Dell™ PowerConnect™ 34XX Systems

User's 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.

May 2005 Rev A01

Contents

2 Hardware Description

3 Installing the PowerConnect 3424/P and PowerConnect 3448/P

6 Configuring System Information

Figures

Tables

1

Introduction

PowerConnect 3424/3448 and PowerConnect 3424P/3448P are stackable, advanced multi-layer devices. PowerConnect units can function either as stand-alone, multi-layer, switching devices or stackable devices with up to six stacking members.

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

System Description

PowerConnect 3424/3448 and PowerConnect 3424P/3448P combine versatility with minimal management. The PowerConnect 3424 and 3448 series include the following device types:

- PowerConnect 3424
- PowerConnect 3424P
- PowerConnect 3448
- PowerConnect 3448P

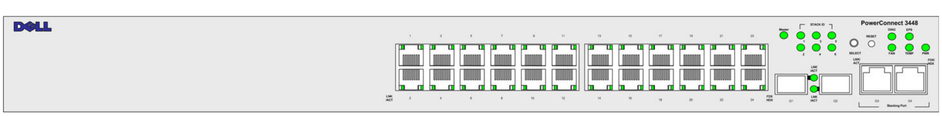
PowerConnect 3424

The PowerConnect 3424 provides 24 10/100Mbps ports plus two SFP ports, and two Copper ports which can be used to forward traffic in a stand-alone device, or as stacking ports when the device is stacked. The device also provides one RS-232 console port. The PowerConnect 3424 is a stackable device, but also operates as a stand-alone device.

PowerConnect 3424P

The PowerConnect 3424P provides 24 10/100Mbps ports plus two SFP ports, and two Copper ports which can be used to forward traffic in a stand-alone device, or as stacking ports when the device is stacked. The device also provides one RS-232 console port. The PowerConnect 3424P is a stackable device, but also operates as a stand-alone device. The PowerConnect 3424P also provides Power over Ethernet (PoE).

Figure 1-1. PowerConnect 3424 and PowerConnect 3424P



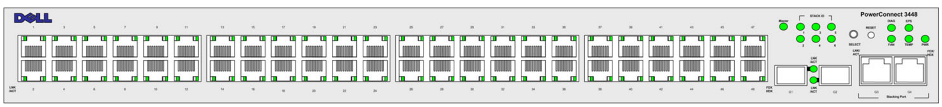
PowerConnect 3448

The PowerConnect 3448 provides 48 10/100Mbps ports plus two SFP ports, and two Copper ports which can be used to forward traffic in a stand-alone device, or as stacking ports when the device is stacked. The device also provides one RS-232 console port. The PowerConnect 3448 is a stackable device, but also functions as a stand-alone device.

PowerConnect 3448P

The PowerConnect 3448P provides 48 10/100Mbps ports, two SFP ports, and two copper ports that can be used to forward traffic when the device is in stand-alone mode, or as stacking ports when the device is part of a stack. The device also provides one RS-232 console port. In addition, PowerConnect 3448P provides PoE.

Figure 1-2. PowerConnect 3448 and PowerConnect 3448P



Stacking Overview

PowerConnect 3424/P and PowerConnect 3448/P stacking provides multiple switch management through a single point as if all stack members are a single unit. All stack members are accessed through a single IP address through which the stack is managed. The stack is managed from a:

- Web-based interface
- SNMP Management Station
- Command Line Interface (CLI)

PowerConnect 3424/P and PowerConnect 3448/P devices support stacking up to six units per stack, or can operate as stand-alone units.

During the Stacking setup, one switch is selected as the Stack Master and another stacking member can be selected as the Backup Master. All other devices are selected as stack members, and assigned a unique Unit ID.

Switch software is downloaded separately for each stack members. However, all units in the stack must be running the same software version.

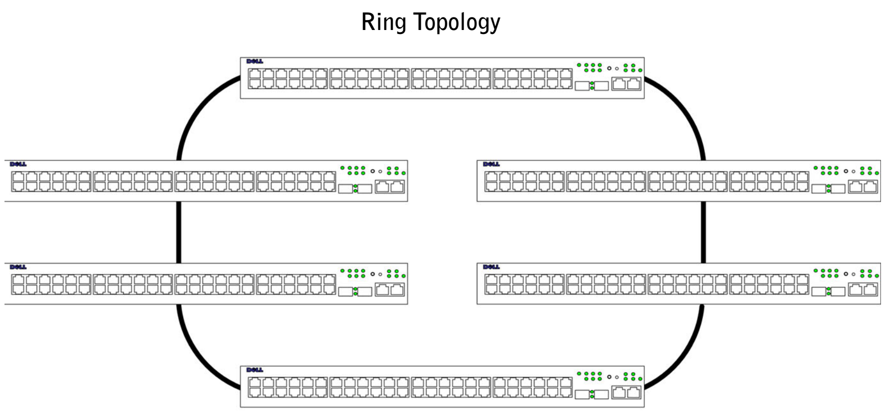
Switch stacking and configuration is maintained by the Stack Master. The Stack Master detects and reconfigures the ports with minimal operational impact in the event of:

- Unit Failure
- Inter-unit Stacking Link Failure
- Unit Insertion
- Removal of a Stacking Unit

Understanding the Stack Topology

The PowerConnect 3400 series operates in a Ring topology. A stacked Ring topology is where all devices in the stack are connected to each other forming a circle. Each device in the stack accepts data and sends it to the device to which it is attached. The packet continues through the stack until it reaches its destination. The system discovers the optimal path on which to send traffic.

Figure 1-3. Stacking Ring Topology



Most difficulties incurred in Ring topologies occur when a device in the ring becomes non-functional, or a link is severed. With the PowerConnect 3424/P and PowerConnect 3448/P stack, the system automatically switches to a Stacking Failover topology without any system downtime. An SNMP message is automatically generated, but no stack management action is required. However, the stacking link or stacking member must be repaired to ensure the stacking integrity.

After the stacking issues are resolved, the device can be reconnected to the stack without interruption, and the Ring topology is restored.

Stacking Failover Topology

If a failure occurs in the stacking topology, the stack reverts to Stacking Failover Topology. In the Stacking Failover topology, devices operate in a chain formation. The Stack Master determines where the packets are sent. Each unit is connected to two neighboring devices, except for the top and bottom units.

Stacking Members and Unit ID

Stacking Unit IDs are essential to the stacking configuration. The stacking operation is determined during the boot process. The operation mode is determined by the Unit ID selected during the initialization process. For example, if the user selected the stand-alone mode, the device boots in the boot-up process as a stand-alone device.

The device units are shipped with a default Unit ID of the stand-alone unit. If the device is operating as a stand-alone unit, all stacking LEDs are off.

Once the user selects a different Unit ID, it is not erased, and remains valid, even if the unit is reset.

Unit ID 1 and Unit ID 2 are reserved for Master enabled units. Unit IDs 3 to 6 can be defined for stack members.

When the Master unit boots or when inserting or removing a stack member, the Master unit initiates a stacking discovering process.

NOTE: If two members are discovered with the same Unit ID the stack continues to function, however only the unit with the older join time joins the stack. A message is sent to the user, notifying that a unit failed to join the stack.

Removing and Replacing Stacking Members

Unit 1 and Unit 2 are Master enabled units. Unit 1 and Unit 2 are either designated as Master Unit or Backup Master Unit. The stack Master assignment is performed during the configuration process. One Master enabled stack member is elected as Master, and the other Master enabled stack member is elected as Backup Master, according to the following decision process:

- If only one Stack Master enabled unit is present, it is elected as the Master.
- If two Master enabled stacking members are present, and one has been manually configured as the Stack Master, the manually configured member is elected as Stack Master.
- If two Master enabled units are present and neither has been manually configured as the Master, the one with the longer up-time is elected as the Stack Master.
- If two Master enabled units are present and both have been manually configured as the Master, the one with the longer up-time is elected as the Stack Master.
- If the two Master enabled stacking members are the same age, Unit 1 is elected as the Stack Master.

  NOTE: Two stacking member are considered the same age if they were inserted within a ten minute interval.

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 to be the same age. If there are two Master enabled stack members that are the same age, then Unit 1 is elected master.

The Stack Master and the Backup Master maintain a Warm Standby. The Warm Standby ensures that the Backup Master takes over for the Stack Master if a failover occurs. This guarantees that the stack continues to operate normally.

During the Warm Standby, the Master and the Backup Master are synchronized with the static configuration only. When the Stacking Master is configured, the Stack Master must synchronize the Stacking Backup Master. The Dynamic configuration is not saved, for example, dynamically learned MAC addresses are not saved.

Each port in the stack has a specific Unit ID, port type, and port number, which are part of both the configuration commands and the configuration files. Configuration files are managed only from the device Stack Master, including:

- Saving to the FLASH
- Uploading Configuration files to an external TFTP Server
- Downloading Configuration files from an external TFTP Server

NOTE: Stack configuration for all configured ports is saved, even if the stack is reset and/or the ports are no longer present.

Whenever a reboot occurs, topology discovery is performed, and the Master learns all units in the stack. Unit IDs are saved in the unit and are learned through topology discovery. If a unit attempts to boot without a selected Master, and the unit is not operating in stand-alone mode, the unit does not boot.

Configuration files are changed only through explicit user configuration. Configuration files are not automatically modified when:

- Units are Added
- Units are Removed
- Units are reassigned Unit IDs
- Units toggle between Stacking Mode and Stand-alone Mode

Each time the system reboots, the Startup Configuration file in the Master unit is used to configure the stack.

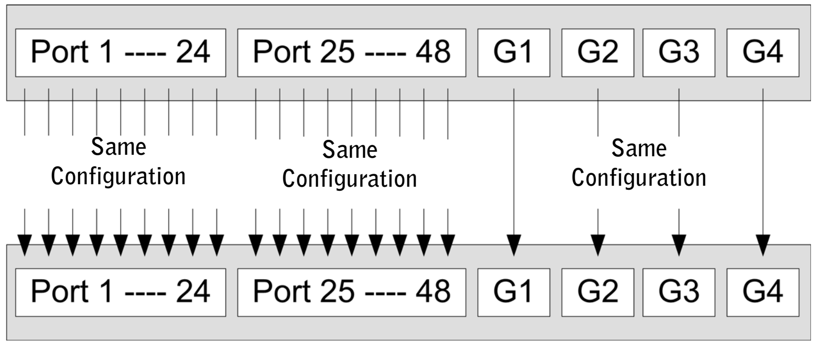
If a stack member is removed from the stack, and then replaced with a unit with the same Unit ID, the stack member is configured with the original device configuration. Only ports which are physically present are displayed in the PowerConnect OpenManage Switch Administrator home page, and can be configured through the web management system. Non-present ports are configured through the CLI or SNMP interfaces.

Exchanging Stacking Members

If a stack member with the same Unit ID replaces an existing Unit ID with the same Unit ID, the previous device configuration is applied to the inserted stack member. If the new inserted device has either more or fewer ports than the previous device, the relevant port configuration is applied to the new stack member. For example,

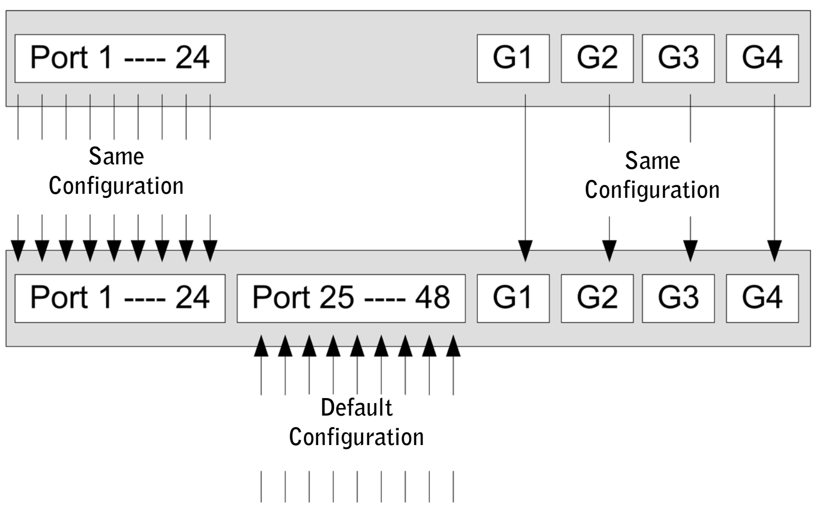
- If a PowerConnect 3424/P replaces PowerConnect 3424/P, all port configurations remain the same.
- If a PowerConnect 3448/P replaces the PowerConnect 3448/P, all port configurations remain the same.

Figure 1-4. PowerConnect 3448/P replaces PowerConnect 3448/P



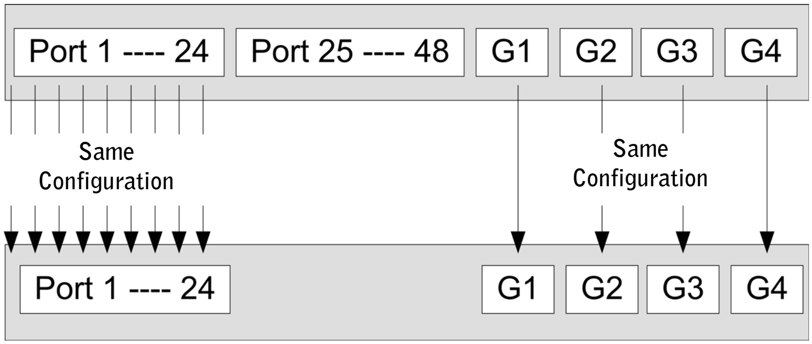
- If a PowerConnect 3448/P replaces PowerConnect 3424/P, the first 3448/P 24 FE ports receive the 3424/P 24 FE port configuration. The GE port configurations remain the same. The remaining ports receive the default port configuration.

Figure 1-5. PowerConnect 3424/P port replaces PowerConnect 3448/P port



- If a PowerConnect 3424/P replaces PowerConnect 3448/P, the PowerConnect 3424/P 24 FE ports receives the first 24 FE PowerConnect 3448/P port configuration. The GE port configurations remain the same.

Figure 1-6. PowerConnect 3448/P port replaces PowerConect 3424/P Port



Switching from the Stack Master to the Backup Stack Master

The Backup Master replaces the Stack Master if the following events occur:

- The Stack Master fails or is removed from the stack.
- Links from the Stack Master to the stacking members fails.
- A soft switchover is performed with either via web interface or the CLI.

Switching between the Stack Master and the Backup Master results in a limited service loss. Any dynamic tables are relearned if a failure occurs. The running configuration file is synchronized between Stack Master and the Backup Master, and continues running on the Backup Master.

Features Overview

This section describes the device features. For a complete list of all updated device features, see the latest software version **Release Notes**.

Power over Ethernet

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

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

For more information about Power over Ethernet, see "Managing Power over Ethernet".

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.

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 Configuration" 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 Flow Control for ports or LAGs, see "Defining Port Configuration" or "Defining LAG Parameters."

Virtual Cable Testing (VCT)

VCT detects and reports copper link cabling occurrences such as open cables and cable shorts. For more information on testing cables, see "Running Cable Diagnostics".

MDI/MDIX Support

The device automatically detects whether the cable connected to an RJ-45 port is crossed or straight through, when auto-negotiation is enabled.

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/MDIX for ports or LAGs, see "Defining Port Configuration" or "Defining LAG Parameters."

Auto Negotiation

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

The PowerConnect 3400 series enhances auto negotiation by providing port advertisement. Port advertisement allows the system administrator to configure the port speeds that are advertised.

For more information on auto-negotiation, see "Defining Port Configuration" or "Defining LAG Parameters."

MAC Address Supported Features

MAC Address Capacity Support

The device supports up to 8K MAC addresses. The device reserves specific MAC addresses for system use.

Static MAC Entries

MAC entries can be manually entered in the Bridging Table, as an alternative to learning them from incoming frames. These user-defined entries are not subject to aging, and are preserved across resets and reboots.

For more information, see "Defining Static Addresses."

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 "Viewing Dynamic Addresses."

VLAN-aware MAC-based Switching

The device always performs VLAN-aware bridging. Classic bridging(IEEE802.1D) is not performed, where frames are forwarded based only on their destination MAC address. However, a similar functionality can be configured for untagged frames. Frames addressed to a destination MAC address that is not associated with any port are flooded to all ports of the relevant VLAN.

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 "Assigning Multicast Forward All Parameters."

Layer 2 Features

IGMP Snooping

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."

Full 802.1Q VLAN Tagging Compliance

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

GVRP Support

GARP VLAN Registration Protocol (GVRP) provides IEEE 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q 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 Parameters."

Private VLANs

Private VLAN ports, a Layer 2 security feature, provide isolation between ports within the same Broadcast domain.

For more information on Private VLANs, see "Configuring Private VLANs".

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 Static Addresses."

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 "Defining Rapid Spanning Tree."

IEEE 802.1s Multiple Spanning Tree

Multiple Spanning Tree (MSTP) operation maps VLANs into STP instances. MSTP provides differing load balancing scenario. Packets assigned to various VLANs are transmitted along different paths within MSTP Regions (MST Regions). Regions are one or more MSTP bridges by which frames can be transmitted. The standard lets administrators assign VLAN traffic to unique paths.

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

Link Aggregation

Link Aggregation

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

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

LAG is composed of ports with the same speed, set to full-duplex operation.

For more information, see "Defining LAG Parameters."

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 devices. LACP automatically determines, configures, binds, and monitors the port binding within the system.

For more information, see "Aggregating Ports."

BootP and DHCP Clients

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 SNMP traps to a Trap Recipient List.

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

SNMP Versions 1, 2 and 3

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

For more information, see "Defining SNMP Parameters".

Web Based Management

With the 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

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

For more information, see "Managing Files."

TFTP Trivial File Transfer Protocol

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

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

SNTP

The Simple Network Time Protocol (SNTP) assures accurate network Ethernet Switch clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. 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."

Domain Name System

Domain Name System (DNS) converts user-defined domain names into IP addresses. Each time a domain name is assigned the DNS service translates the 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.

For more information, see "Configuring Domain Name Systems".

Traceroute

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

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 Settings."

SSH

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

TACACS+

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

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

Password Management

Password management provides increased network security and improved password control. Passwords for SSH, Telnet, HTTP, HTTPS, and SNMP access are assigned security features. For more information on Password Management, see "Managing Passwords".

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 about the command description, syntax, default values, guidelines, and examples.

2

Hardware Description

Port Description

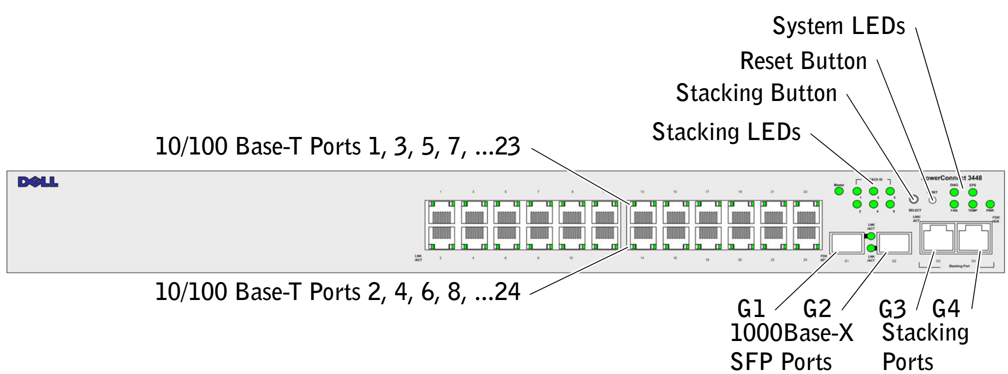
PowerConnect 3424 Port Description

The PowerConnect 3424 device is configured with the following ports:

- **24 Fast Ethernet ports** — RJ-45 ports designated as 10/100Base-T ports
- **2 Fiber ports** — Designated as 1000Base-X SFP ports
- **2 Gigabit ports** — Designated as 1000Base-T ports
- **Console port** — RS-232 based port

The following figure illustrates the PowerConnect 3424 front panel.

Figure 2-1. PowerConnect 3424 Front Panel



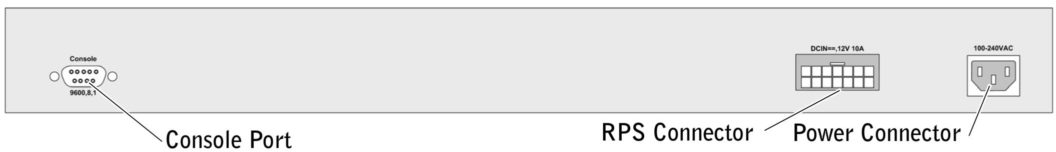
The front panel contains 24 RJ-45 ports number 1-24. The upper row of ports is marked with odd numbers 1-23, and the lower row of ports is marked with even numbers 2-24. In addition, the front panel also contains ports G1 - G2 which are fiber ports and ports G3- G4 which are copper ports. Ports G3 - G4 can either be used as stacking ports, or used to forward network traffic in a stand-alone device.

There are two buttons on the front panel. The Stack ID button is used to select the unit number. The second button is the Reset Button which is used to manually reset the device. The Reset button does not extend beyond the unit's front panel surface, so reset by pressing it accidentally is prevented. On the front panel are all the device LEDs.

The following figure illustrates the PowerConnect 3424 back:

Figure 2-2. PowerConnect 3424 Back Panel

The back panel contains an RPS connector, console port, and power connector.



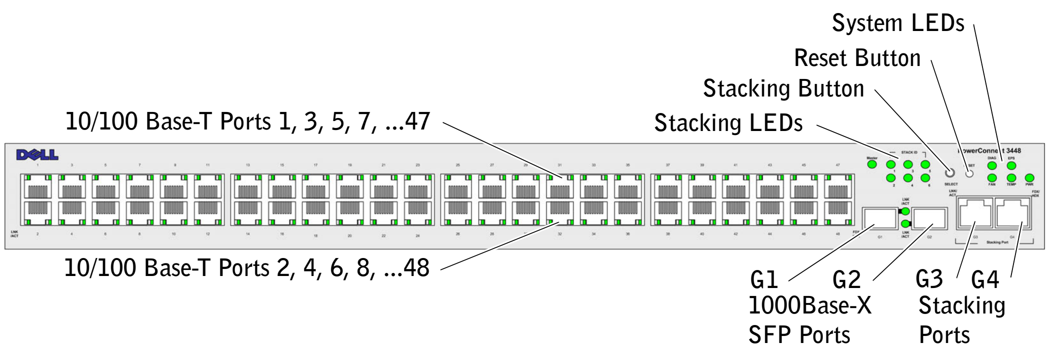
PowerConnect 3448 Port Description

The PowerConnect 3448 device is configured with the following ports:

- **48 FE ports** — RJ-45 ports designated as 10/100Base-T ports
- **2 Fiber ports** — Designated as 1000Base-X SFP ports
- **2 Gigabit ports** — Designated as 1000Base-T ports
- **Console port** — RS-232 Console based port

The following figure illustrates the PowerConnect 3448 front panel.

Figure 2-3. PowerConnect 3448 Front Panel

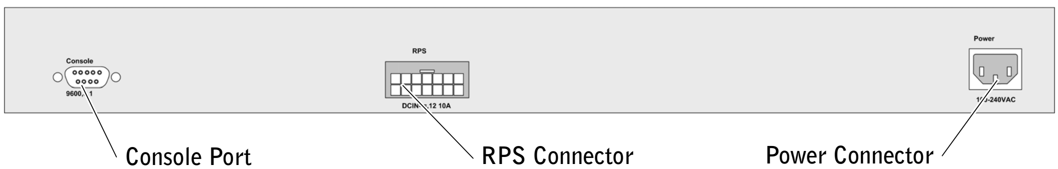


The front panel contains 48 RJ-45 ports number 1-48. The upper row of ports is marked by odd numbers 1-47, and the lower row of ports is marked with even numbers 2-48. In addition, the front panel also contains ports G1 - G2 which are fiber ports and ports G3- G4 which are copper ports. Ports G3- G4 can either be used as stacking ports, or used to forward network traffic in a stand-alone device.

