 2 is inserted in the first minute of a ten-minute cycle, and Unit 1 is inserted in fifth minute of the same cycle, the units are considered the same age.

MD5

Message Digest 5. An algorithm that produces a 128-bit hash. MD5 is a variation of MD4, and increases MD4 security. MD5 verifies the integrity of the communication, authenticates the origin of the communication.

MDI

Media Dependent Interface. A cable used for end stations.

MDIX

Media Dependent Interface with Crossover (MDIX). A cable used for hubs and switches.

MIB

Management Information Base. MIBs contain information describing specific aspects of network components.

Multicast

Transmits copies of a single packet to multiple ports.

N

NMS

Network Management System. An interface that provides a method of managing a system.

Node

A network connection endpoint or a common junction for multiple network lines. Nodes include:

- Processors
- Controllers

- Workstations

O

OID

Object Identifier. Used by SNMP to identify managed objects. In the SNMP Manager/ Agent network management paradigm, each managed object must have an OID to identify it.

P

Packets

Blocks of information for transmission in packet switched systems.

PDU

Protocol Data Unit. A data unit specified in a layer protocol consisting of protocol control information and layer user data.

PING

Packet Internet Groper. Verifies if a specific IP address is available. A packet is sent to another IP address and waits for a reply.

Port

Physical ports provide connecting components that allow microprocessors to communicate with peripheral equipment.

Port Mirroring

Monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from one port to a monitoring port.

For more information on port mirroring, see **Defining Port Mirroring Sessions**.

Port Speed

Indicates port speed of the port. Port speeds include:

- Ethernet 10 Mbps
- Fast Ethernet 100Mbps
- Gigabit Ethernet 1000 Mbps

Protocol

A set of rules that governs how devices exchange information across networks.

Q

QoS

Quality of Service. QoS allows network managers to decide how and what network traffic is forwarded according to priorities, application types, and source and destination addresses.

Query

Extracts information from a database and presents the information for use.

R

RADIUS

Remote Authentication Dial-In User Service. A method for authenticating system users, and tracking connection time.

RMON

Remote Monitoring. Provides network information to be collected from a single workstation.

Router

A device that connects to separate networks. Routers forward packets between two or more networks. Routers operate at a Layer 3 level.

RSTP

Rapid Spanning Tree Protocol. Detects and uses network topologies that allow a faster convergence of the spanning tree, without creating forwarding loops.

Running Configuration File

Contains all Startup file commands, as well as all commands entered during the current session. After the device is powered down or rebooted, all commands stored in the Running Configuration file are lost.

S

Segmentation

Divides LANs into separate LAN segments for bridging and routing. Segmentation eliminates LAN bandwidth limitations.

Server

A central computer that provides services to other computers on a network. Services may include file storage and access to applications.

SNMP

Simple Network Management Protocol. Manages LANs. SNMP based software communicates with network devices with embedded SNMP agents. SNMP agents gather network activity and device status information, and send the information back to a workstation.

SNTP

Simple Network Time Protocol. SNTP assures accurate network switch clock time synchronization up to the millisecond.

SoC

System on a Chip. An ASIC that contains an entire system. For example, a telecom SoC application can contain a microprocessor, digital signal processor, RAM, and ROM.

Spanning Tree Protocol

Prevents loops in network traffic. The Spanning Tree Protocol (STP) provides tree topography for any arrangement of bridges. STP provides one path between end stations on a network, eliminating loops.

SSH

Secure Shell. Logs into a remote computer via a network, executes commands, and to transfers files from one computer to another.

Startup Configuration

Retains the exact device configuration when the device is powered down or rebooted.

Subnet

Sub-network. Subnets are portions of a network that share a common address component. On TCP/IP networks, devices that share a prefix are part of the same subnet. For example, all devices with a prefix of 157.100.100.100 are part of the same subnet.

Subnet Mask

Used to mask all or part of an IP address used in a subnet address.

Switch

Filters and forwards packets between LAN segments. Switches support any packet protocol type.

T

TCP/IP

Transmissions Control Protocol. Enables two hosts to communicate and exchange data streams. TCP guarantees packet delivery, and guarantees packets are transmitted and received in the order their sent.

Telnet

Terminal Emulation Protocol. Enables system users to log in and use resources on remote networks.

TFTP

Trivial File Transfer Protocol. Uses User Data Protocol (UDP) without security features to transfer files.

Trap

A message sent by the SNMP that indicates that system event has occurred.

Trunking

Link Aggregation. Optimizes port usage by linking a group of ports together to form a single trunk (aggregated groups).

U

UDP

User Data Protocol. Transmits packets but does not guarantee their delivery.

Unicast

A form of routing that transmits one packet to one user.

V

VLAN

Virtual Local Area Networks. Logical subgroups with a Local Area Network (LAN) created via software rather than defining a hardware solution.

W

WAN

Wide Area Networks. Networks that cover a large geographical area.

Wildcard Mask

Specifies which IP address bits are used, and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all the bits are important.

For example, if the destination IP address 149.36.184.198 and the wildcard mask is 255.36.184.00, the first two bits of the IP address are used, while the last two bits are ignored.

Index