There are two buttons on the front panel. The Stack ID button is used to select the unit number. The second button is the Reset Button which is used to manually reset the device. The Reset button does not extend beyond the unit's front panel surface, so reset by pressing it accidentally is prevented. On the front panel are all the device LEDs.

The following figure illustrates the PowerConnect 3448 back panel:

Figure 2-4. PowerConnect 3448 Back Panel



The back panel contains an RPS connector, console port and power connector.

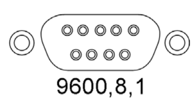
SFP Ports

The Small Form Factor Plugable (SFP) ports are a Two-Wire Serial Interface (TWSI) for communication via a Complex Programmable Logic Device (CPLD) which is designated as 1000Base-SX or LX.

RS-232 Console Port

One DB-9 connector for a terminal connection is used for debugging, software download etc. The default baud rate is 9,600 bps. The baud rate can be configured from 2400 bps up to 115,200 bps.

Figure 2-5. Console Port



Physical Dimensions

The PowerConnect 3424/P and PowerConnect 3448/P devices have the following physical dimensions:

PoE Model:

- **Width** — 440 mm (17.32 inch)
- **Depth** — 387 mm (15.236 inch)
- **Height** — 43.2 mm (1.7 inch)

Non-PoE Device:

- **Width** — 440 mm (17.32 inch)
- **Depth** — 257 mm (10.118 inch)
- **Height** — 43.2 mm (1.7 inch)

LED Definitions

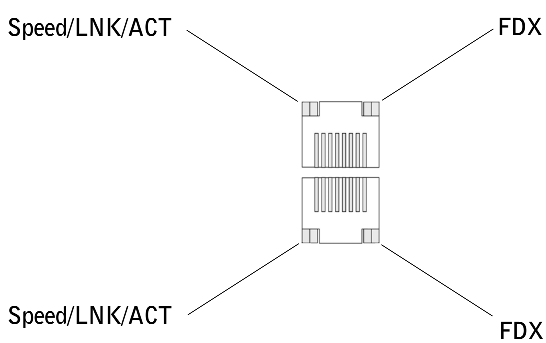
The front panel contains light emitting diodes (LED) that indicate the status of links, power supplies, fans, and system diagnostics.

Port LEDs

Each 10/100/1000 Base-T port and 10/100 Base-T port has two LEDs. The speed LED is located on the left side of the port, while the link/duplex/activity LED is located on the right side.

The following figure illustrates the 10/100 Base-T port LEDs on The PowerConnect 3424 /P and PowerConnect 3448/P switches:

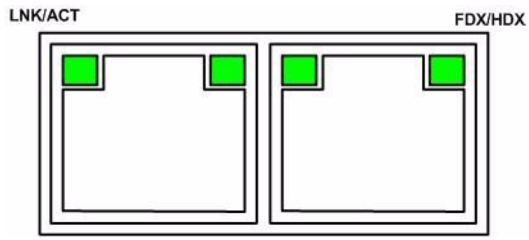
Figure 2-6. RJ-45 Copper Based 10/100 BaseT LEDs



The RJ-45 100 Base-T port on the PowerConnect 3424 /P and PowerConnect 3448/P has two LEDs marked as LNK/ACT.

The following figure illustrates the 100 Base-T LEDs.

Figure 2-7. RJ-45 1000 BaseT LED



The RJ-45 LED indications for PowerConnect 3424 and PowerConnect 3448 are described in the following table:

Table 2-1. PowerConnect 3424 and PowerConnect 3448 RJ-45 100BaseT LED Indications

LED	Color	Description
Link/Activity/Speed	Green Static	The port is running at 100 Mbs.
	Green Flashing	The port is either transmitting or receiving data at 100 Mbps.
	Yellow Static	The port is running at 10 Mbs.
	Yellow Flashing	The port is either transmitting or receiving data at 10 Mbps.
	OFF	The port is currently not operating.
FDX	Green Static	The port is currently operating in Full Duplex mode.
	OFF	The port is currently operating in Half Duplex mode,

The RJ-45 LED indications for PowerConnect 3424P and PowerConnect 3448P are described in the following table:

Table 2-2. PowerConnect 3424P and PowerConnect 3448P RJ-45 Copper based 100BaseT LED Indications

LED	Color	Description
Speed/Link/Act	Green Static	The port is currently linked at 100 Mbps.
	Green Flashing	The ports is currently operating at 100 Mbps.
	OFF	The port is currently operating at 10 Mbps or is not linked.
FDX	Green Static	The Powered Device (PD) is detected and is operating at normal load. For more information about Powered Devices, see "*Managing Power over Ethernet*".
	Green Flashing	The port is operating at transitional mode. The PD is being detected, or is faulty. For more information about Power over Ethernet, see "*Managing Power over Ethernet*".
	Amber Static	An overload or short has occurred on the Powered Device. For more information about Power over Ethernet faults, see "*Managing Power over Ethernet*".
	Amber Flashing	The powered device power conception exceeds the predefined power allotment. For more information about Power over Ethernet power allotments, see "*Managing Power over Ethernet*".
	OFF	No powered device is detected.

Gigabit Port LEDs

The following table describes the Gigabit (stacking port) LEDs:

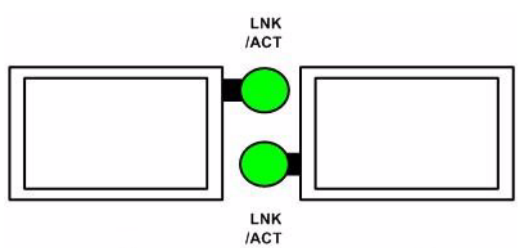
Table 2-3. PowerConnect 3424 and PowerConnect 3448 RJ-45 Copper based 100BaseT LED Indications

LED	Color	Description
Link/Activity/Speed	Green Static	The port is running at 1000 Mbs.
	Green Flashing	The port is either transmitting or receiving data at 1000 Mbps.
	Yellow Static	The port is running at 10 or 100Mbs.
	Yellow Flashing	The port is either transmitting or receiving data at 10 or 100 Mbps.
	OFF	The port is currently not operating.
FDX	Green Static	The port is currently operating in Full Duplex mode.
	OFF	The port is currently operating in Half Duplex mode.

SFP LEDs

The SFP ports each have one LED marked as LNK/ACT. On the PowerConnect 3424/P and PowerConnect 3448/P devices, the LEDs are located between ports and are round in shape. The following figures illustrate the LEDs on each device.

Figure 2-8. SFP Port LEDs



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

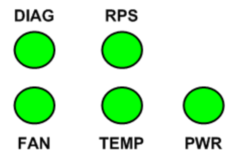
Table 2-4. SFP Port LED Indications

LED	Color	Description
Link/Activity	Green Static	A link is established.
	Green Flashing	The port is currently transmitting or receiving data.
	OFF	The port is currently not linked.

System LEDs

The system LEDs of The PowerConnect 3424 /P and PowerConnect 3448/P devices provide information about the power supplies, fans, thermal conditions, and diagnostics. The following figure illustrates the system LEDS.

Figure 2-9. System LEDs



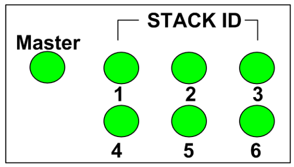
The following table describes the system LED indications.

Table 2-5. System LED Indicators

LED	Color	Description
Power Supply (PWR)	Green Static	The switch is turned on.
	OFF	The switch is turned off.
Redundant Power Supply (RPS) (models: 3424 and 3448)	Green Static	The RPS is currently operating.
	Red Static	The RPS failed.
	OFF	The redundant power supply is not plugged in.
Redundant Power Supply (RPS) (models: 3424P and 3448P)	Green Static	The RPS is currently operating.
	OFF	The redundant power supply has failed or is not plugged in.
Diagnostics (DIAG)	Green Flashing	The system diagnostic test is currently in progress.
	Green Static	The system diagnostic test passed successfully.
	Red Static	The system diagnostic test failed.
	OFF	The system is operating normally.
Temperature (TEMP)	Red Static	The device has crossed the permitted temperature range.
	OFF	The device is operating within the permitted temperature range.
Fan (FAN)	Green Static	All device fans are operating normally.
	Red Static	One or more of the device fans is not operating.

The Stacking LEDs indicate the unit position in the stack. The following figure illustrates the LEDs on the front panel.

Figure 2-10. Stacking LEDs



The Stacking LEDs are numbered 1- 6. Each stacking unit has one stacking LED lit, indicating its Unit ID number. If either Stacking LED 1 or 2 is lit, it indicates that the device is either the Stack Master or Backup Master.

Table 2-6. Stacking LED Indications

LED	Color	Description
All Stacking LEDs	OFF	The switch is currently a stand-alone device.
Stacking LED 1-6 (S1-S6)	Green Static	The device is designated as Stacking Unit N.
	OFF	The device is not designated as Stacking Unit N.
Stacking Master LED	Green Static	The device is the Stack Master
	OFF	The device is not the Stack Master.

Power Supplies

The device has an internal power supply unit (AC unit) and a connector to connect PowerConnect 3424/P and PowerConnect 3448/P devices to a PowerConnect EPS-470 unit, or to connect PowerConnect 3424 and PowerConnect 3448 devices to a PowerConnect RPS-600 unit. The PowerConnect 3424/P and PowerConnect 3448/P devices have an internal power supply (12 Volt).

Operation with both power supply units is regulated through load sharing. Power supply LEDs indicate the status of the power supply.

The PowerConnect 3424/P and PowerConnect 3448/P devices have an internal power supply of 470W (12V/-48V), with a total of 370W for 24 ports PoE device.

AC Power Supply Unit

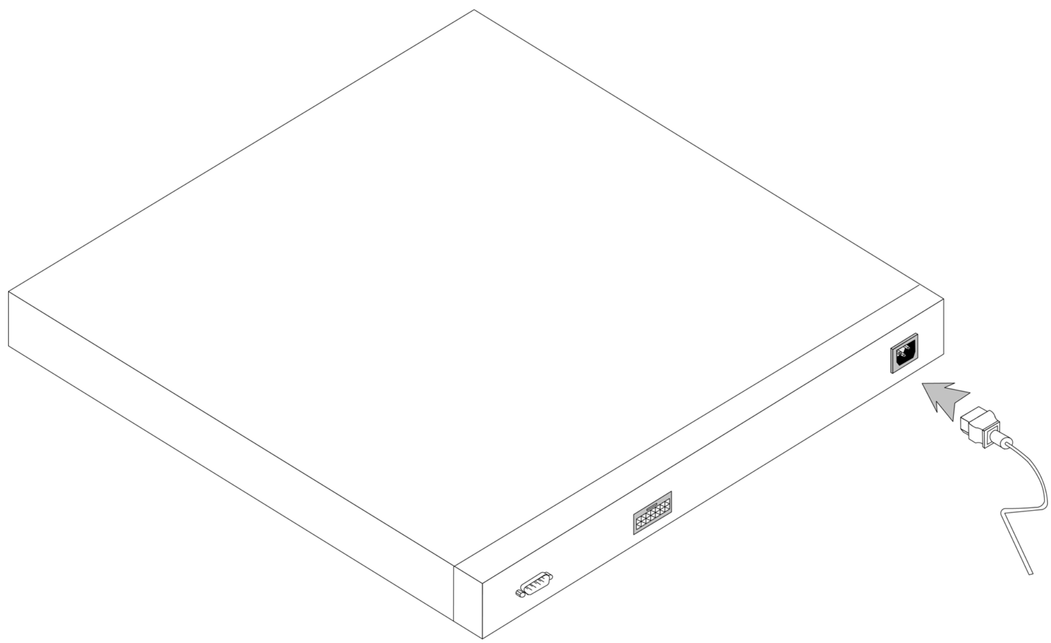
The AC power supply unit operates from 90 to 264 VAC, 47 to 63 Hz. The AC power supply unit uses a standard connector. LED indicator is on the front panel and indicates whether the AC unit is connected.

DC Power Supply Unit

The PowerConnect 3424 and PowerConnect 3448 switches connect to an external RPS-600 unit to provide a redundant power option. No configuration is required. The front panel "RPS" LED indicates whether the external RPS-600 is connected. See Table 2-5 for RPS LED definition.

The PowerConnect 3424/P and PowerConnect 3448/P switches connect to an external EPS-470 unit to provide a redundant power option. No configuration is required. The front panel "RPS" LED indicates whether the external EPS-470 is connected. See Table 2-5 for RPS LED definition.

Figure 2-11. Power Connection



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

Stack ID Button

The device front panel contains a Stack ID button used to manually select the Unit ID for the Stack Master and members.

The Stack Master and members must be selected within 15 seconds of booting the device. If the Stack Master is not selected within 15 seconds, the device is booted in stand-alone mode. To select a Unit ID for the device, reboot the device.

The Stack Master receives the Unit ID of 1 or 2. If both Unit 1 and Unit 2 are present, the unit that is not elected functions as the Backup Master. Stack members receive a separate Unit ID (3-6). For example, if there are four units in a stack, the Master unit is either 1 or 2, the backup Master is either 1 or 2 depending on the Unit ID of the Master unit, the third member is 3, and the fourth Stack member is 4.

NOTE: The device does not automatically detect a stand-alone unit. If a Unit ID has already been selected, press the Stack ID button several times until no stacking LED is lit.

Reset Button

The PowerConnect 3424/P and PowerConnect 3448/P switches have a reset button, located on the front panel, for manual reset of the device. If the Master device is reset, the entire stack is reset. If only a member unit is reset, the remain stacking members are not reset.

The single reset circuit of the switch is activated by power-up or low-voltage conditions.

Ventilation System

The PowerConnect 3424/P and PowerConnect 3448/P switches with the PoE feature have five built-in fans. The non-PoE PowerConnect 3424 and PowerConnect 3448 devices have two built-in fans. Operation can be verified by observing the LED that indicates if one or more fans is faulty.

3

Installing the PowerConnect 3424/P and PowerConnect 3448/P

Site Preparation

The PowerConnect 3424 /P and PowerConnect 3448/P devices can be mounted in a standard 48.26-am (19-inch) equipment rack, placed on a tabletop or mounted on a wall. Before installing the unit, verify that the chosen location for installation meets the following site requirements:

- **Power** — The unit is installed near an easily accessible 100-240 VAC, 50-60 Hz outlet.
- **General** — The Redundant Power Supply (RPS) is correctly installed by checking that the LEDs on the front panel are illuminated.
- **PoE Models** — The RPS is currently installed by checking that the PoE LEDs on the front panel are illuminated.
- **Clearance** — There is adequate frontal clearance for operator access. Allow clearance for cabling, power connections, and ventilation.
- **Cabling** — The 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 50ºC (32 to 122ºF) at a relative humidity of up to 95 percent, nonconducting.

Unpacking

Package Contents

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

- Device/Switch
- AC power cable
- RS-232 crossover cable
- Self-adhesive rubber pads
- Rack-mount kit for rack installation or wall mounting kit
- Documentation CD
- Product Information Guide

Unpacking the Device

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

1. Place the box on a clean flat surface.
2. Open the box or remove the box top.
3. Carefully remove the device from the box and place it on a secure and clean surface.
4. Remove all packing material.
5. Inspect the device and accessories for damage. Report any damage immediately.

Mounting the Device

The following mounting instructions apply to The PowerConnect 3424/P and PowerConnect 3448/P devices. The Console port is on the back panel. The power connectors are positioned on the back panel. Connecting a Redundant Power Supply (RPS) is optional, but is recommended. The RPS connector is on the back panel of the devices.

Installing in a Rack

CAUTION: Read the Safety Information included in the Product Information Guide for safety information on devices connected to or that support the SWI.

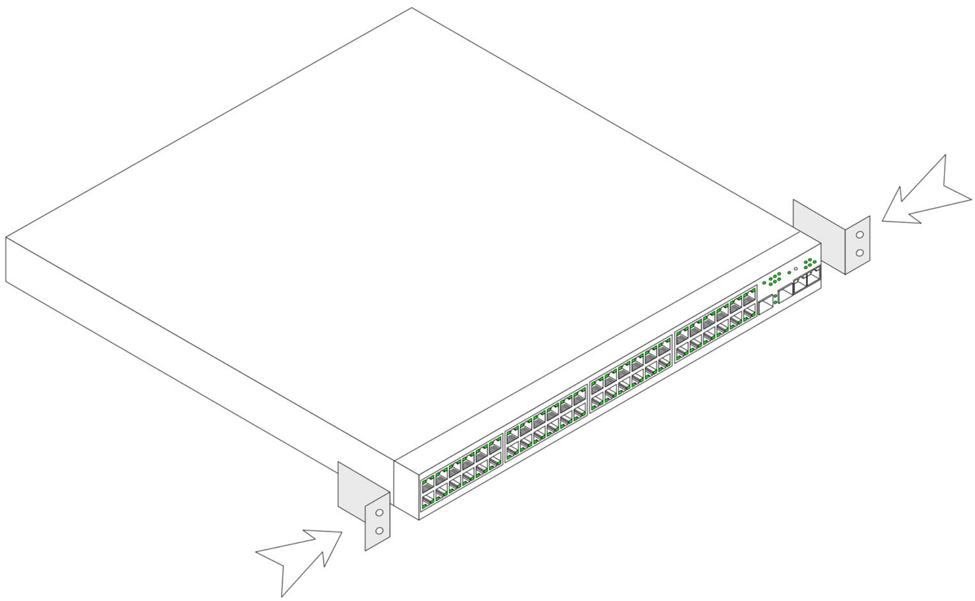
CAUTION: Disconnect all cables from the unit before mounting the device in a rack or cabinet.

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 that the mounting holes on the device line up to the mounting holes on the rack-mounting bracket.

The following figure illustrates where to mount the brackets.

Figure 3-1. Bracket Installation for Rack Mounting



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 48.26 cm (19 inch) rack, ensuring that the rack-mounting holes on the device line up to the mounting holes 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. Ensure that the ventilation holes are not obstructed.

Installing on a Flat Surface

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 Attach the self-adhesive rubber pads on each marked location on the bottom of the chassis.

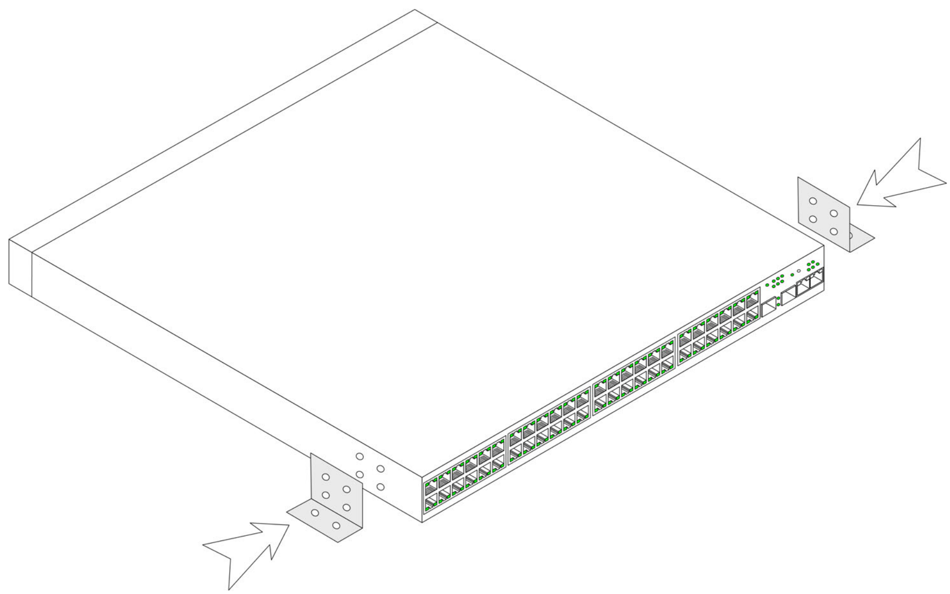
2 Set the device on a flat surface, leaving 5.08 cm (2 inch) on each side and 12.7 cm (5 inch) at the back.

3 Ensure that the device has proper ventilation.

Installing the Device on a Wall

1 Place the supplied wall-mounting bracket on one side of the device, ensuring that the mounting holes on the device line up to the mounting holes on the rack-mounting bracket. The following figure illustrates where to mount the brackets.

Figure 3-2. Bracket Installation for Mounting on a Wall



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

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

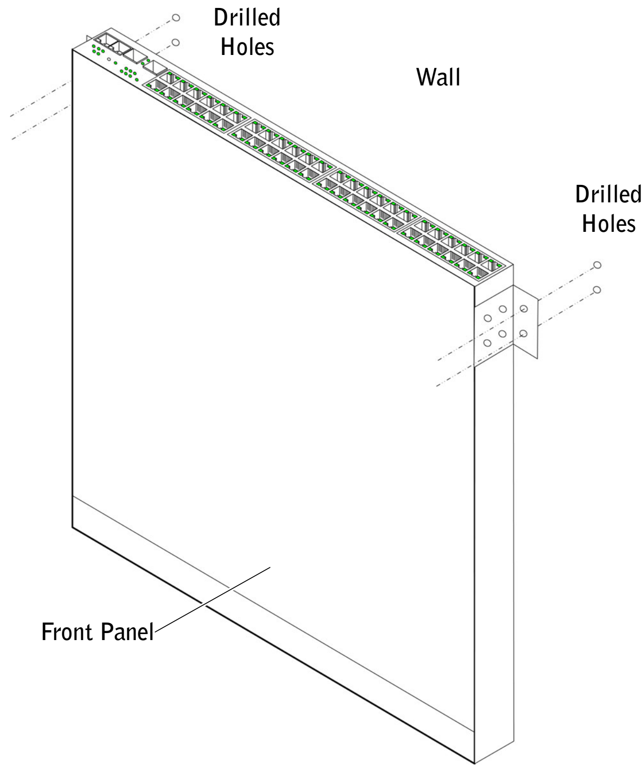
4 Place the device on the wall in the location where the device is being installed.

5 On the wall mark the locations where the screws to hold the device must be prepared.

6 Drill holes and place all plugs (not provided) in the holes, in the marked location.

7 Secure the unit to the wall with screws (not provided). Ensure that the ventilation holes are not obstructed.

Figure 3-3. Mounting a Device on a Wall



Connecting to a Terminal

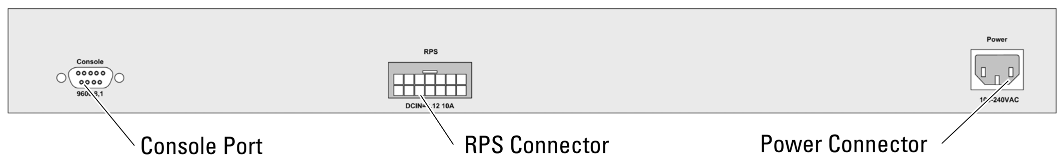
1. Connect an RS-232 crossover cable to the ASCII terminal or the serial connector of a desktop system running terminal emulation software.
2. Connect the female DB-9 connector at the other end of the cable to the device serial port connector.

Connecting a Device to a Power Supply

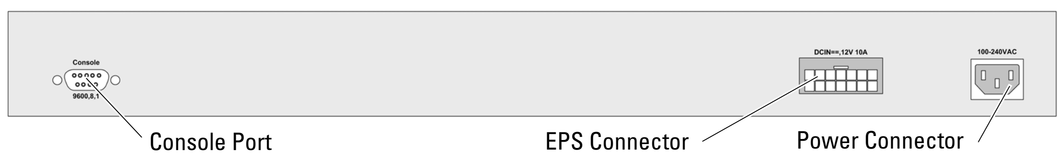
Connect the supplied AC power cable to the AC power connector on the back panel.

NOTE: Do not connect the power cable to a grounded AC outlet at this time. Connect the device to a power source in the steps detailed in "Starting and Configuring the Device".

Figure 3-4. Back-Panel Power Connector



PowerConnect 3424/3448 Rear View



PowerConnect 3424P/3448P Rear View

After connecting the device to a power source, confirm that the device is connected and operating correctly by examining the LEDs on the front panel.

Installing a Stack

Overview

Each device can operate as a stand-alone device or can be a member in a stack. Up to six devices or up to 192 ports are supported per stack.

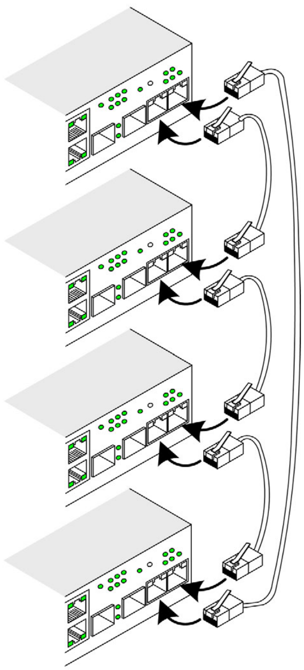
All stacks must have a Master unit, and may have a Master Backup unit, with any other devices connected to the stack as Members.

Stacking PowerConnect 3400 Series Switches

Each PowerConnect 3400 series stack contains a single Master unit, and may have a Master Backup unit, while the remaining units are considered stacking Members.

PowerConnect 3400 series switches use the RJ-45 Gigabit Ethernet ports (G3 and G4) for stacking. This enables added stacking capabilities to the devices without adding additional device accessories. To stack the devices together, insert a standard Category 5 cable into port G3 in the uppermost device in the stack, and into port G4 of the device immediately below it in the stack. Repeat this process until all devices are connected. Connect the bottommost device's port G3 in the stack to port G4 of the uppermost device in the stack.

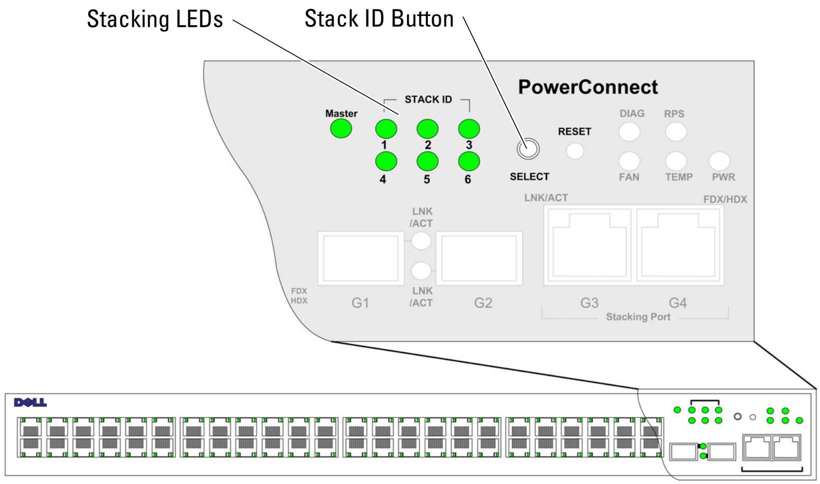
Figure 3-5. Stacking Cable Diagram



NOTE: In stacking mode ports designated as G3 and G4 are not displayed in the EWS. The effect is of not being present on the device. This is because the ports receive a different index for stacking.

Stack unit identification is performed on the device front panel using the Stack ID button.

Figure 3-6. Stacking Configuration and Identification Panel



Each stack device has a unique identifying unit ID that defines the unit's position and function in the stack. If the device is a stand-alone unit, the Stack LED is not illuminated. The default setting is stand-alone.

The unit ID is manually configured by using the Stack ID button. The unit ID is indicated by the Stack ID LEDs. Unit ID 1 and 2 are reserved for the Master and Backup Master unit, and unit ID 3 to 6 are for Member units.

Unit ID Selection Process

The unit ID selection process is as follows:

1. Ensure that the stand-alone/Master device Console port is connected to a VT100 terminal device or VT100 terminal emulator via the RS-232 crossover cable.
2. Locate an AC power receptacle.
3. Deactivate the AC power receptacle.
4. Connect the device to the AC receptacle.
5. Activate the AC power receptacle.

   When powering up, the configured LED number (corresponding to the previously saved unit ID) begins to flash. The LED flashes for 15 seconds. During this period, select a specific Stack ID by pressing the Stack ID button until the appropriate Stack ID LED is illuminated.

6 **Selection Process** — To advance the stacking ID LED number, continue pressing the Stack ID button. When LED 6 is flashing, pressing the Stack ID button results in the device being configured as a stand-alone. Pressing the Stack ID button again advances the Stack ID to 1. Unit 1 and Unit 2 are master-enabled units. See "Stacking Overview" master-election process.

7 **End selection process** — The unit ID selection process is completed when the 15-second flashing period has transpired. The Stack ID button becomes unresponsive and the unit ID is set to the LED ID flashing at the end of the period.

NOTE: These steps should be performed one unit at a time until all stack members are powered up and their Stack IDs are selected. Performing the steps one unit at a time will allow for sufficient time to select the Stack ID for each unit. However, the entire stack should be cabled as per the "Stacking Cable Diagram" before powering up the devices.

Starting and Configuring the Device

After completing all external connections, connect a terminal to the device to configure the device. Performing the additional advanced functions is described in the section "Advanced Configuration".

NOTE: Before proceeding, read the release notes for this product. Download the release notes from the Dell Support website at **support.dell.com**.

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

Connecting to the Device

To configure the device, the device must be connected to a console. However, if the device is part of a stack, only one device called the Master unit in the stack needs to be connected to a terminal. Because the stack operates as a single device, only the Master unit is configured.

Connecting the Terminal to the Device

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
- An 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:

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

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

3 Set the data rate to 9600 baud.

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

5 Set flow control to *none*.

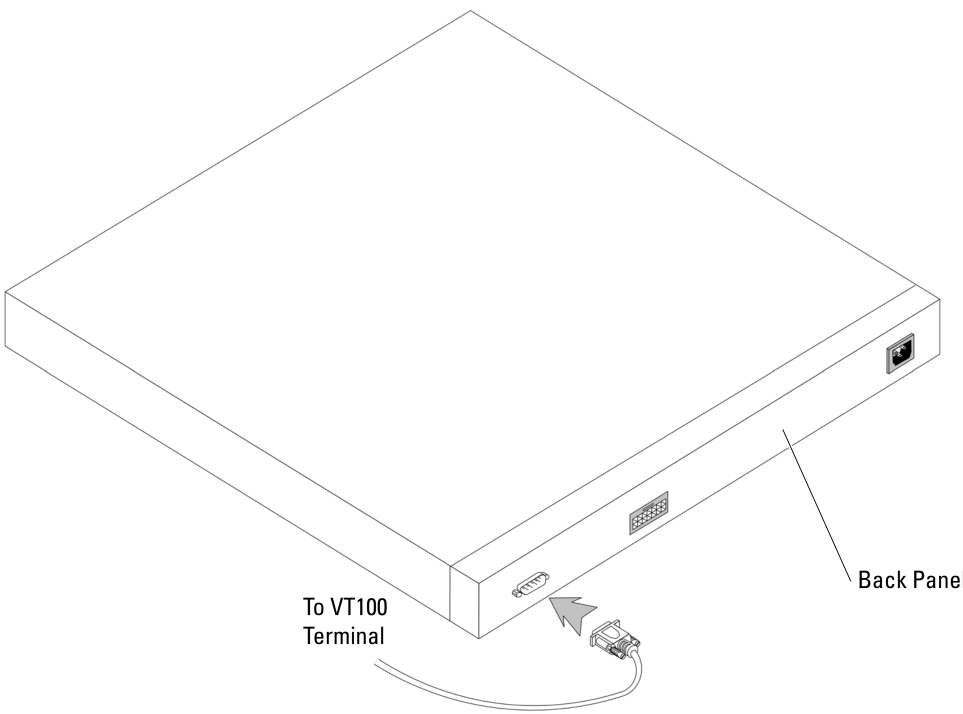
6 Under Properties, select VT100 for Emulation mode.

7 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 you have Windows 2000 Service Pack 2 or later 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.

8 Connect the female connector of the RS-232 crossover cable directly to the device Console port on the Master unit/stand-alone device, and tighten the captive retaining screws.
The PowerConnect 3400 Series Console port is on the rear panel.

Figure 3-7. Connecting to PowerConnect 3400 Series Console Port



NOTE: A console can be connected to the Console port on any unit in the stack, but stack management is performed only from the stack master (unit ID 1 or 2).

4

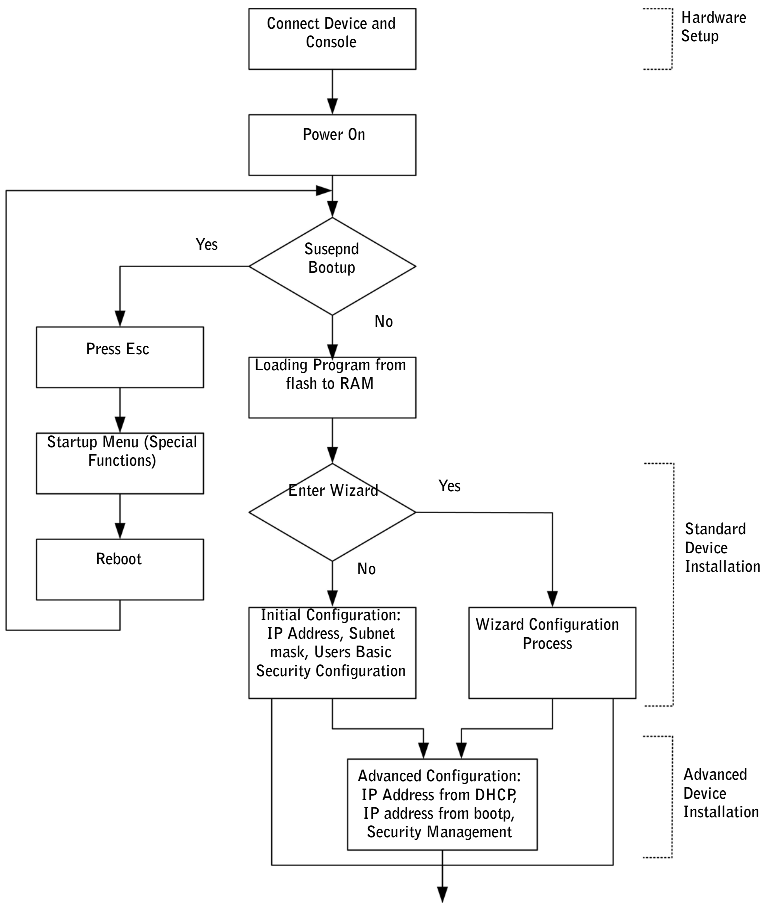
Configuring PowerConnect 3424/P and 3448/P

Configuration Procedures

After all the device external connections are completed, a terminal is connected to the device to monitor the boot and other procedures. The order of installation and configuration procedures is illustrated in the following figure:

NOTE: Before proceeding, read the release notes for this product. Download the release notes from **support.dell.com**.

Figure 4-1. Installation and Configuration Flow



Booting the Switch

When the power is turned on with the local terminal already connected, the switch 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 passes successfully, a valid executable image is loaded into RAM. POST messages are displayed on the terminal and indicate test success or failure.

The boot process runs approximately 30 seconds.

Initial Configuration

NOTE: Before proceeding, read the release notes for this product. Download the release notes from the Dell Support website at **support.dell.com**.

NOTE: The initial configuration assumes the following:

- The PowerConnect device was never configured before and is in the same state as when you received it.
- The PowerConnect device booted successfully.
- The console connection is established and the console prompt is displayed on the screen of a VT100 terminal device.

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

If this is the first time the device has booted up, or if the configuration file is empty because the device has not been configured, the user is prompted to use the Setup Wizard. The Setup Wizard provides guidance through the initial device configuration, and gets the device up and running as quickly as possible.

NOTE: Obtain the following information from the network administrator before configuring the device:

- The IP address to be assigned to the VLAN 1 interface through which the device is to be managed (by default, every port is a member of the VLAN 1)
- The IP subnet mask for the network
- The default gateway (next hop router) IP address for configuring the default route.
- SNMP community string and SNMP management system IP address (optional)
- Username and password

The Setup Wizard guides you through the initial switch configuration, and gets the system up and running as quickly as possible. You can skip the Setup Wizard, and manually configure the device through the device CLI mode.

The Setup Wizard configures the following fields.

- SNMP Community String and SNMP Management System IP address (optional)
- Username and Password
- Device IP address
- Default Gateway IP address

The following is displayed:

```
Welcome to Dell Easy Setup Wizard

The Setup Wizard guides you through the initial switch
configuration, and gets you up and running as quickly as
possible. You can skip the setup wizard, and enter CLI mode to
manually configure the switch.
```

```
The system will prompt you with a default answer; by pressing
enter, you accept the default.
You must respond to the next question to run the setup wizard
within 60 seconds, otherwise the system will continue with
normal operation using the default system configuration.

Would you like to enter the Setup Wizard (you must answer this
question within 60 seconds? (Y/N)[Y]Y
You can exit the Setup Wizard at any time by entering [ctrl+Z].
```

If you enter [N], the Setup Wizard exits. If there is no response within 60 seconds, the Setup Wizard automatically exits and the CLI console prompt appears.

If you enter [Y], the Setup Wizard provides interactive guidance through the initial device configuration.

NOTE: If there is no response within 60 seconds, and there is a BootP server on the network, an address is retrieved from the BootP server.

NOTE: You can exit the Setup Wizard at any time by entering [ctrl+z].

Wizard Step 1

The following is displayed:

```
The system is not setup for SNMP management by default.
To manage the switch using SNMP (required for Dell Network
Manager) you can

•  Setup the initial SNMP version 2 account now.

•  Return later and setup additional SNMP v1/v3 accounts.

For more information on setting up SNMP accounts, please see
the user documentation.

Would you like to setup the SNMP management interface now?
(Y/N)[Y]Y
```

Enter [N] to skip to Step 2.

Enter [Y] to continue the Setup Wizard. The following is displayed:

```
To setup the SNMP management account you must specify the
management system IP address and the "community string" or
password that the particular management system uses to access
the switch. The wizard automatically assigns the highest access
level [Privilege Level 15] to this account.
You can use Dell Network Manager or CLI to change this setting,
and to add additional management systems. For more information
on adding management systems, see the user documentation.
To add a management station:
```

```
Please enter the SNMP community string to be used:
[Dell_Network_Manager]
Please enter the IP address of the Management System (A.B.C.D)
or wildcard (0.0.0.0) to manage from any Management Station:
[0.0.0.0]
```

Enter the following:

- SNMP community string, for example, Dell_Network_Manager.
- IP address of the Management System (A.B.C.D), or wildcard (0.0.0.0) to manage from any Management Station.

NOTE: IP addresses and masks beginning with zero cannot be used.

Press **Enter**.

Wizard Step 2

The following is displayed:

```
Now we need to setup your initial privilege (Level 15) user
account.
This account is used to login to the CLI and Web interface.
You may setup other accounts and change privilege levels later.
For more information on setting up user accounts and changing
privilege levels, see the user documentation.
To setup a user account:
Enter the user name<1-20>:[admin]
Please enter the user password:*
Please reenter the user password:*
```

Enter the following:

- User name, for example "admin"
- Password and password confirmation.

NOTE: If the first and second password entries are not identical, the user is prompted until they are identical.

Press **Enter**.

Wizard Step 3

The following is displayed:

```
Next, an IP address is setup.
The IP address is defined on the default VLAN (VLAN #1), of
which all ports are members. This is the IP address you use to
access the CLI, Web interface, or SNMP interface for the
switch.To setup an IP address:
```

```
Please enter the IP address of the device (A.B.C.D):[1.1.1.1]
Please enter the IP subnet mask (A.B.C.D or nn):
[255.255.255.0]
```

Enter the IP address and IP subnet mask, for example 1.1.1.1 as the IP address and 255.255.255.0 as the IP subnet mask.

Press **Enter**.

Wizard Step 4

The following is displayed:

```
Finally, setup the default gateway.
Please enter the IP address of the gateway from which this
network is reachable (e.g. 192.168.1.1).Default gateway
(A.B.C.D):[0.0.0.0]
```

Enter the default gateway.

Press **Enter**. The following is displayed (as per the example parameters described):

```
This is the configuration information that has been collected:

==============================================================

SNMP Interface = Dell_Network_Manager@0.0.0.0
User Account setup = admin
Password = *
Management IP address = 1.1.1.1 255.255.255.0
Default Gateway = 1.1.1.2

==============================================================
```

Wizard Step 5

The following is displayed:

```
If the information is correct, please select (Y) to save the
configuration, and copy to the start-up configuration file.
If the information is incorrect, select (N) to discard
configuration and restart the wizard: (Y/N)[Y]Y
```

Enter [N] to skip to restart the Setup Wizard.

Enter [Y] to complete the Setup Wizard. The following is displayed:

```
Configuring SNMP management interface
Configuring user account......
Configuring IP and subnet......

Thank you for using Dell Easy Setup Wizard. You will now enter
CLI mode.
```

Wizard Step 6

The CLI prompt is displayed.

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 the IP address is not. 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 1/e1
console(config-if)# ip address dhcp hostname powerconnect
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)#
```

The interface receives the IP address automatically.

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

IP Address      I/F      Type


-------------   ------   -------

100.1.1.1/24    vlan 1   dynamic
```

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

NOTE: If you configure a DHCP IP address, this address is dynamically retrieved, and the `ip address dhcp` command is saved in the configuration file. In the event of master failure, the backup will again attempt to retrieve a DHCP address. This could result in one of the following:

- The same IP address may be assigned.
- A different IP address may be assigned, which could result in loss of connectivity to the management station.
- The DHCP server may be down, which would result in IP address retrieval failure, and possible loss of connectivity to the management station.

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 device 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.

NOTE: Passwords can be secured by using password management commands to force aging-out of passwords, or expiration of passwords. For more information, see "Security Management and Password Configuration".

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.

You can enter the Startup menu when booting the device. The user input is to 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  ****************
************************************************
Boot1 Checksum Test..............................PASS
Boot2 Checksum Test..............................PASS
Flash Image Validation Test......................PASS
BOOT Software Version 1.0.0.05 Built  06-Jan-2005  14:46:49
Carrier board, based on PPC8247
128 MByte SDRAM. I-Cache 16 KB. D-Cache 16 KB. Cache Enabled.
Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom.
```

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
```

The following sections describe the available Startup menu options.

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

NOTE: Technical support personnel only can operate the Diagnostics Mode (option `[4])`. For this reason, Enter Diagnostics Mode is not described in this guide.

Download Software - option [1]

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

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

*** Running  SW  Ver. 1.0.0.30  Date  09-Jan-2005  Time  14:30:02

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

HW version is

Base Mac address is  : 00:00:b0:45:54:00

Dram size is  : 128M bytes

Dram first block size is  : 36864K bytes

Dram first PTR is  : 0x1C00000

Flash size is: 16M

Loading running configuration.

Number of configuration items loaded: 5

Loading startup configuration.

Number of configuration items loaded: 5

Device configuration:

Slot 1 - PowerConnect 3424 HW Rev.  0.0

-------------------------------

-- Unit Number 1  Standalone --

-------------------------------

BOXP_high_appl_init: dpssIpcInitStandAlone

Tapi Version: v1.3.1.6P_01_03

Core Version: v1.3.1.6P_01_02

01-Jan-2000 01:01:19 %INIT-I-InitCompleted: Initialization task is
completed

01-Jan-2000 01:01:19 %Box-I-FAN-STAT-CHNG: FAN# 1 status changed -
operational.
```

```
01-Jan-2000 01:01:19 %Entity-I-SEND-ENT-CONF-CHANGE-TRAP: entity configuration change trap.

01-Jan-2000 01:01:19 %Box-I-FAN-STAT-CHNG: FAN# 2 status changed - operational.

01-Jan-2000 01:01:19 %Box-I-PS-STAT-CHNG: PS# 1 status changed - operational.
```

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.

Erase FLASH File - option [2]

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.

To erase 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 - option [3]

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 when entering the local terminal only:

1 From the Startup menu, type `[3]` and press **<Enter>**. The password is deleted.

Enter your choice or press 'ESC' to exit:

```
Current password will be ignored!
```

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

Enter Diagnostic Mode - option [4]

For Technical Support only.

Set Terminal Baud-Rate - option [5]

To set the terminal baud-rate, type `[5]` and press **<Enter>**.

Enter your choice or press 'ESC' to exit:

```
Set new device baud-rate: 38,400
```

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 downloading 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 from 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 `arc` file).

3 Enter the **show version** command 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   1.0.0.30 (date 27-Jan-2005 time 13:42:41)

Boot version 1.0.0.05 (date 27-Jan-2005 time 15:12:20)

HW version
```

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

```
console# show bootvar
Images currently available on the Flash
Image-1 active (selected for next boot)
Image-2 not active
console#
```

5 Enter the **copy tftp:**//{tftp address}/{file name} **image** command 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 command, enter the **show bootvar** command 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:

```
console# boot system image-2
console# show bootvar
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 the show version command 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   1.0.0.30 (date 27-Jan-2005 time 13:42:41)

Boot version 1.0.0.05 (date 27-Jan-2005 time 15:12:20)

HW version
```

4 Enter the **copy tftp:**//{tftp address}/{file name} **boot** command 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.

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 all 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 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 100BaseT 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, thus 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 with the half duplex mode. By default, this feature is disabled. It can be enabled per port. The back-pressure mechanism prevents the sender from transmitting additional traffic temporarily. The receiver may occupy a link so it becomes unavailable for additional traffic.

Switching Port Default Settings

The following table gives the port default settings.

Table 4-7. Port Default Settings

Function	Default Setting
Port speed and mode	10/100BaseT copper: auto-negotiation 100 Mbps full duplex
	10/100/1000BaseT copper / SFP: auto-negotiation1000 Mbps full duplex
Port forwarding state	Enabled
Port tagging	No tagging
Flow Control	Off (disabled on ingress)
Back Pressure	Off (disabled on ingress)

5

Using Dell OpenManage Switch Administrator

This section provides an introduction to the Dell OpenManage Switch Administrator user interface.

Starting the Application

NOTE: Before starting the application the IP address must be defined. For more information, see Initial Configuration.

1 Open a web browser.

2 Enter the device's IP address in the address bar and press <Enter>.

3 When the **Log In** window displays, enter a user name and password.

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

4 Click **OK**.

The **Dell OpenManage™ Switch Administrator** home page displays.

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 5-1. Switch Administrator Components

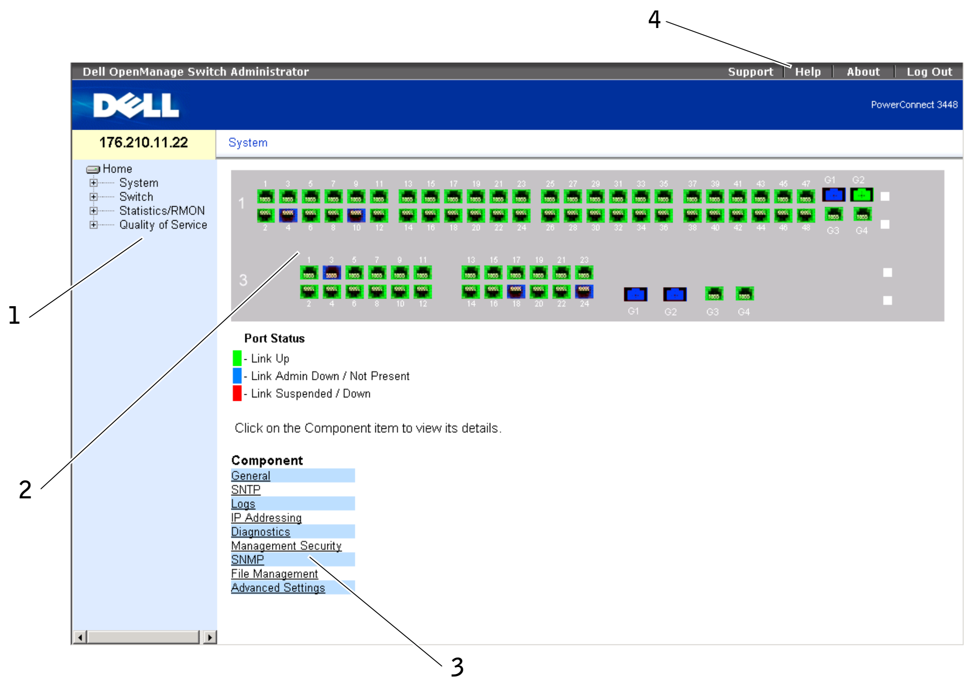


Table 5-8 lists the interface components with their corresponding numbers.

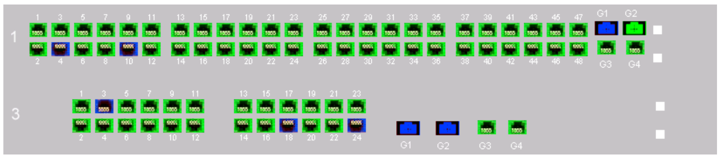
Table 5-8. Interface Components

Component	Description
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 home page contains a graphical representation of the device front panel.

Figure 5-2. PowerConnect Device Port Indicators



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

Table 5-9. PowerConnect Port and Stacking Indicators

Component	Description
Port Indicators	
Green	The port is currently enabled.
Red	An error has occurred on the port.
Blue	The port is currently disabled.
Red	The device is not currently linked in a stack.

NOTE: The Port LEDs are not reflected in PowerConnect front panel in the OpenManage Switch Administrator. LED status can only be determined by viewing the actual device. However, the Stacking LEDs reflect the Stacking port status. 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. Interface buttons are divided into the following categories:

Information Buttons

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

Table 5-10. Information Buttons

Button	Description
Support	Opens the Dell Support page at **support.dell.com**
Help	Online help that contains information to assist in configuring and managing the device. The online help pages are context-sensitive. For example, if the **IP Addressing** page is open, the help topic for that page displays when **Help** is clicked.
About	**C**ontains the version and build number and Dell copyright information.
Log Out	Opens the Log Out window.

Device Management Buttons

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

Table 5-11. Device Management Buttons

Button	Description
Apply Changes	Applies set 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 Arrows	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.
Draw	Creates statistics charts on-the-fly.

Field Definitions

Fields which are user-defined can contain between 1 -159 characters, unless otherwise noted on the OpenManage Switch Administrator web page. All letters or characters can be used, except the following:

- \
- /
- :
- *
- ?
- <
- >
- |

Accessing the Device Through the CLI

You can manage the device over a direct connection to the Terminal port or via a Telnet connection. If access is via a Telnet connection, ensure that 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 "Initial Configuration".

NOTE: Ensure that the software has been downloaded to the device before using the CLI to remotely access the device.

Terminal 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, enter the **exit** Privileged EXEC mode command.

The session quits.

NOTE: If a different user logs into the system in the Privileged 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. RS-232 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 to manage the device. 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.**

   The Telnet session begins.

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 terminal 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 terminal 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 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.

   To return from Privileged EXEC mode to User EXEC mode, type `disable` and press <Enter>.

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 the **configure** command 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> key combination.

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#
```

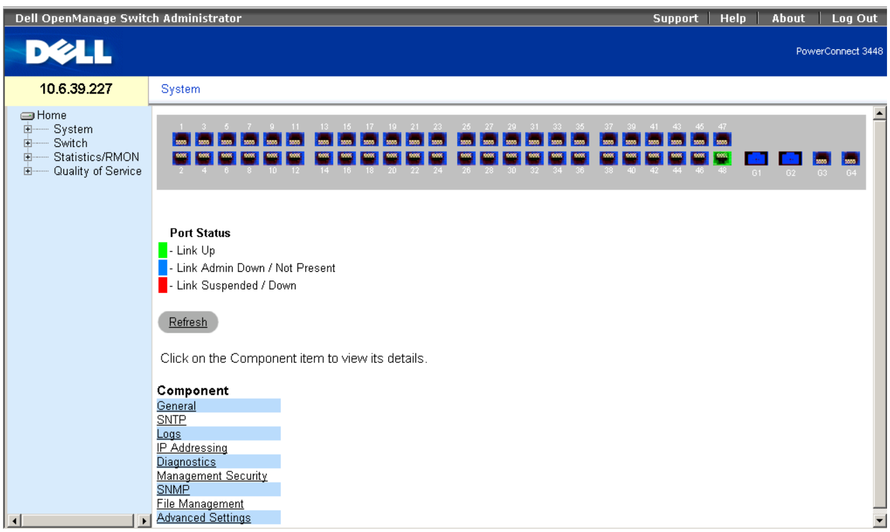
For a complete list of the CLI modes, see the **Dell™ PowerConnect™3424/P and PowerConnect 3448/P CLI Guide**.

6

Configuring System Information

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

Figure 6-1. System



Defining General Switch Information

The **General** page contains links to pages that allow network managers to configure switch parameters.

Viewing Switch Asset Information

The **Asset** page contains parameters for configuring and viewing 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 6-2. Asset

The **Asset** page contains the following fields:

System Name (0-159 Characters) — Defines the user-defined device name.

System Contact (0-159 Characters) — Indicates the name of the contact person.

System Location (0-159 Characters) — The location where the system is currently running.

MAC Address — Indicates the device MAC address.

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

Date (DD/MMM//YY) — The current date. The format is day, month, year, for example, 10/OCT/03 is October 10, 2003.

Time (HH:MM:SS) — Indicates the time. The format is hour, minute, second, for example, 20:12:21 is eight twelve and twenty-one seconds in the evening.

Unit No. — Indicates the unit number for which the device asset information is displayed.

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

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

Serial No. — The device serial number.

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 6-12. Asset CLI Commands

CLI Command	Description
hostname *name*	Indicates 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 *text*	Sets the device asset tag.
show stack <1-6>	Displays the system stack information.
show system [**unit** *unit*]	Displays system information.
show system id [**unit** *unit*]	Displays system identity information.

The following is an example of defining the device host name, system contact and device location as well as setting the time and date of the system clock using the CLI commands:

```
console(config)# hostname dell
dell (config)# snmp-server contact Dell_Tech_Supp
dell (config)# snmp-server location New_York
dell (config)# exit
Console(config)# snmp-server host 10.1.1.1 management 2
Console# clock set 13:32:00 7 Mar 2002
Console# show clock
15:29:03 Jun 17 2002
```

The following is an example of displaying system information for a stand-alone device using the CLI commands:

```
console# show system id
Service tag     :
Serial number   : 51
Asset tag       :

console# show system
System Description:            Ethernet Switch
System Up Time                 0,00:00:57
(days,hour:min:sec):
System Contact:
System Name:                   CARRIER-1
System Location:
System MAC Address:            00:00:00:08:12:51
System Object ID:              1.3.6.1.4.1.674.10895.3006
Type:                          PowerConnect 3424
```

```
Main Power Supply Status:      OK
Fan 1 Status:                  NOT OPERATIONAL
Fan 2 Status:                  NOT OPERATIONAL
Temperature (Celsius):         30
Temperature Sensor Status:     OK
```

The following is an example of displaying system information for a stacked devices using the CLI commands:

```
console# show system id

Unit     Serial number          Asset tag  Service tag
----     -------------          ---------  -----------
1        893658972              mkt-1      89788978
2        893658973              mkt-2      89788979
3        893658974              mkt-3      89788980
4        893658975              mkt-4      89788981
5        893658976              mkt-5      89788982
6        893658977              mkt-6      89788983

console# show system

Unit     Type
----     -----------------
1        PowerConnect 3424
2        PowerConnect 3424
3        PowerConnect 3428
4        PowerConnect 3424P
5        PowerConnect 3424P
6        PowerConnect 3424P
```

```
Unit     Main Power Supply      Redundant Power Supply
----     -----------------      ----------------------
1        OK
2        OK
3        OK
4        OK                     OK
5        OK                     OK
6        OK                     OK

Unit     Fan1        Fan2        Fan3        Fan4        Fan5
----     ----        ----        ----        ----        ----
1        OK          OK
2        OK          OK
3        OK          OK
4        OK          OK          OK          OK          OK
5        OK          OK          OK          OK          OK
6        OK          OK          OK          OK          OK

Unit     Temperature (Celsius)   Temperature Sensor Status
----     --------------------    -------------------------
1        30                     OK
2        30                     OK
3        30                     OK
4        30                     OK
5        30                     OK
6        30                     OK
```

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, and 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:

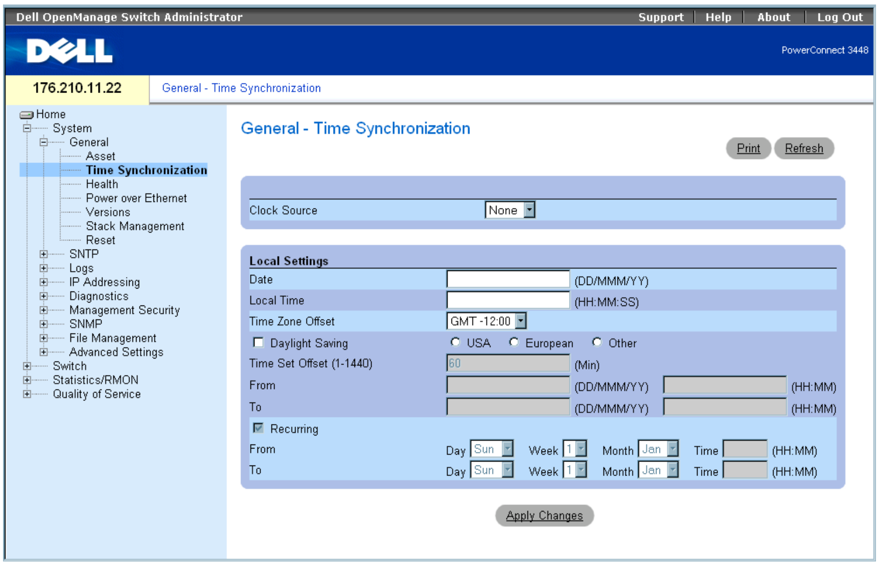
- **Albania** — Last weekend of March until the last weekend of October.
- **Australia** — From the end of October until the end of March.
- **Australia - Tasmania** — From beginning of October until the end of March.
- **Armenia** — Last weekend of March until the last weekend of October.
- **Austria** — 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 until 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 until 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** — Last weekend of March until the last weekend of 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 6-3. Time Synchronization



The **Time Synchronization** page contains the following fields:

Clock Source

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

> **SNTP** — Indicates that the system time is set via an SNTP server. For more information, see **Configuring SNTP Settings**.
>
> **None** — Indicates that the system time is not set by an external source.

Local Settings

Date — Defines the system date. The field format is DD/MMM/YY, for example, 04/May/50.

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 +1:00, while the local time in New York is GMT –5:00.

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 device's 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.

Time Set Offset (1-1440) — For non USA and European countries, the amount of time for DST can be set in minutes. The default time is 60 minutes.

From — Defines the time that DST begins in countries other than USA or Europe, in the format DD/MMM/YY in one field and time in another. For example, if DST begins on the 25th October 2007 5:00 am, the two fields are defined as 25/Oct/07 and 05:00. 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 DD/MMM/YY in one field and time in another. For example, DST ends on the 23rd March 2008 12:00 am, the two fields are defined as 23/Mar/08 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 fields.
3. Click **Apply Changes**.

   The local 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.

NOTE: The following steps must be completed before setting the summer clock:

1. Configure the summer time.
2. Define the time zone.
3. Set the clock.

For example:

```
console(config)# clock summer-time recurring usa
console(config)# clock time zone 2 zone TMZ2
console(config)# clock set 10:00:00 apr 15 2004
```

Table 6-13. Clock Setting CLI Commands

CLI	Description
clock source sntp	Configures an external time source for the system clock.
clock time zone *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.

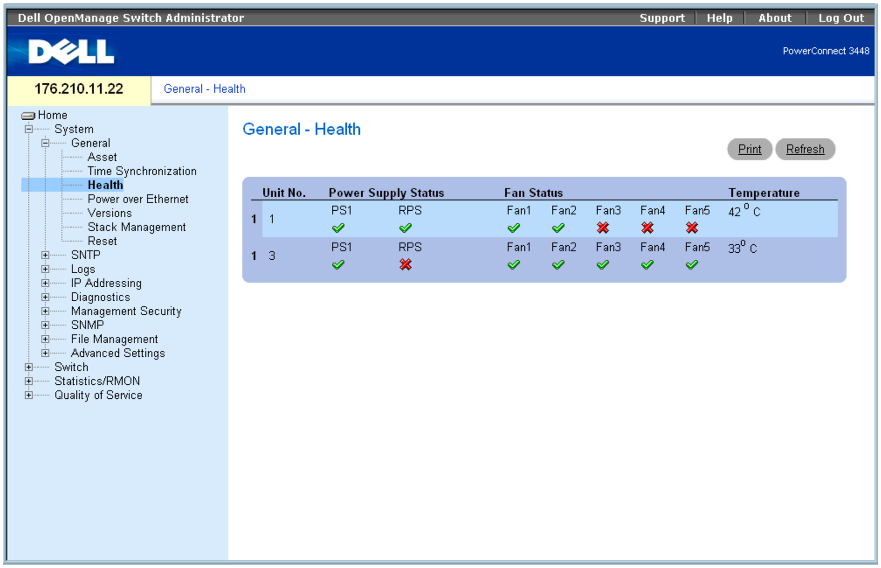
The following is an example of the CLI commands:

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

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

console(config)# clock source sntp

console(config)# interface ethernet e14

console(config-if)# sntp client enable

console(config-if)# exit

console(config)# sntp broadcast client enable
```

Viewing System Health Information

The **System Health** page displays physical device information, including information about the device's power and ventilation sources. To open the **System Health** page, click **System→General→Health** in the tree view.

Figure 6-4. System Health



The **System Health** page contains the following fields:

Unit No. — Indicates the unit number for which the device asset information is displayed.

Power Supply Status — The device has two power supplies. Power supply 1 is displayed as PS1 in the interface, while the redundant power supply is displayed as RPS. The possible field values are:

 — The power supply is operating normally.

 — The power supply is not operating normally.

Not Present — The power supply is currently not present.

Fan Status — The non-PoE devices have two fans, while the PoE devices have five fans. Each fan is denoted as fan plus the fan number in the interface. The possible field values are:

 — The fan is operating normally.

 — The fan is not operating normally.

Not Present — A fan is currently not present.

Temperature — The temperature at which the device is currently running. The device temperature is displayed in Celsius. The device temperature threshold is 0-40 C (32-104F). The following table displays the temperature in Fahrenheit in increments of 5.

Table 6-14. Celsius to Fahrenheit Conversion Table

Celsius	Fahrenheit
0	32
5	41
10	50
15	59
20	68
25	77
30	86
35	95
40	104

Viewing System Health Information Using the CLI Commands

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

Table 6-15. System Health CLI Command

CLI Command	Description
show system [**unit** *unit*]	Displays system information.

The following is an example of the system health CLI command.

```
Console> show system

System Description: Ethernet switch
System Up Time (days,hour:min:sec): 1,22:38:21
System Contact:
System Name: RS1
System location:
System MAC Address: 00.10.B5.F4.00.01
Sys Object ID: 1.3.6.1.4.1.674.10895.3004
Type: PowerConnect 3424
Temperature Sensors:
```

```
Unit      Sensor        Temperature (Celsius)    Status
----      ------        ---------------------    ------
1         1                       41             OK
1         2                       41             OK
2         1                       42             OK
2         2                       42             OK

Unit      Power Supply  Source      Status
----      ------------  ------      ------
1         Main          AC          OK
2         Secondary     AC          OK

Unit      Fan           Status
----      ---           ------
1         CPU           OK
2         CPU           OK
```

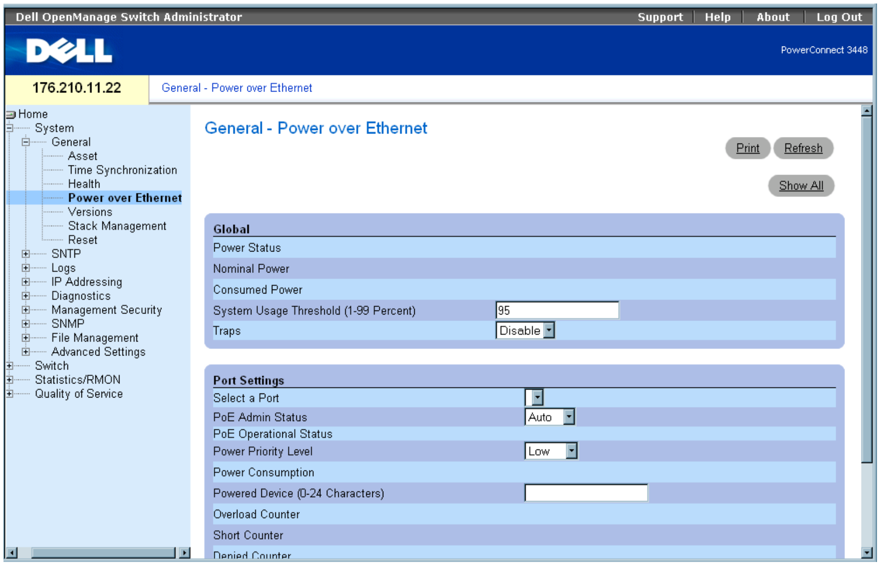
Managing Power over Ethernet

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

Powered Devices are devices which receive power from the PowerConnect power supplies, for example IP phones. Powered Devices are connected to the PowerConnect device via Ethernet ports. Powered devices are connected via either all PowerConnect 3424P's 24 FE ports or all PowerConnect 3448P's 48 FE ports.

To open the **Power Over Ethernet** page. click **System →General →Power over Ethernet** in the tree view.

Figure 6-5. Power Over Ethernet



The **Power Over Ethernet** page contains the following sections:

- Global
- Port Settings

Global

The Power over Ethernet Global Settings section contains the following fields:

Power Status — Indicates the inline power source status.

On — Indicates that the power supply unit is functioning.

Off — Indicates that the power supply unit is not functioning.

Faulty — Indicates that the power supply unit is functioning, but an error has occurred. For example, a power overload or a short circuit.

Nominal Power — Indicates the actual amount of power the device can supply. The field value is displayed in Watts.

Consumed Power — Indicates the amount of the power used by the device. The field value is displayed in Watts.

System Usage Threshold (1-99 Percent) — Indicates the percentage of power consumed before an alarm is generated. The field value is 1-99 percent. The default is 95 percent.

Traps — Enables or Disables receiving PoE device traps. The default is disabled.

Port Settings

Select a Port — Indicates the specific interface for which PoE parameters are defined and assigned to the powered interface connected to the selected port.

PoE Admin Status — Indicates the device PoE mode. The possible field values are:

> **Auto** — Enables the Device Discovery protocol, and provides power to the device using the PoE module. The Device Discovery Protocol enables the device to discover Powered Devices attached to the device interfaces, and to learn their classification. This is the default settings.
>
> **Never** — Disables the Device Discovery protocol, and stops the power supply to the device using the PoE module.

PoE Operational Status — Indicates if the port is enabled to work on PoE. The possible field values are:

> **On** — Indicates the device is delivering power to the interface.
>
> **Off** — Indicates the device is not delivering power to the interface.
>
> **Test Fail** —Indicates the powered device test has failed. For example, a port could not be enabled and cannot be used to deliver power to the powered device.
>
> **Testing** — Indicates the powered device is being tested. For example, a powered device is tested to confirm it is receiving power from the power supply.
>
> **Searching** — Indicates that the PowerConnect device is currently searching for a powered device. Searching is the default PoE operational status.
>
> **Fault** — Indicates that the PowerConnect device has detected a fault on the powered device. For example, the powered device memory could not be read.

Power Priority Level — Determines the port priority if the power supply is low. The port power priority is used if the power supply is low. The field default is low. For example, if the power supply is running at 99% usage, and port 1 is prioritized as high, but port 3 is prioritized as low, port 1 is prioritized to receive power, and port 3 may be denied power.

> **Critical** — Assigns the highest power priority level.
>
> **High** — Assigns the second highest power priority level.
>
> **Low** — Assigns the lowest power priority level.

Power Consumption — Indicates the amount of power assigned to the powered device connected to the selected interface. Devices are classified by the powered device, and the PowerConnect devices use the classification information. The field values are represented in Watts. The possible field values are:

> **0.44 – 12.95** — Indicates that the port is assigned a power consumption level of .44 to 12.95 Watts.
>
> **0.44 – 3.8** — Indicates that the port is assigned a power consumption level of .44 to 3.8 Watts.

3.84 – 6.49 — Indicates that the port is assigned a power consumption level of 3.84 to 6.49 Watts.

6.49 – 12.95 — Indicates that the port is assigned a power consumption level of 6.49 to 12.95 Watts.

Power Device (0-24 characters) — Provides a user-defined powered device description. The field can contain up to 24 characters.

Overload Counter — Indicates the total power overload occurrences.

Short Counter — Indicates the total power shortage occurrences.

Denied Counter — Indicates times the powered device was denied power.

Absent Counter — Indicates the times the power supply was stopped to the powered device because the powered device was no longer detected.

Invalid Signature Counter — Indicate the times an invalid signature was received. Signatures are the means by which the powered device identifies itself to the PSE. Signatures are generated during powered device detection, classification, or maintenance.

Defining PoE Settings

1. Open the **Power Over Ethernet** page.
2. Define the fields.
3. Click **Apply Changes**.

   PoE settings are defined, and the device is updated.

Managing PoE Using the CLI Commands

The following table summarizes the equivalent CLI commands for viewing fields displayed on the **Power Over Ethernet** page.

Table 6-16. System Health CLI Commands

CLI Command	Description
power inline {auto | never}	Configures the administrative mode of the inline power on an interface.
power inline powered-device *pd-type*	Adds a description of the powered device type.
power inline priority {**critical** | **high** | **low**}	Configures the priority of the interface from the point of view of inline power management.

Table 6-16. **System Health CLI Commands** *(continued)*

CLI Command	Description
power inline usage-threshold	Configures the threshold for triggering alarms
power inline traps enable	Enables PoE device traps
show power inline [*ethernet interface*]	Displays PoE configuration information

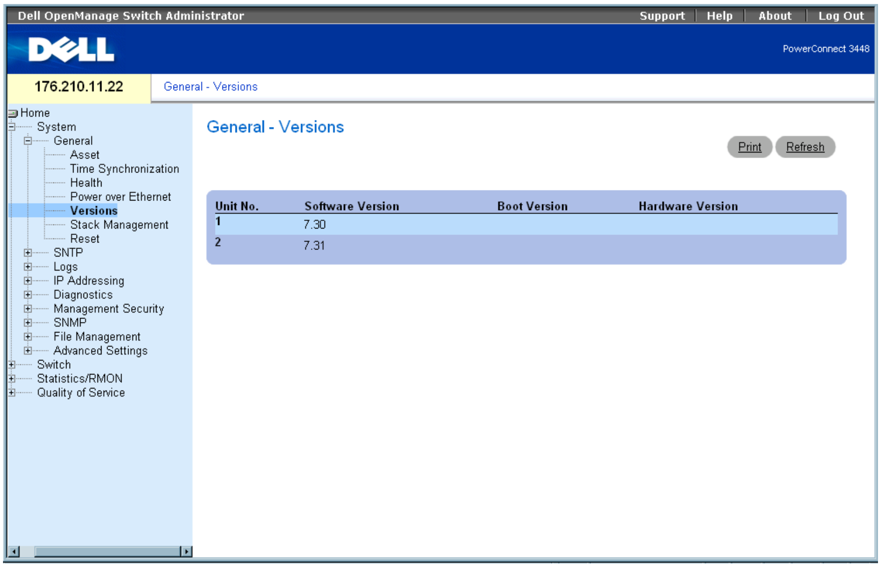
The following is an example of the PoE CLI commands.

```
Console# show power inline
Power: On
Nominal Power: 150 Watts
Consumed Power: 120 Watts (80%)
Usage Threshold: 95%
Traps: Enabled
Port  Powered Device   State  Priority  Status  Classification [W]
----  --------------   -----  --------  ------  ------------------
1/e1  IP Phone Model A Auto   High      On      0.44 - 12.95
2/e1  Wireless AP      Auto   Low       On      0.44 - 3.84
      Model
3/e1                   Auto   Low       Off     N/A

Console# show power inline ethernet 1/e1
Port  Powered Device   State  Priority  Status  Classification [W]
----  --------------   -----  --------  ------  ------------------
1/1e  IP Phone Model A Auto   High      On      0.44 - 12.95
Overload Counter: 1
Short Counter: 0
Denied Counter: 0
Absent Counter: 0
Invalid Signature Counter: 0
```

Viewing Version Information

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 6-6. Versions



The **Versions** page contains the following fields:

Unit No. — Indicates the unit number for which the device versions are displayed.

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

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

Hardware Version — The current device hardware version.

Displaying Device Versions Using the CLI

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

Table 6-17. Versions CLI Commands

CLI Command	Description
`show version`	Displays system version information.

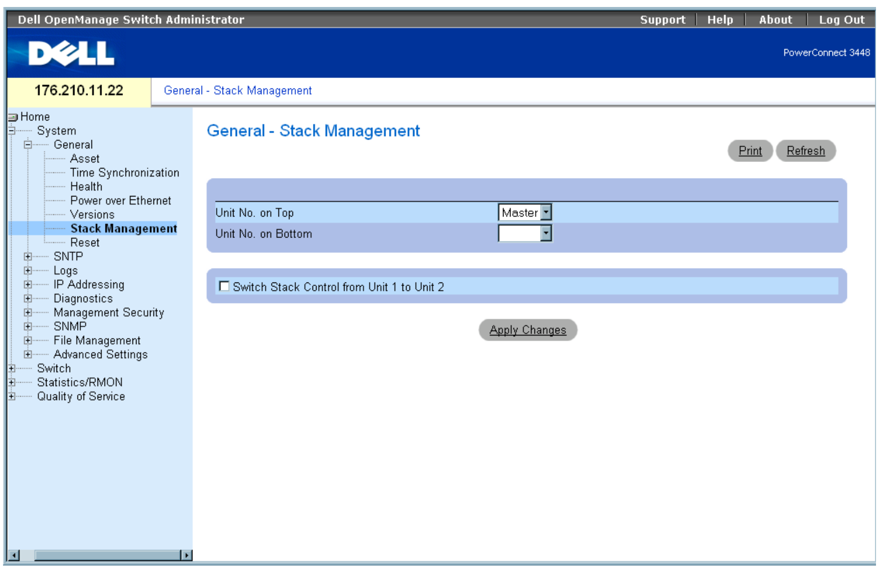
The following is an example of the CLI commands:

```
console> show version
SW version 1.0.0.0 (date 23-Jan-2005 time 17:34:19)
Boot version 1.0.0.0 (date 11-Jan-2005 time 11:48:21)
HW version 1.0.0
```

Managing Stack Members

The **Stack Management** page allows network managers to either reset the entire stack or a specific device. To open the **Stack Management** page, click **System →General →Stack Management** in the tree view.

Figure 6-7. Stack Management



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.

Unit No. on Top — First stack member number. Possible values are Master and 1-6.

Unit No. on Bottom — Second stack member number. Possible values are Master and 1-6.

Switch Stack Control from Unit 1 to Unit 2 — Enables switching from the current stack Master to the backup Master unit.

NOTE: Resetting the Master Unit resets the entire stack.

Switching Between Stack Masters

1. Open the **Stack Management** page.
2. Check the **Switch Stack Control from Unit 1 to Unit 2** check box.
3. Click **Apply Changes**.

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

   The device is reset. After the device is reset, a prompt for a user name and password displays.

Configuring Stack Display Order

1. Open the **Stack Management** page.
2. Define the stack topology by defining the top and bottom units. These units should be neighbors.
3. Click **Apply Changes**.

   The display order is reconfigured on the System page.

Managing Stacks Using the CLI Commands

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

Table 6-18. Stack Management CLI Commands

CLI Command	Description
reload	Reloads the operating system.
stack reload	Reloads stack members.
stack master	Forces the selection of stack master

The following is an example of the CLI commands:

```
console# reload
Are you sure you want to erase running configuration (y/n) [n]
```

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.

The **Reset** page contains the following field:

Reset Unit No. — Resets the selected stacking member.

NOTE: Save all changes to the Startup 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" on page 212.

Resetting the Device

1 Open the **Reset** page.

2 Select a unit in the **Reset Unit Number** field.

3 Click **Apply Changes.**

A confirmation message displays.

4 Click **OK**.

The device is reset. After the device is reset, a prompt for a user name and password is displayed.

5 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 6-19. 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 switch supports the Simple Network Time Protocol (SNTP). SNTP assures accurate network switch clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. SNTP operates only as a client, and cannot provide time services to other systems.

The switch 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 switch receives time from stratum 1 and above. The following is an example of stratums:

- **Stratum 0 —** Indicates a real time clock is used as the time source, for example, a GPS system.
- **Stratum 1** — Indicates that 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** — Indicates that 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.

The device can poll the following server types for the server time: Unicast, Anycast and Broadcast.

Polling for Unicast information is used for polling a server for which the IP address is known. SNTP servers that are configured on the device are the only ones that are polled for synchronization information. T1-T4 are used to determine server time. This is the preferred method for synchronizing device time as it is most secure. If this method is selected, SNTP information is accepted only from SNTP servers defined on the device using the **SNTP Servers** page.

Polling for Anycast information is used when the server IP address is unknown. If this method is selected, all SNTP servers on the network can send synchronization information . The device is synchronized when it proactively requests synchronization information. The best response (lowest stratum) from the first 3 SNTP servers to respond to a request for synchronization information is used to set the time value. Time levels T3 and T4 are used to determine the server time.

Using Anycast polling to get time information for synchronizing device time is preferred to using Broadcast polling to get time information. However, this method is less secure than unicast polling, because SNTP packets are accepted from SNTP servers that are not configured on the device.

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 to the message. If Broadcast polling is enabled, any synchronization information is accepted, even if it has not been requested by the device. This is the least secure method.

The device retrieves synchronization information, either by actively requesting information or at every poll interval. If Unicast, Anycast and Broadcast polling are enabled, the information is retrieved in this order:

- Information from servers defined on the device is preferred. If Unicast polling is not enabled or if no servers are defined on the device, the device accepts time information from any SNTP server that responds.
- If more than one Unicast device responds, synchronization information is preferred from the device with the lowest stratum.
- If the servers have the same stratum, synchronization information is accepted from the SNTP server that responded first.

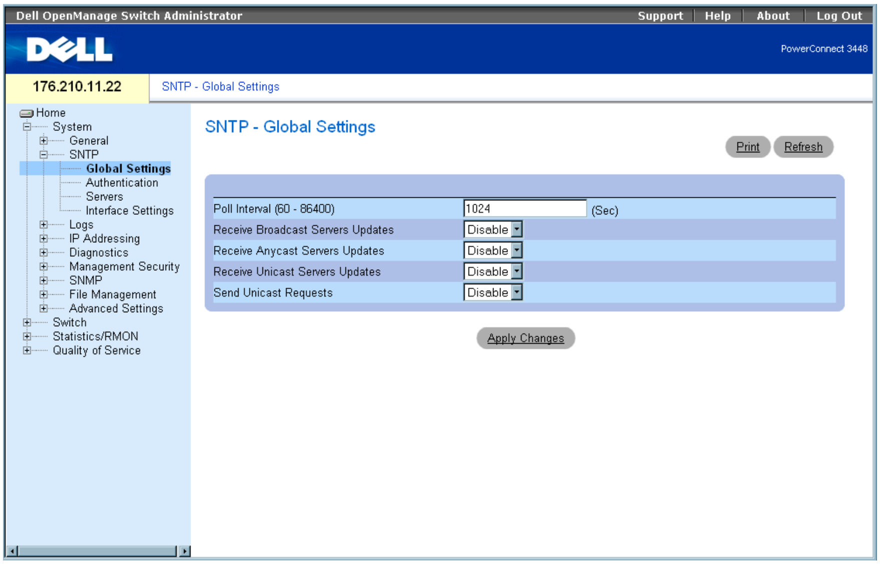
MD5 (Message Digest 5) Authentication safeguards device synchronization paths to SNTP servers. MD5 is an algorithm that produces a 128-bit hash. MD5 is a variation of MD4, and increases MD4 security. MD5 verifies the integrity of the communication, authenticates the origin of the communication.

To open the SNTP page, 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→Global Settings** in the tree view.

Figure 6-8. SNTP Global Settings



The **SNTP Global Settings** page contains the following fields:

Poll Interval (60-86400) — Defines the interval (in seconds) at which the SNTP server is polled for Unicast information. By default, the poll interval is 1024 seconds.

Receive Broadcast Servers Updates — Listens to the SNTP servers for Broadcast server time information on the selected interfaces, when enabled.

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.

Send Unicast Requests — Sends SNTP Unicast server time information requests to the SNTP server, when enabled.

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 fields.
3. Click **Apply Changes**.

   The local clock settings are applied.

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 6-20. 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

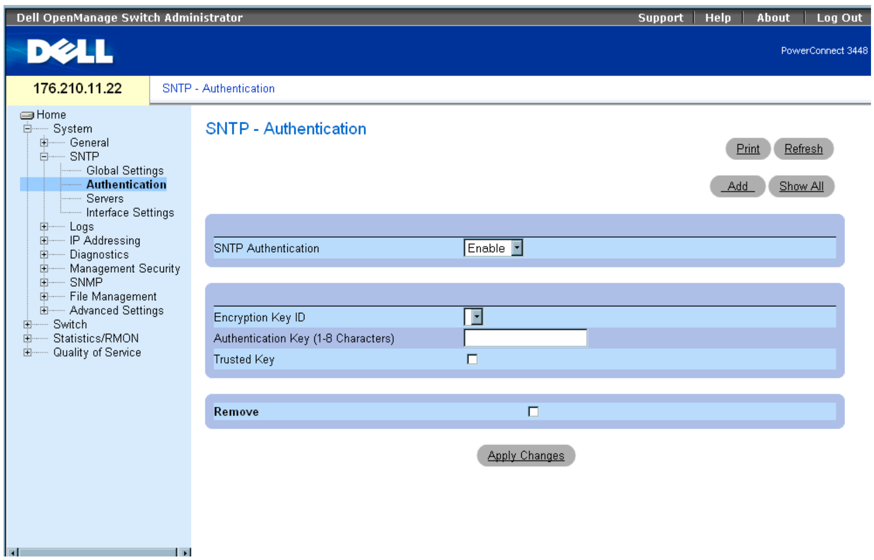
The following is an example of the CLI commands:

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

Defining SNTP Authentication Methods

The **SNTP Authentication** page enables SNTP authentication between the device 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 6-9. SNTP Authentication



The **SNTP Authentication** page contains the following:

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 up to 4294967295.

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

Trusted Key — Indicates the encryption key used (Unicast) to authenticate the SNTP server.

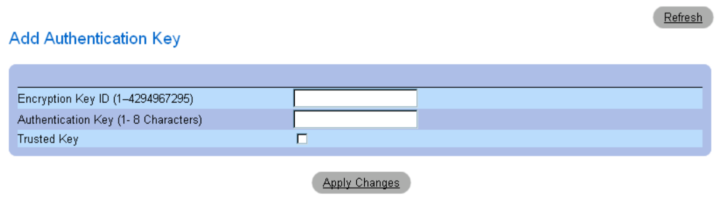
Remove — Removes selected authentication keys, when checked.

Adding an SNTP Authentication Key

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

   The **Add Authentication Key** page opens:

Figure 6-10. Add Authentication Key



3 Define the fields.

4 Click **Apply Changes**.

The SNMP authentication key is added, and the device is updated.

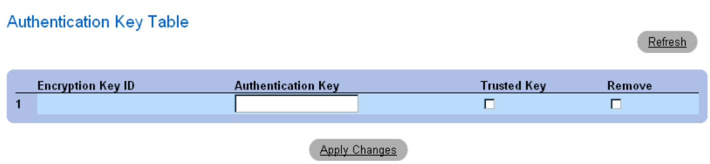
Displaying the Authentication Key Table

1 Open the **SNTP Authentication** page.

2 Click **Show All**.

The **Authentication Key Table** opens:

Figure 6-11. Authentication Key Table



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 6-21. SNTP Authentication CLI Commands

CLI Command	Description
sntp authenticate	Defines authentication for received Simple Network Time Protocol (SNTP) traffic from servers.
sntp trusted key	Authenticates the identity of a system to which SNTP will synchronize.
sntp authentication-key *number* **md5** *value*	Defines an authentication key for SNTP.

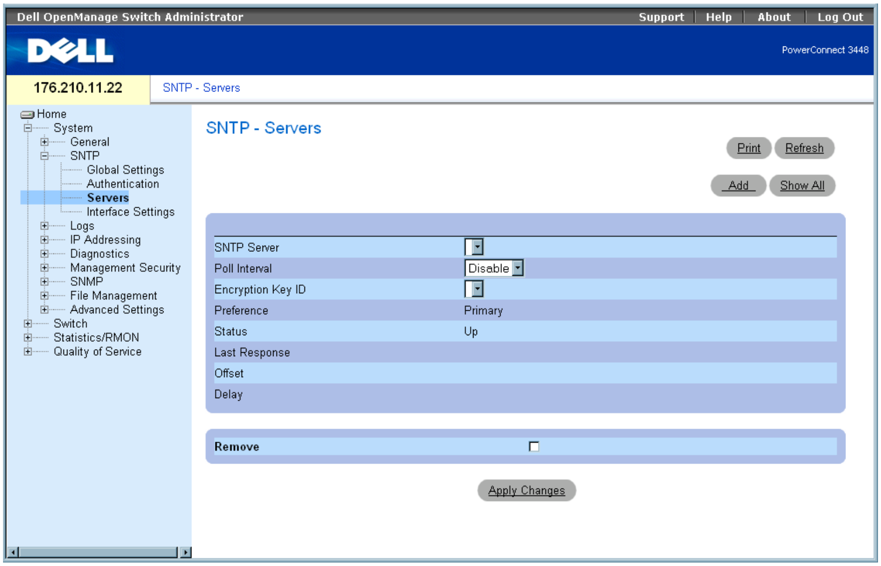
The following is an example of the CLI commands:

```
console(config)# sntp authentication-key 8 md5 Calked
console(config)# sntp trusted-key 8
Console(config)# sntp authenticate
```

Defining SNTP Servers

You can enable SNTP servers, as well as add new SNTP servers, from the **SNTP Servers** page. To open the **SNTP Servers** page, click **System →SNTP →Servers** in the tree view.

Figure 6-12. SNTP Servers



The **SNTP Servers** page contains the following fields:

SNTP Server — Select a user-defined SNTP server IP address. Up to eight SNTP servers can be defined.

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

Encryption Key ID — Indicates 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 — The operating SNTP server status. The possible field values are:

Up — The SNTP server is currently operating normally.

Down — Indicates that a SNTP server is currently not available. For example, the SNTP server is currently not connected or is currently down.

In progress — The SNTP server is currently sending or receiving SNTP information.

Unknown — The progress of the SNTP information currently being sent is unknown. For example, the device is currently looking for an interface.

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

Offset — Timestamp difference between the device local clock and the acquired 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 Servers** list, when selected.

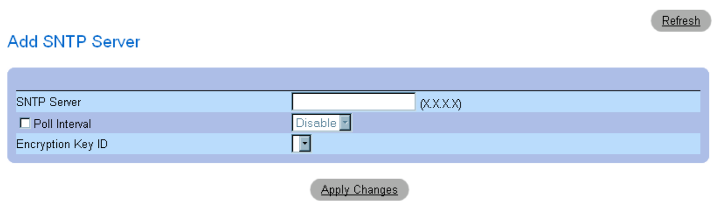
Adding an SNTP Server

1 Open the **SNTP Servers** page.

2 Click **Add**.

The **Add SNTP Server** page opens:

Figure 6-13. Add SNTP Server



3 Define the fields.

4 Click **Apply Changes**.

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

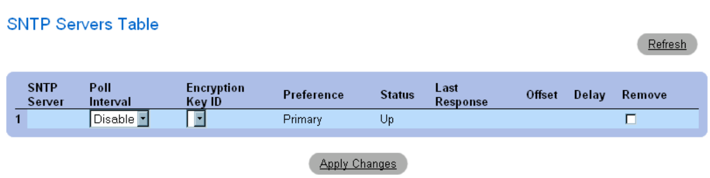
Displaying the SNTP Server Table

1 Open the **SNTP Servers** page.

2 Click **Show All**.

The **SNTP Servers Table** opens:

Figure 6-14. SNTP Servers Table



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 Server** page.

Table 6-22. 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 SNTP traffic from a server.

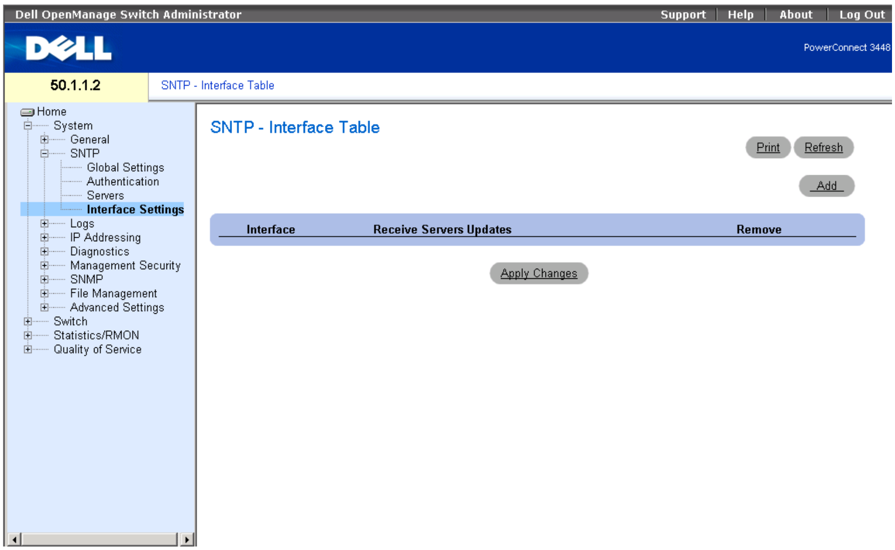
The following is an example of the CLI commands:

```
Console(config)# sntp server 100.1.1.1 poll key 10
```

Defining SNTP Interfaces

The **SNTP Interface Settings** page contains SNTP interface information. To open the **SNTP Interface Settings** page, click **System→SNTP→Interface Settings**.

Figure 6-15. SNTP Interface Settings



The **SNTP Interface Settings** page contains the following fields:

Unit No. — Indicates the stacking member on which the SNTP interface is enabled.

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

Receive Servers Updates — Enables or disables SNTP on the specific interface.

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

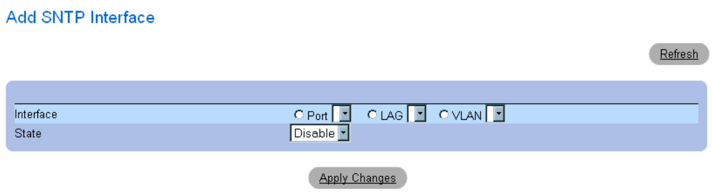
Adding an SNTP Interface

1 Open the **SNTP Interface Settings** page.

2 Click **Add**.

The **Add SNTP Interface** page opens.

Figure 6-16. Add SNTP Interface



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 Interface Settings** page.

NOTE: An IP address must be defined on the interface in order to define it as an Anycast or Broadcast interface.

Table 6-23. SNTP Interface Settings 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 for displaying SNTP interfaces:

```
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:1/e1, 1/e3
```

Managing Logs

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

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 System Logs protocol 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. The distribution of logging messages to the various destinations, such as the logging buffer, logging file or Syslog server, is controlled by the Syslog configuration parameters. Users can define up-to eight Syslog servers.

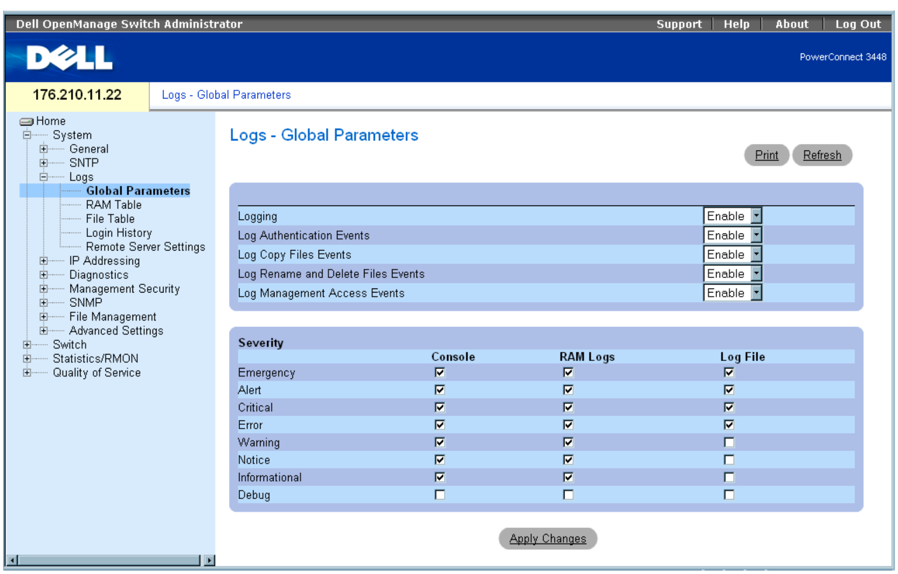
The following table contains the Log Severity Levels:

Table 6-24. 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 fields 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 6-17. Global Log Parameters



The **Global Log Parameters** page contains the following parameters:

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

Log Authentication Events — Enables generating logs when users are authenticated.

Log Copy Files Events — Enables generating logs when files are copied.

Log Rename and Delete Files Events — Enables generating logs when backup configuration files are renamed or deleted.

Log Management Access Events — Enables generating logs when the device is accessed using a management method. For example, each time the device is accessed using SSH, a device log is generated.

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, an attempt was made to download a non-existing configuration file.
>
> **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, a copy operation has failed.
>
> **Warning** — The lowest level of a device warning. For example, the device is functioning, but a port link is currently down.
>
> **Notice** — Provides important device information.
>
> **Informational** — Provides device information. For example, a port is currently up.
>
> **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 6-25. 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" on page 123**.
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.

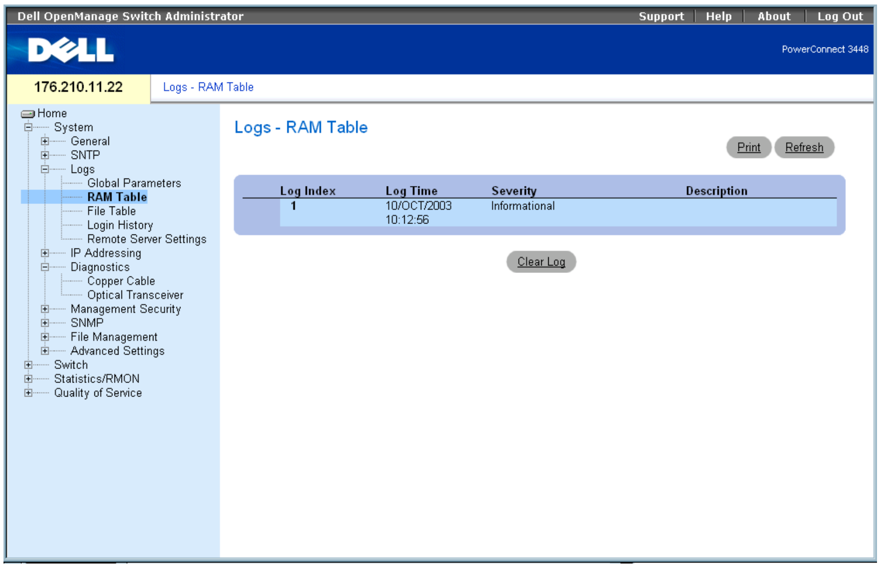
The following is an example of the CLI commands:

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

Viewing the 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 Table** in the tree view.

Figure 6-18. RAM Log Table



The **RAM Log Table** contains the following fields:

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

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

Severity — Indicates the log severity.

Description — Description of the log entry.

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 6-26. 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.

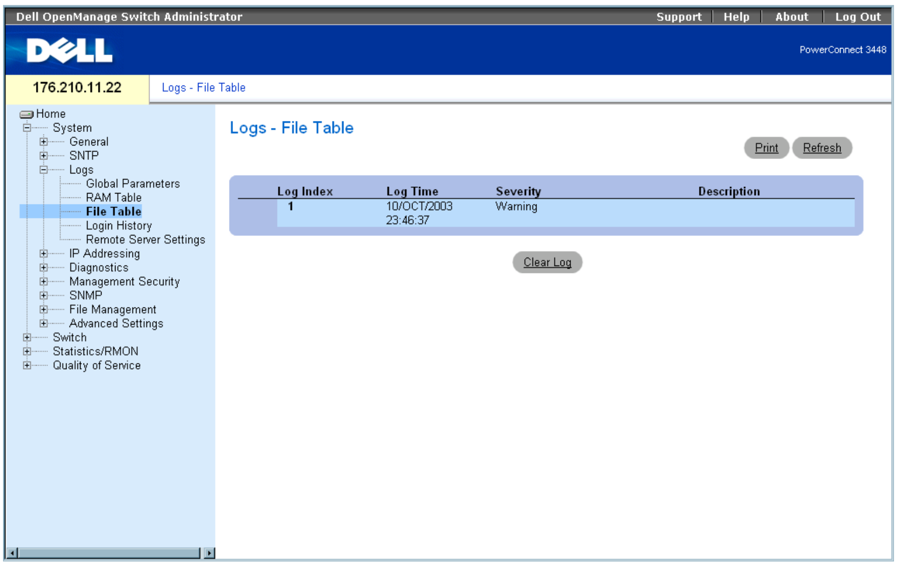
The following is an example of the CLI commands:

```
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: 1/e14

01-Jan-2000 01:01:36 :%LINK-W-Down: 1/e13

01-Jan-2000 01:01:36 :%LINK-W-Down: 1/e12

01-Jan-2000 01:01:36 :%LINK-W-Down: 1/e15

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


console# clear logging

Clear Logging Buffer [y/n]?
```

Viewing 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→File Table** in the tree view.

Figure 6-19. Log File Table



The **Log File Table** contains the following fields:

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

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

Severity — Indicates 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 6-27. 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:

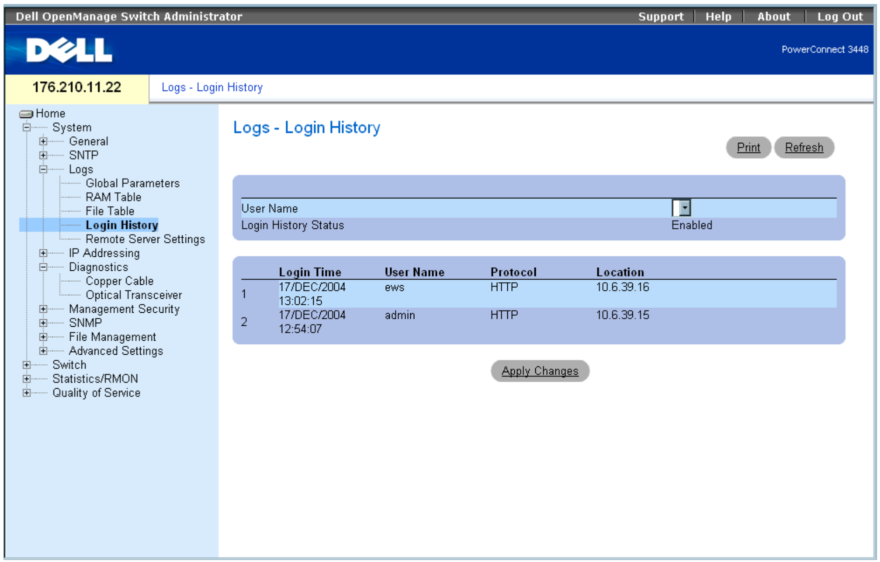
```
console# show logging file

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.

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

01-Jan-2000 01:11:49 :%LINK-I-Up: 1/e11

01-Jan-2000 01:11:46 :%LINK-I-Up: 1/e12

01-Jan-2000 01:11:42 :%LINK-W-Down: 1/e13

01-Jan-2000 01:11:35 :%LINK-I-Up: 1/e14
```

Viewing the Device Login History

The **Login History** page contains information for viewing and monitoring device utilization, including the time the user logged in and the protocol used to log on to the device.

To open the **Login History** page, click **System→Logs→Login History** in the tree view.

Figure 6-20. Login History



The **Login History** page contains the following fields:

User Name — Contains a user-defined device user name list.

Login History Status — Indicates if password history logs are enabled on the device.

Login Time — Indicates the time the selected user logged on to the device.

User Name — Indicates the user that logged on to the device.

Protocol — Indicates the means by which the user logged on to the device.

Location — Indicates the IP address of the station from which the device was accessed.

Viewing Login History

1. Open the **Login History** page.
2. Select a user in the **User Name** field.
3. Click **Apply Changes**.

   The login information for the selected user is displayed.

Displaying the Device Login History using CLI Commands

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

Table 6-28. Log File Table CLI Commands

CLI Command	Description
show users login-history	Displays password management history information.

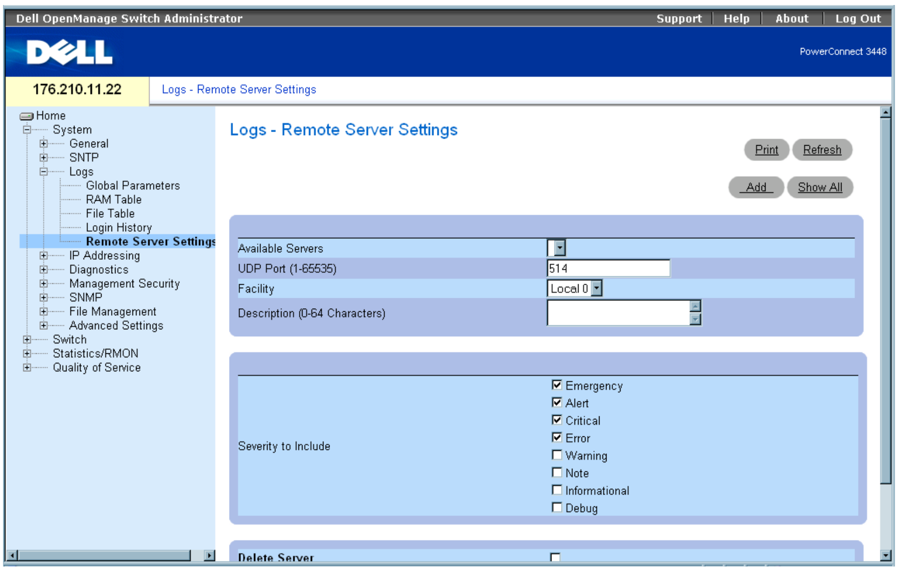
The following is an example of the CLI commands:

```
console# show users login-history


Login Time      Username        Protocol        Location
-----------     --------        --------        ----------
Jan 1. 2005     Anna            HTTP            172.16.1.8
23:58:17
Jan 1. 2005     Errol           HTTP            172.16.0.8
07:59:23
Jan 1. 2005     Amy             Serial
08:23:48
Jan 1. 2005     Alan            SSH             172.16.0.8
08:29:29
Jan 1. 2005     Bob             HTTP            172.16.0.1
08:42:31
Jan 1. 2005     Cindy           Telnet          172.16.1.7
08:49:52
```

Modifying Remote Log Server Definitions

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 server. To open the **Remote Log Server Settings** page, click **System→Logs→Remote Server Settings** in the tree view.

Figure 6-21. Remote Log Server Settings



The **Remote Log Server Settings** page contains the following fields:

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 field default is Local 7. 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.

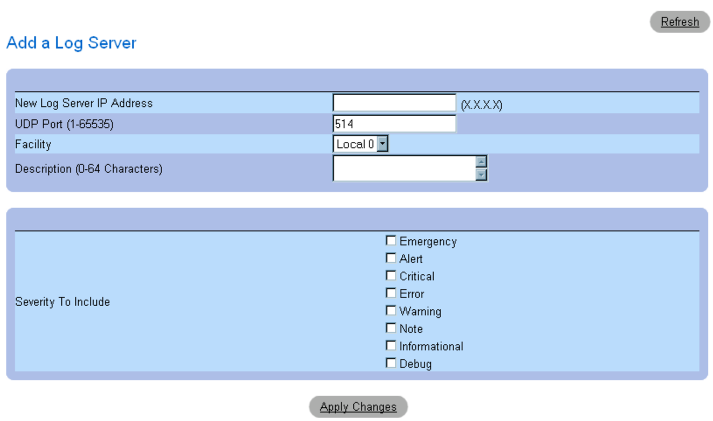
Defining a New Server:

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

2 Click **Add.**

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

Figure 6-22. Add a Log Server



The **Add a Log Server** page contains the additional field:

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.

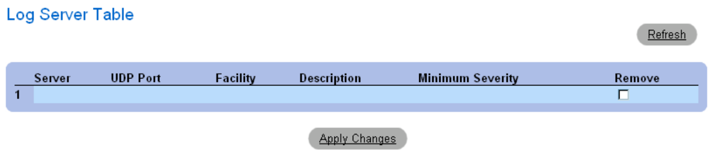
Displaying the Remote Log Servers Table:

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

2 Click **Show All**.

The **Log Servers Table** page opens:

Figure 6-23. Log Servers Table



Removing a Log Server from the Log Servers Table Page:

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

   The **Log Servers Table** page opens.
3. Select a **Log Servers Table** entry.
4. Select the **Remove** check box to remove the server(s).
5. Click **Apply Changes**.

   The **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 equivalent CLI command for working with remote log servers.

Table 6-29. 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(config)# end

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: 1/e11

03-Mar-2004 12:02:01 :%LINK-W-Down: 1/e12

03-Mar-2004 12:02:01 :%LINK-I-Up: 1/e13
```

Defining IP Addressing

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 to devices. Packets are forwarded to the default IP when packets 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:

User Defined — The device's Gateway IP address.

Active — Indicates if the Gateway is active.

Remove User Defined — Removes the device's Gateway from the **Default Gateway** drop-down list, when selected.

Selecting a Device's Gateway:

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 device's Default Gateway is selected and the device is updated.

Removing a Device's 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 a Device's Gateway Using the CLI Commands

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

.

Table 6-30. Default Gateway CLI Commands

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

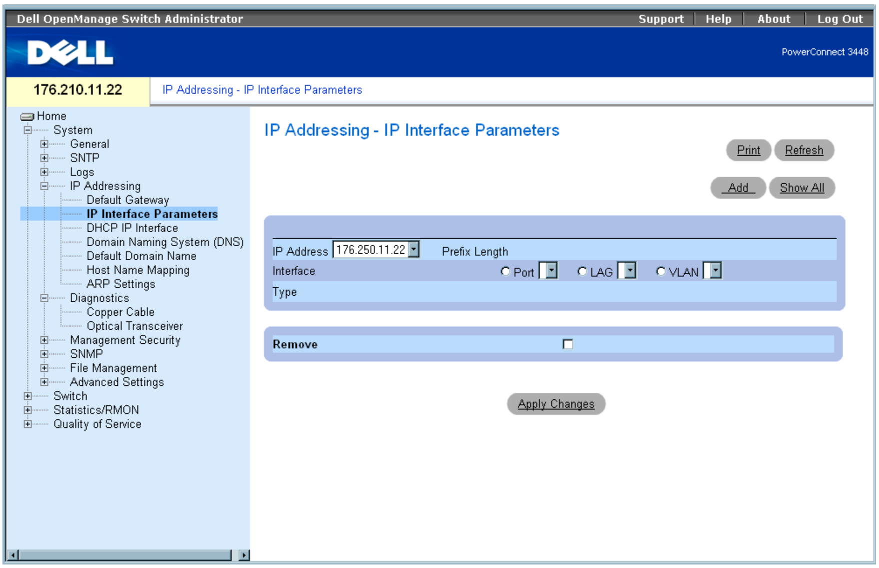
The following is an example of the CLI commands:

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

Defining IP Interfaces

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

Figure 6-24. IP Interfaces Parameters



The **IP Interfaces Parameters** page contains the following parameters:

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.

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

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

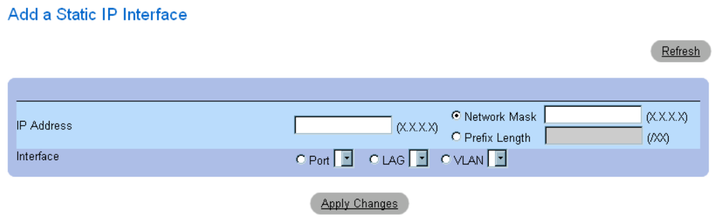
Remove — When selected, removes the interface from the **IP Address** drop-down menu.

Adding an IP Interface

1. Open the **IP Interfaces Parameters** page.
2. Click **Add**.

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

Figure 6-25. Add a Static IP Interface



Network Mask — Indicates the subnetwork mask of the source IP address.

3 Complete the fields on the page.

4 Click **Apply Changes**.

The new IP address is added to the interface, and the device is updated.

Modifying IP Address Parameters

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

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

3 Modify the interface type.

4 Click **Apply Changes**.

The parameters are modified, and the device is updated.

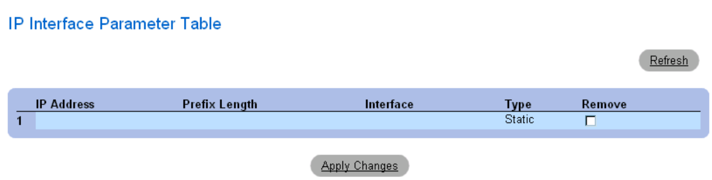
Deleting IP Addresses

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

2 Click **Show All.**

The **IP Interface Parameters Table** page opens:

Figure 6-26. IP Interface Parameter Table



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 Interfaces Parameters** page.

Table 6-31. 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.

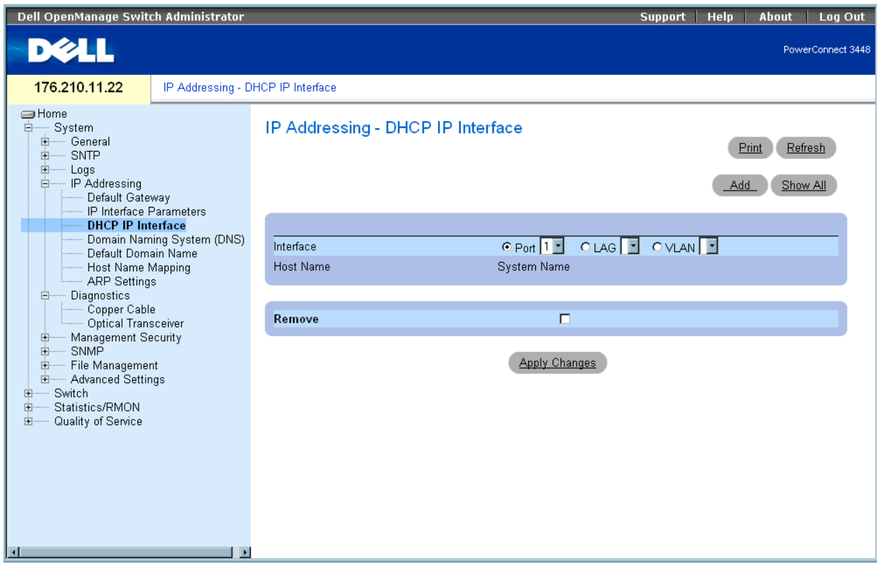
The following is an example of the CLI commands:

```
console(config)# interface vlan 1
console(config-if)# ip address 92.168.1.123 255.255.255.0
console(config-if)# no ip address 92.168.1.123
console(config-if)# end
console# show ip interface vlan 1
Gateway IP Address       Activity status
---------------------------------------
192.168.1.1                    Active
IP address         Interface         Type
-------------------------------------------------
192.168.1.123/24       VLAN 1       Static
```

Defining DHCP IP Interface Parameters

The **DHCP IP Interface** page contains parameters for defining DHCP clients connected to the device. To open the **DHCP IP Interface** page, click **System→IP Addressing→DHCP IP Interface** in the tree view.

Figure 6-27. DHCP IP Interface



The **DHCP IP Interface** page contains the following fields:

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 host name.

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 6-32. 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(config)# interface ethernet 1/e11
console(config-if)# ip address dhcp
```

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 into 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 Naming System (DNS)** in the tree view.

Figure 6-28. Domain Naming System (DNS)

The **Domain Naming System (DNS)** page contains the following fields:

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

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

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

Set DNS Server Active — Activates the selected DNS server.

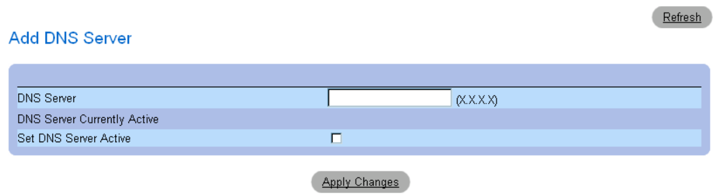
Remove DNS Server — When selected, removes the selected DNS server.

Adding a DNS Server

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

   The **Add DNS Server** page opens:

Figure 6-29. Add DNS Server



DNS Server — DNS Server IP address.

3 Define the relevant fields.

4 Click **Apply Changes**.

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

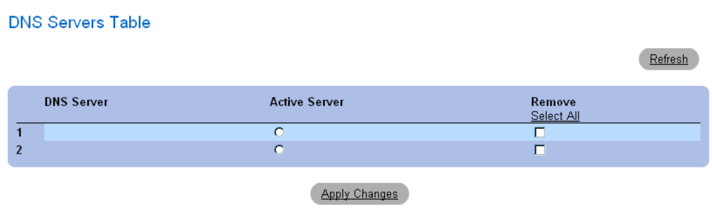
Displaying the DNS Servers Table

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

2 Click **Show All.**

The **DNS Server Table** opens:

Figure 6-30. DNS Server Table



Removing DNS Servers

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

2 Click **Show All.**

The **DNS Server Table** page opens.

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

4 Select the **Remove** checkbox.

5 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 6-33. 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.
ip domain-lookup	Enables DNS system for translating host names to IP addresses.

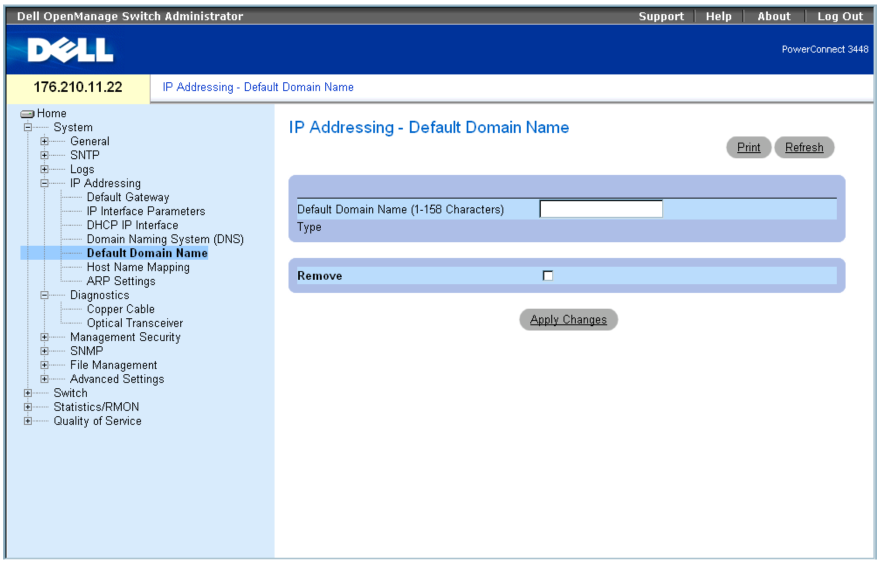
The following is an example of the CLI commands:

```
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**.

Figure 6-31. Default Domain Name



The **Default Domain Name** page contains the following fields:

Default Domain Name (1-158 characters) — Contains a user-defined default domain name. When defined, the default domain name is applied to all unqualified host names.

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

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

Remove — When checked, removes the default domain name.

Defining DNS Domain Names Using the CLI Commands

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

Table 6-34. 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.

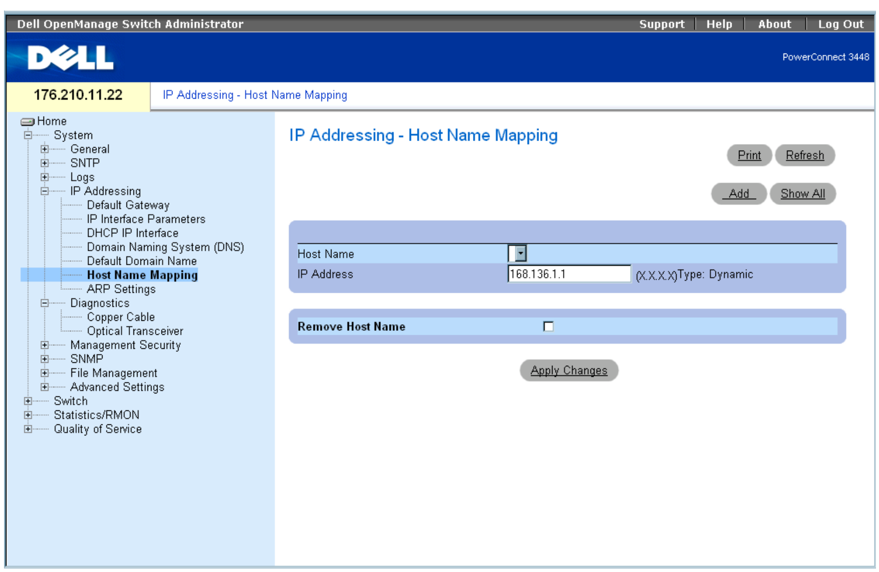
The following is an example of the CLI commands:

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

Mapping Domain Host

The **Host Name Mapping** page provides parameters for assigning IP addresses to static host names. On this page, one IP address per host can be assigned. To open the **Host Name Mapping** page, click **System→IP Addressing→Host Name Mapping** in the tree view.

Figure 6-32. Host Name Mapping



The **Host Name Mapping** page contains the following fields:

Host Name — Contains a Host Name list. Host Names are defined in the **Add Host Name Mapping** page. Each host provides one IP address.

IP Address (X.X.X.X) — Provides an IP address that is assigned to the specified host name.

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

Dynamic — The IP address is created dynamically.

Static — The IP address is a static IP address.

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

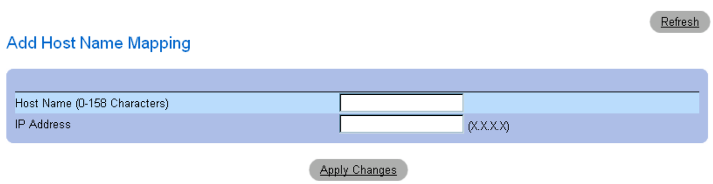
Adding Host Domain Names

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

2 Click **Add**.

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

Figure 6-33. Add Host Name Mapping



3 Define the relevant fields.

4 Click **Apply Changes**.

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

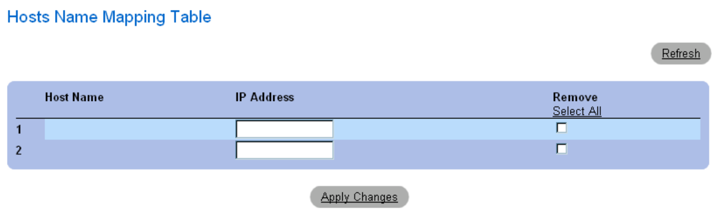
Displaying the Hosts Name Mapping Table

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

2 Click **Show All**.

The **Hosts Name Mapping Table** page opens:

Figure 6-34. Hosts Name Mapping Table



Removing Host Name from IP Address Mapping

1. Open the **Host Name Mapping** page.
2. Click **Show All.**
3. The **Host Mapping Table** page opens.
4. Select a **Host Name Mapping Table** entry.
5. Check the **Remove** checkbox.
6. Click **Apply Changes**.

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

Mapping IP addresses 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 6-35. Domain Host Name CLI Commands

CLI Command	Description
ip host *name address*	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.

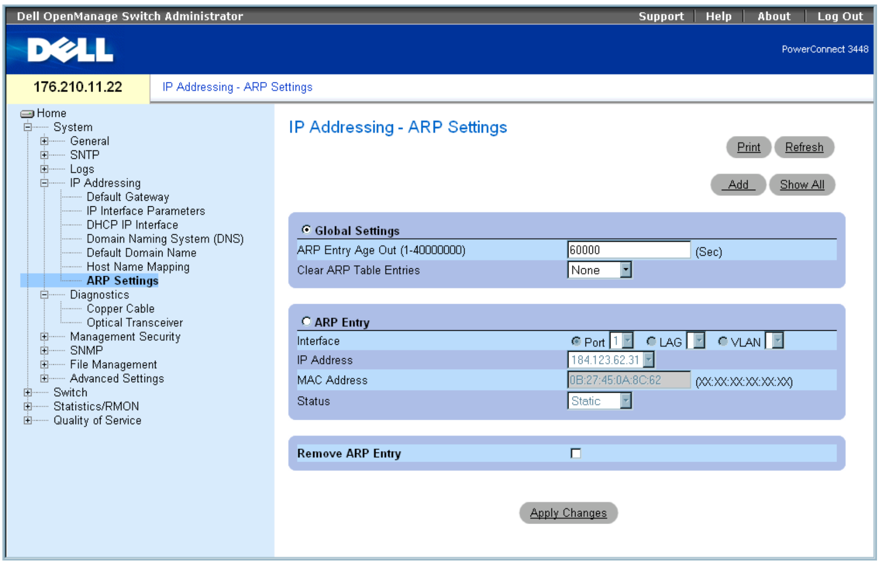
The following is an example of the CLI commands:

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

Defining ARP Settings

The Address Resolution Protocol (ARP) converts IP addresses into physical addresses, and maps the IP address to a MAC address. ARP allows a host to communicate with other hosts only when the IP address of its neighbors is known. To open the **ARP Settings** page, click **System→IP Addressing→ARP** in the tree view.

Figure 6-35. ARP Settings



The **ARP Settings** page contains the following fields:

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 passes between ARP requests about an ARP table entry. After this period, the entry is deleted from the table. The range is **1 - 40000000**. 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 Ethernet devices.

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.
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** page opens.

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 6-36. 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)# arp timeout 12000

console(config)# exit

console# show arp

ARP timeout: 12000 Seconds

Interface   IP address      HW address          Status

---------   ----------      ----------          ------

1/e11       10.7.1.102      00:10:B5:04:DB:4B   Dynamic

1/e12       10.7.1.135      00:50:22:00:2A:A4   Static
```

Running Cable Diagnostics

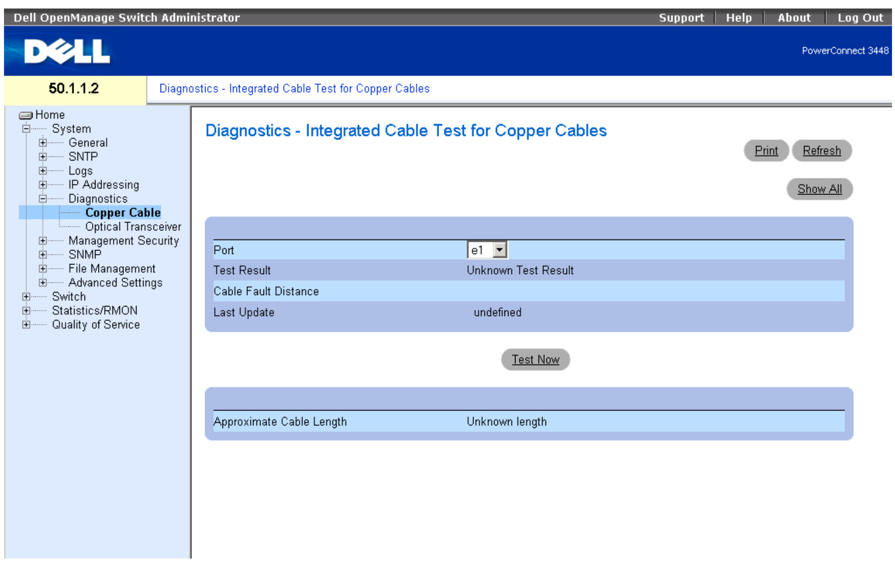
The **Diagnostics** page contains links to pages for performing virtual cable tests on copper cables. To open the **Diagnostics** page, click **System→Diagnostics** in the tree view.

Viewing Copper Cable Diagnostics

The **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 **Copper Cables** page, click **System→Diagnostics→Copper Cable** in the tree view.

Figure 6-36. Copper Cables



The **Copper Cables** page contains the following fields:

Port — The port to which the cable is connected.

Test Result — The cable test results. The possible field 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.

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 **Copper Cables** page.

3 Select an interface to test.

4 Click **Test Now**.

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

Displaying Virtual Cable Test Results Table

1 Open the **Copper Cables** page.

2 Click **Show All**.

   The **Integrated Cable Test Results Table** page opens.

NOTE: This screen displays the results of tests that have been previously run, but does not actually perform the test on all ports now.

In addition to the fields in the **Copper Cables** page, the **Integrated Cable Test Results Table** contains the following field:

Unit No. — The unit number for which the cable is displayed.

Performing Copper Cable Tests Using CLI Commands

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

Table 6-37. 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 1/e3
Cable is open at 100 meters.

Console# show copper-port cable-length
Port            Length (meters)
----            ---------------
1/e3            110-140
1/e4            Fiber
```

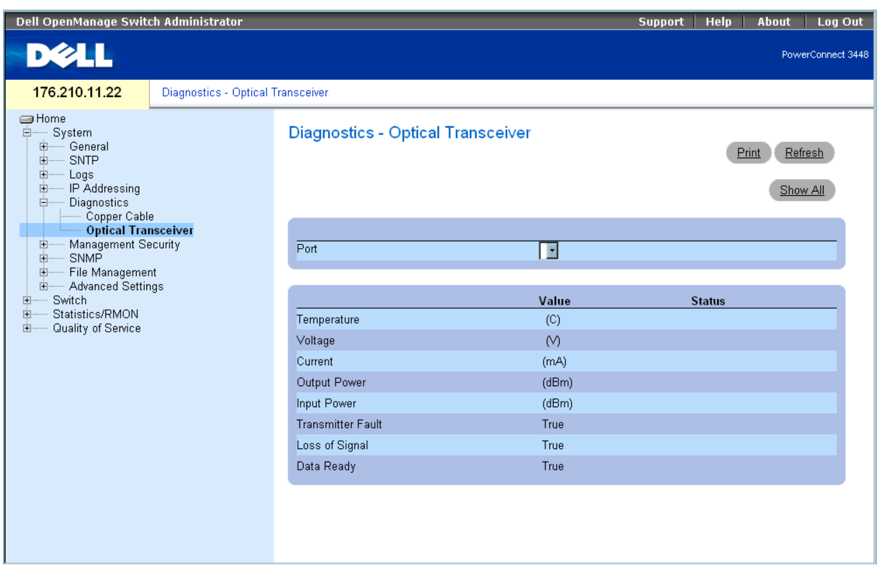
NOTE: The cable length returned by the Integrated Cable Tester (ICT) is an approximation in the ranges of up to 50 meters, 50m-80m, 80m-110m, 110m-120m, or more than 120m. The deviation may be up to 20 meters, and cable length measurement does not operate for 10 Mbps links.

Viewing Optical Transceiver Diagnostics

Use the **Optical Transceiver** page to perform tests on Fiber Optic cables. To open the **Optical Transceiver** page, click **System→Diagnostics→Optical Transceiver** in the tree view.

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

Figure 6-37. Optical Transceiver



The **Optical Transceiver** page contains the following fields:

Port — The port IP address on which the cable is tested.

Temperature — The temperature (C) 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 the Optical Transceiver Diagnostics Test Results Table

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

   The test runs and the **Optical Transceiver Diagnostics Table** page opens.

In addition to the fields in the **Optical Transceiver** page, the **Optical Transceiver Diagnostics Table** contains the following field:

Unit No. — The unit number for which the cable is displayed.

- **N/A** — Not Available, N/S - Not Supported, W - Warning, E - Error

NOTE: Finisar transceivers do not support transmitter fault diagnostic testing.

NOTE: Fiber Optic analysis feature works only on SFPs that support the digital diagnostic standard SFF-872.

Performing Fiber Optic Cable Tests Using CLI Commands

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

Table 6-38. 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# show fiber-ports optical-transceiver detailed


Port   Temp   Voltage   Current   Output   Input     POWER    LOS
       [C]              [Volt]    [mA]     [mWatt]   TX       Fault
                                                     [mWatt]
----   ----   ------    -----     ------   ------    ------   -----
1/e1   48     5.15      50        1.789    1.789     No       No
1/e2   43     5.15      10        1.789    1.789     No       No
```

Managing Switch 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 or source IP subnets.

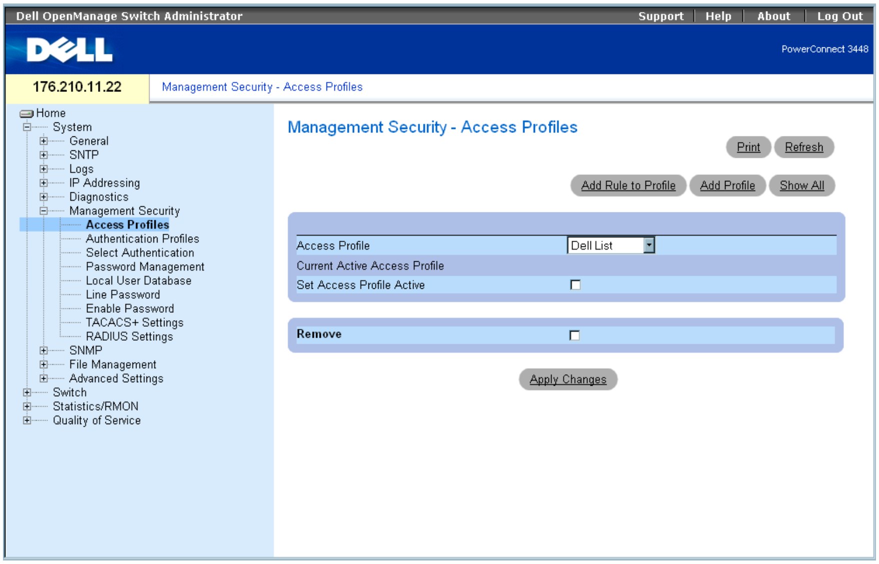
Management access can be separately defined for each type of management access method, including Web (HTTP), Secure Web (HTTPS), Telnet, and Secure Telnet.

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 up to 256 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 6-38. Access Profiles



The **Access Profiles** page contains following fields:

Access Profile — User-defined Access Profile lists. The Access Profile list contains a default value of **Console Only**. When this access profile is selected, active management of the device is performed using the console connection 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 in which the rules are implemented.

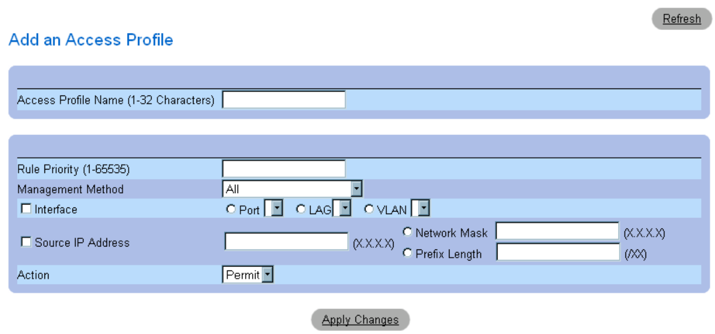
Defining Rules for an Access Profile:

1 Open the **Access Profiles** page.

2 Click **Add Profile.**

The **Add an Access Profile** page opens:

Figure 6-39. Add an Access Profile



The **Add an Access Profile** page contains the following additional fields:

Access Profile Name (1-32 Characters) — User-defined name for the access profile. The Access Profile name can contain up to 32 characters.

Rule Priority (1-65535) — The rule priority. When the packet is matched to a rule, user groups are either granted access or denied access to device management. The rule order is set by defining a rule priority using this field. The rule number is essential to matching packets to rules, as packets are matched on a first-fit basis. The rule priorities can be viewed in the **Profile Rules Table**.

Management Method — The management method for which the access profile is defined. Users with this access profile are denied or permitted access to the device from the selected management method (line).

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, then 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 (X.X.X.X) — 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 (X.X.X.X) — The IP subnetwork mask.

Prefix Length (/XX) — 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.

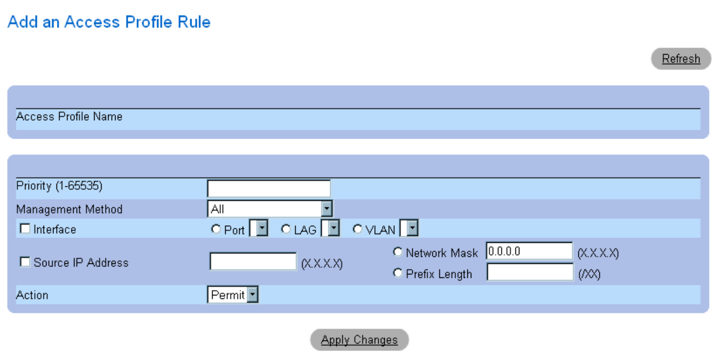
Adding Rules to Access Profile

NOTE: The first rule must be defined to beginning matching traffic to access profiles.

1 Open the **Access Profile** page.
2 Click **Add Rule to Profile**.

The **Add an Access Profile Rule** page opens:

Figure 6-40. Add an Access Profile Rule



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

The rule is added to the access profile, and the device is updated.

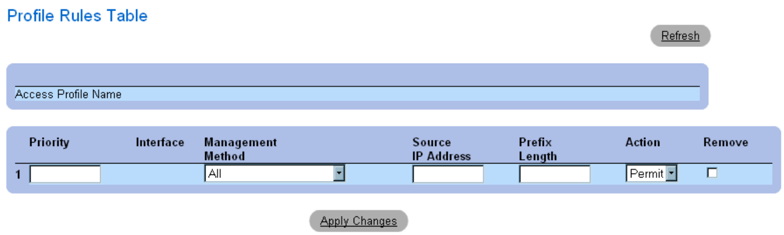
Viewing the Profile Rules Table

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 6-41. Profile Rules Table



Removing a Rule

1. Open the **Access Profiles** page.
2. Click **Show All**.

   The **Profile Rules Table** page 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 6-39. 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 6-39. 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 1/e1
console(config-macl)# permit ethernet 1/e2
console(config-macl)# deny ethernet 1/e3
console(config-macl)# deny ethernet 1/e4
console(config-macl)# exit
console(config)# management access-class mlist
console(config)# exit
console# show management access-list
mlist
-----
permit ethernet 1/e1
permit ethernet 1/e2
deny ethernet 1/e3
deny ethernet 1/e4
! (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 the authentication fails using the first method, the authentication process ends.

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 6-42. Authentication Profiles

The **Authentication Profiles** page contains the following fields:

Authentication Profile Name — User-defined authentication profile lists to which user-defined authentication profiles are added. The defaults are **Network Default** and **Console Default**.

- **Login** — Specifies the user-defined authentication profile list for login passwords.
- **Enable** — Specifies the user-defined authentication profile list for enable passwords.

Optional Methods — User authentication methods. The 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 Settings**.

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. Available for default profile only.

Remove — Removes the selected profile, when selected. Active profiles can not be deleted. Available for user-defined profiles only.

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. The authentication occurs in the order the authentication methods are listed.
4. Click **Apply Changes**.

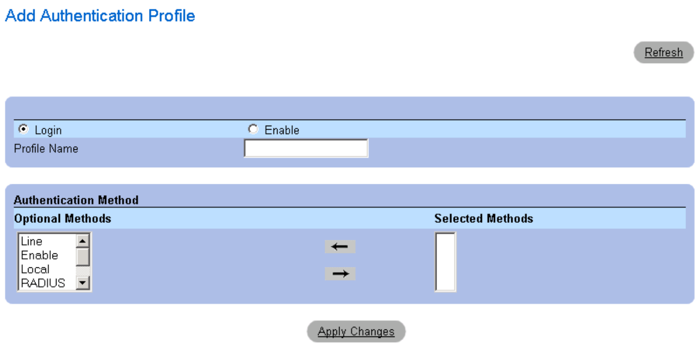
   The user authentication profile is updated to the device.

Adding an Authentication Profile:

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

   The **Add Authentication Profile** page opens:

Figure 6-43. Add Authentication Profile



3 Configure the profile.

NOTE: Do not include blank spaces in the name of the new profile.

4 Click **Apply Changes**.

The authentication profile is updated to the device.

Displaying the Authentication Profiles Table:

1 Open the **Authentication Profiles** page.

2 Click **Show All**.

The **Authentication Profiles Table** page opens.

Deleting an Authentication Profile:

1 Open the **Authentication Profiles** page.

2 Click **Show All**.

The **Authentication Profile Table** 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 6-40. 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.

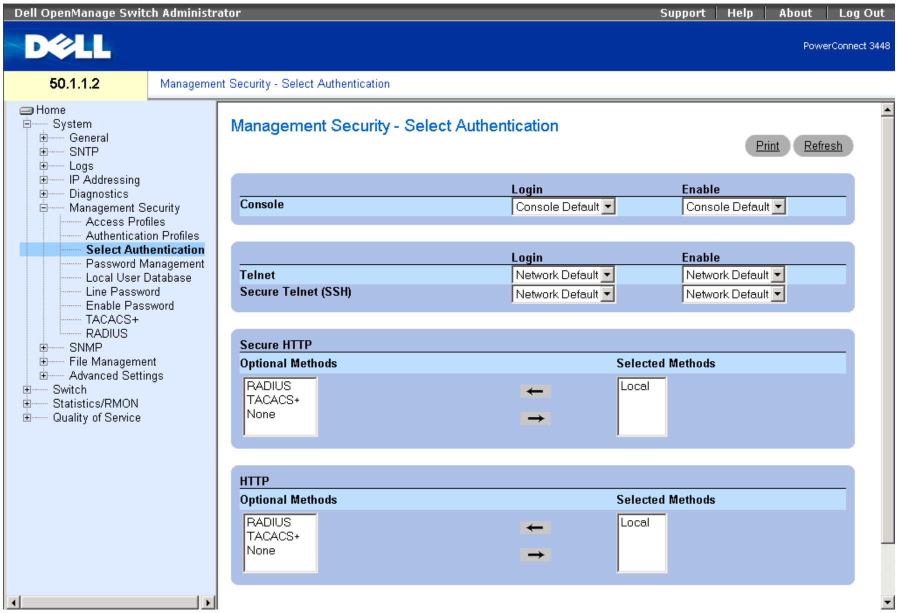
The following is an example of the CLI commands:

```
console(config)# aaa authentication login default radius local
enable none

console(config)# no aaa authentication login default
```

Selecting 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 List 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 6-44. Select Authentication



The **Select Authentication** page contains the following fields:

Console — Authentication profiles used to authenticate console users.

Login — Specifies authentication profiles to be used for users logging into the console interface.

Enable — pecifies authentication profiles to be used for users enabling the Privileged EXEC mode from the console interface.

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 6-41. Select Authentication CLI Commands

CLI Command	Description
enable authentication [**default** | *list-name*]	Indicates the authentication method list when accessing a higher privilege level from a remote Telnet, Console or SSH.
login authentication [**default** | *list-name*]	Indicates the login authentication method list for a remote Telnet, Console or SSH.
ip http authentication *method1* [*method2*.]	Indicates authentication methods for HTTP servers.
ip https authentication *method1* [*method2*.]	Indicates 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
---------------------------------
Console_Default    : None
Network_Default    : Local

Enable Authentication Method Lists
----------------------------------
Console_Default    : Enable   None
Network_Default    : Enable
```

```
Line               Login Method List       Enable Method List
----               -----------------       ------------------
Console            Default                 Default
Telnet             Default                 Default
SSH                Default                 Default

http               : Local
https              : Local
dot1x              :
```

Managing Passwords

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

- Defining minimum password lengths
- Password expiration
- Prevents frequent password reuse
- Locks users out after failed login attempts

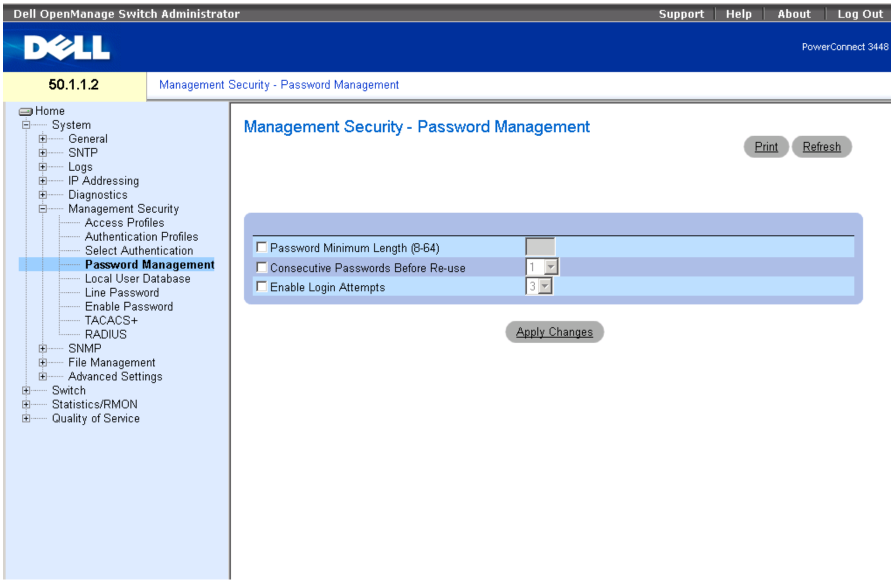
Password aging starts immediately, when password management is enabled. Passwords expire based on the user-defined time/day definition expiration. Ten days prior to password expiration, the device displays a password expiration warning message.

After the password has expired, users can login three additional times. During the three remaining logins an additional warning message displays informing the user that the password must be changed immediately. If the password is not changed,users are locked out of the system, and can only log in using the console. Password warnings are logged in the Syslog file.

If a privilege level is redefined, the user must also be re-defined. However, the password age time expires from the initial user definition.

To open the **Password Management** page, click **System→Management Security→Password Management** in the tree view.

Figure 6-45. Password Management



The **Password Management** page contains the following fields:

Password Minimum Length (8-64) — Indicates the minimum password length, when checked. For example, the administrator can define that all passwords must have a minimum of 10 characters.

Consecutive Passwords Before Re-use — Indicates the amount of times a password is changed, before the password can be reused. Possible field values are 1-10.

NOTE: The user is notified before the password expires and that it must be changed. However, this notification is not displayed to the Web user.

Enable Login Attempts — When checked, enables locking a user out of the device when a faulty password is used more than a user-defined number of times. For example, if this field is checked, configured to 5 and a user attempts to log on five times with an incorrect password, the device locks the user out on the sixth attempt. Possible field values are 1-5.

Defining Password Management

1. Open the **Password Management** page.
2. Define the fields.
3. Click Apply Changes.

   Password management is defined, and the device is updated.

Password Management Using CLI Commands

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

Table 6-42. Password Management Using CLI Commands

CLI Command	Description
password min-length *length*	Defines the minimum password length.
password history *number*	Defines the amount of times a password is changed, before the password can be reused.
password lock-out *number*	Defines the number of times a faulty password is entered before the user is locked out of the device.
show password configuration	Displays password management information.

The following is an example of the CLI commands:

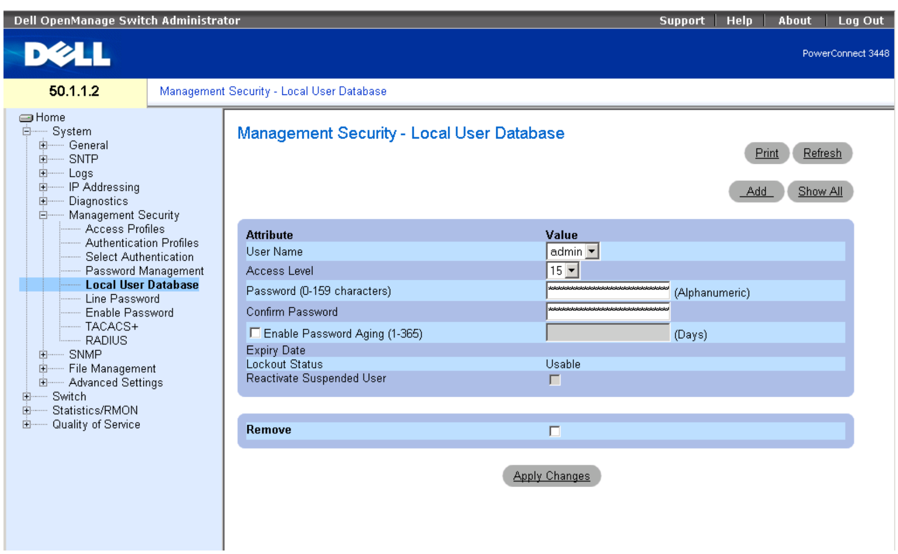
```
console # show passwords configuration


Minimal length: 0

History: Disabled

History hold time: no limit

Lockout control: disabled


Enable Passwords


Level          Password     Password      Lockout
               Aging        Expiry date

-----          --------     -----------   -------

1              -            -             -

15             -            -             -


Line Passwords

```

```
Line          Password     Password       Lockout
              Aging        Expiry date
-------       --------     -----------    -------
Telnet        -            -              -
SSH           -            -              -
Console       -            -              -

console # show users accounts

Username      Privilege    Password       Password       Lockout
                           Aging          Expiry Date
--------      ---------    --------       -----------    -------
nim           15           39             18-Feb-2005
```

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 6-46. Local User Database



The **Local User Database** page contains the following fields:

User Name — List of users.

Access Level — User access level. The lowest user access level is **1** and **15** is the highest user access level. Users with access level 15 are Privileged Users, and only they can access and use the OpenManage Switch Administrator.

Password (0-159 Characters) — User-defined password.

Confirm Password — Confirms the user-defined password.

Enable Password Aging (1-365) — Indicates the amount of time in days that elapses before a password is aged out, when selected.

Expiry Date — Indicates the expiration date of the user-defined password.

Lockout Status — Specifies the number of failed authentication attempts since the user last logged in successfully, when the **Enable Login Attempts** checkbox is selected in the **Password Management** page. Specifies **LOCKOUT**, when the user account is locked.

Reactivate Suspended User — Reactivate the specified user's access rights, when selected. Access rights can be suspended after unsuccessfully attempting to login.

Remove — Removes users from the **User Name** list, when selected.

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**.

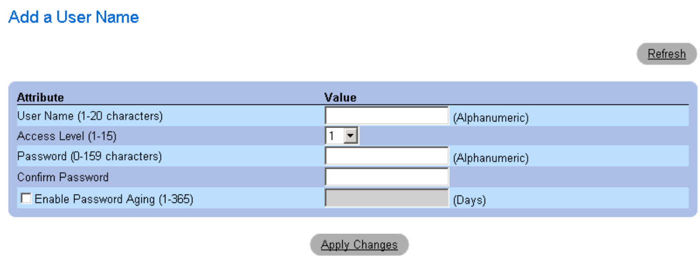
   The user access rights and passwords are defined, and the device is updated.

Defining a New User:

1. Open the **Local User Database** page.
2. Click **Add**.

   The **Add User** page opens:

Figure 6-47. Add a User



3 Define the fields.

4 Click **Apply Changes**.

The new user is defined, and the device is updated.

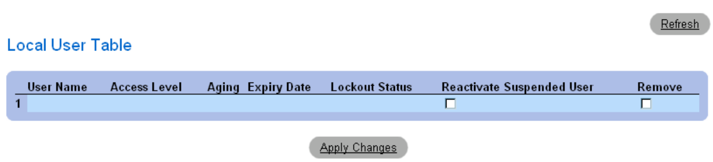
Displaying the Local User Table:

1 Open the **Local User Database** page.

2 Click **Show All.**

The **Local User Table** opens:

Figure 6-48. Local User Table



Reactivating a Suspended User:

1 Open the **Local User Database** page.

2 Click **Show All.**

The **Local User Table** opens.

3 Select a **User Name** entry.

4 Select the **Reactivate Suspended User** check box.

5 Click **Apply Changes**.

The user access rights are reactivated, and the device is updated.

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 6-43. Local User Database CLI Commands

CLI Command	Description
username *name* [**password** *password*] [**level** *level*] [**encrypted**]	Establishes a username-based authentication system.
set username *name* **active**	Reactivates a suspended user's access rights.

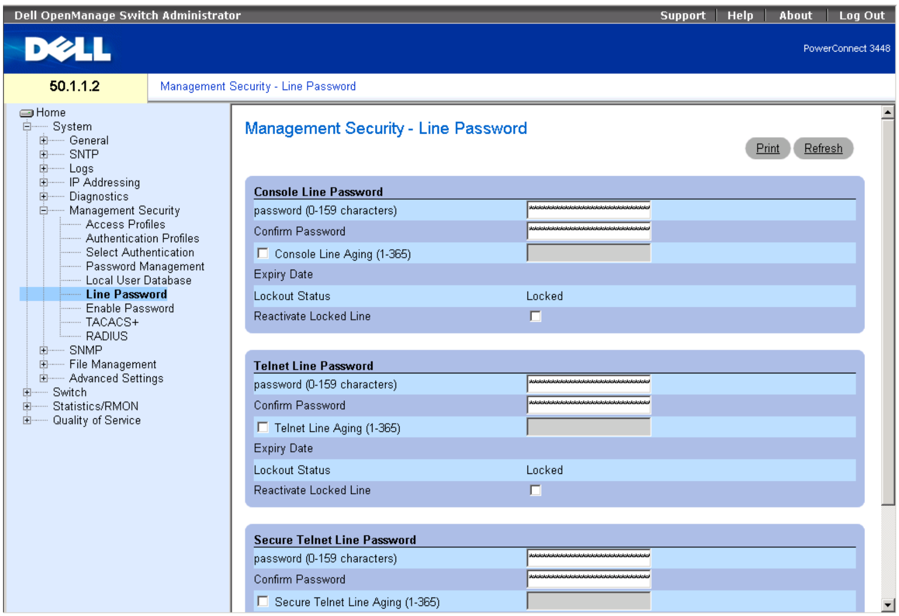
The following is an example of the CLI commands:

```
console(config)# username bob password lee level 15
console# set username bob active
```

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 6-49. Line Password



The **Line Password** page contains the following fields:

Line Password for Console/Telnet/Secure Telnet — The line password for accessing the device via a Console, Telnet, or Secure Telnet session.

Confirm Password for Console/Telnet/Secure Telnet — Confirms the new line password. The password appears in the ***** format.

Line Aging (1-365) for Console/Telnet/Secure Telnet — Indicates the amount of time in days that elapses before a line password is aged out, when selected.

Expiry Date for Console/Telnet/Secure Telnet — Indicates the expiration date of the line password.

Lockout Status for Console/Telnet/Secure Telnet — Specifies the number of failed authentication attempts since the user last logged in successfully, when the **Enable Login Attempts** checkbox is selected in the **Password Management** page. Specifies **LOCKOUT**, when the user account is locked.

Reactivate Locked Line for Console/Telnet/Secure Telnet — Reactivates the line password for a Console/Telnet/Secure Telnet session, when selected. Access rights can be suspended after unsuccessfully attempting to log in.

Defining Line Passwords for Console Sessions

1. Open the **Line Password** page
2. Define the **Console Line Password** 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 **Telnet Line Password** 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 **Secure Telnet Line Password** 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 6-44. Line Password CLI Commands

CLI Command	Description
password *password* [**encrypted**]	Indicates a password on a line.

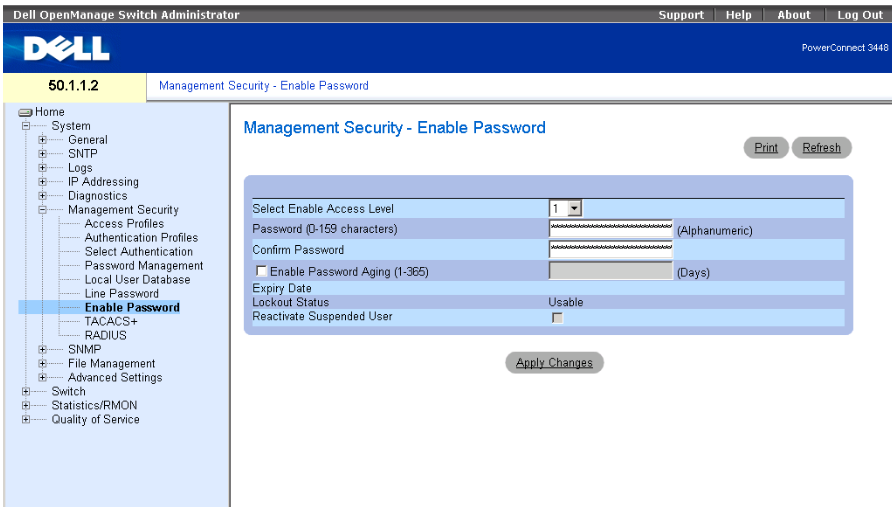
The following is an example of the CLI commands:

```
console(config-line)# password dell
```

Defining Enable Passwords

The **Enable Password** page sets a local password to control access to Normal and Privilege levels. To open the **Enable Password** page, click **System →Management Security →Enable Passwords** in the tree view.

Figure 6-50. Enable Password



The **Enable Password** page contains the following fields:

Select Enable Access Level — Access level associated with the enable password. Possible field values are 1-15.

Password (0-159 characters) — The current enable password.

Confirm Password — Confirms the new enable password. The password appears in the ***** format.

Enable Password Aging (1-365) — Indicates the amount of time in days that elapses before a password is aged out, when selected.

Expiry Date — Indicates the expiration date of the enable password.

Lockout Status — Specifies the number of failed authentication attempts since the user last logged in successfully, when the **Enable Login Attempts** checkbox is selected in the **Password Management** page. Specifies **LOCKOUT**, when the user account is locked.

Reactivate Suspended User — Reactivates the specified user's access rights, when selected. Access rights can be suspended after unsuccessfully attempting to login.

Defining a New Enable Password:

1 Open the **Enable Password** page.

2 Define the 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 **Enable Password** page.

Table 6-45. 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.

The following is an example of the CLI commands:

```
console(config)# enable password level 15 secret
```

Defining TACACS+ Settings

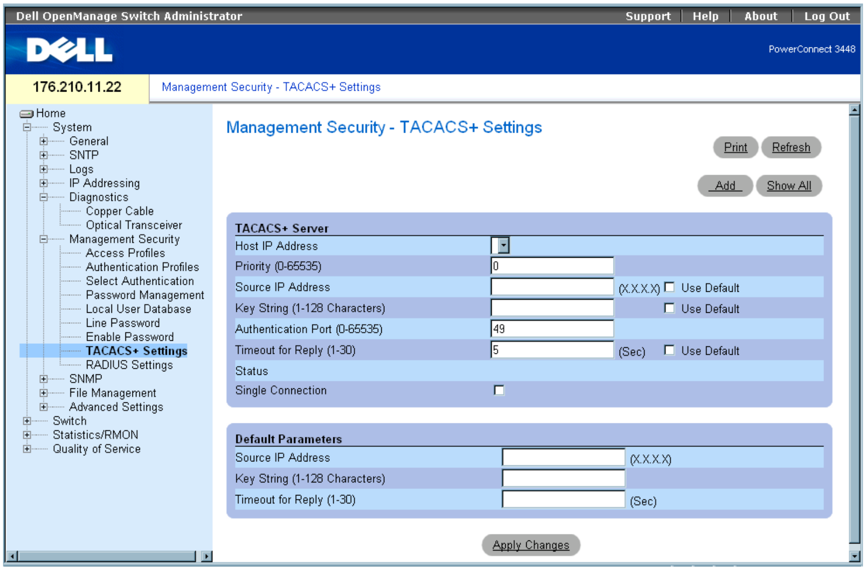
The devices provide Terminal Access Controller Access Control System (TACACS+) client support. TACACS+ provides centralized security for validation of users accessing the device.

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 6-51. TACACS+ Settings



The **TACACS+ Settings** page contains the following fields:

Host IP Address — Indicates the TACACS+ Server IP address.

Priority (0-65535) — Indicates 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 key used on the TACACS+ server. This key is encrypted.

Authentication Port (0-65535) — The port number through which the TACACS+ session occurs. The default is port 49.

Timeout for Reply (1-30) — 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+ 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. The default source IP address is 0.0.0.0.

Key String (0-128 Characters) — The default key string used for authenticating and encrypting all communications between the device and the TACACS+ server. This key is encrypted.

Timeout for Reply (1-30) — The default time that passes before the device and the TACACS+ server connection times out. The default is 5 seconds.

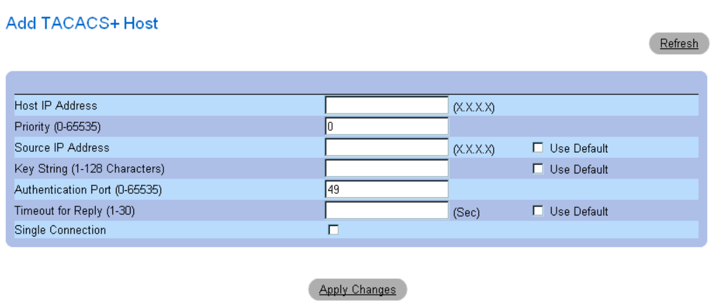
Adding a TACACS+ Server

1 Open the **TACACS+ Settings** page.

2 Click **Add.**

The **Add TACACS+ Host** page opens:

Figure 6-52. Add TACACS+ Host



3 Define the fields.

4 Click **Apply Changes**.

The TACACS+ server is added, and the device is updated.

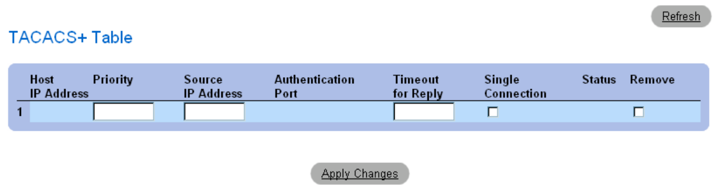
Displaying the TACACS+ Table

1 Open the **TACACS+ Settings** page.

2 Click **Show All**.

The **TACACS+ Table** opens:

Figure 6-53. TACACS+ Table



Removing a TACACS+ Server

1. Open the **TACACS+ Table** 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 6-46. 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*]	Indicates a TACACS+ host.
tacacs-server key *key-string*	Indicates 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*	Indicates the timeout value in seconds. (Range: 1 - 30.)
tacacs-server source-ip *source*	Indicates 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
Device 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
Device Configuration
--------------------
Source IP : 0.0.0.0
console#
```

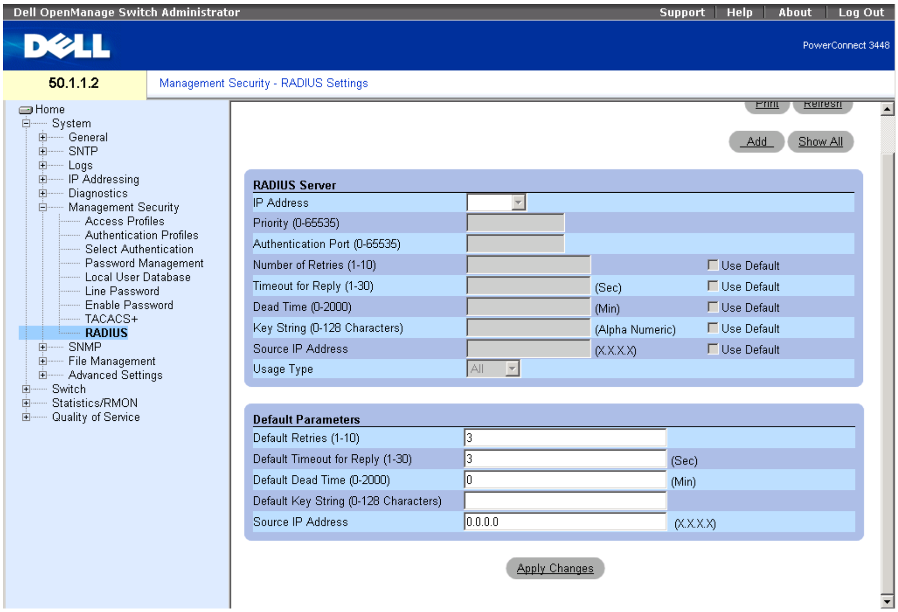
Configuring RADIUS Settings

Remote Authorization Dial-In User Service (RADIUS) servers provide additional security for networks. Up to four RADIUS servers can be defined. RADIUS servers provide a centralized authentication method for:

- Telnet Access
- Secure Shell Access
- Web Access
- Console Access

To open the **RADIUS Settings** page, click **System →Management Security →RADIUS** in the tree view.

Figure 6-54. RADIUS Settings



The **RADIUS Settings** page contains the following pages:

IP Address — The list of Authentication Server IP addresses.

Priority (0-65535) — The server priority. The possible values are 0-65535, where 0 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) — Indicates the number of transmitted requests sent to RADIUS server before a failure occurs. The possible field values are 1-10.

Timeout for Reply (1-30) — Indicates 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.

Dead Time (0-2000) — Indicates the amount of time (in minutes) that a RADIUS server is bypassed for service requests. The range is 0-2000.

Key String (1-128 Characters) — 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 — Indicates the source IP address that is used for communication with RADIUS servers.

Usage Type — Indicates the server usage type. Can be one of the following values: login, 802.1x or all. If unspecified, defaults to all.

The following fields set the RADIUS default values:

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) — Indicates the default number of transmitted requests sent to RADIUS server before a failure occurs.

Default Timeout for Reply (1-30) — Indicates the default amount of the time (in seconds) the device waits for an answer from the RADIUS server before timing out. The default is 5 seconds.

Default Dead time (0-2000) — Indicates the default amount of time (in minutes) that a RADIUS server is bypassed for service requests. The range is 0-2000.

Default Key String (1-128 Characters) — 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 — Indicates the default source IP address that is used for communication with RADIUS servers. The default source IP address is 0.0.0.0.

Defining RADIUS Parameters:

1. Open the **RADIUS Settings** page.
2. Define the fields.
3. Click **Apply Changes**.

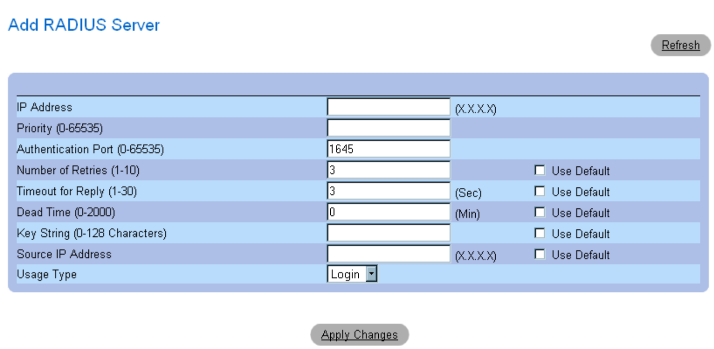
   The RADIUS setting are updated to the device.

Adding a RADIUS Server:

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

   The **Add RADIUS Server** page opens:

Figure 6-55. Add RADIUS Server



3 Define the fields.

4 Click **Apply Changes**.

The new RADIUS server is added, and the device is updated.

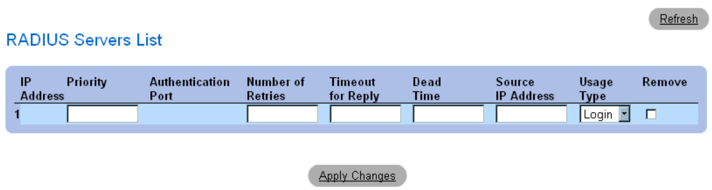
Displaying the RADIUS Server List:

1 Open the **RADIUS Settings** page.

2 Click **Show All**.

The **RADIUS Servers List** opens:

Figure 6-56. RADIUS Servers List



Removing a RADIUS Server

1 Open the **RADIUS Settings** page.

2 Click **Show All**.

The **RADIUS Servers List** opens.

3 Select a **RADIUS Servers List** entry.

4 Select the **Remove** check box.

5 Click **Apply Changes**.

The RADIUS server is removed, and the device is updated.

Defining RADIUS Servers Using CLI Commands

The following table summarizes the equivalent CLI commands for defining fields displayed on the **RADIUS Settings** page.

Table 6-47. RADIUS Server CLI Commands

CLI Command	Description
radius-server timeout *timeout*	Sets the interval for which a router waits for a server host to reply.
radius-server retransmit *retries*	Specifies the number of times the software searches the list of RADIUS server hosts.

Table 6-47. RADIUS Server CLI Commands *(continued)*

CLI Command	Description
radius-server deadtime *deadtime*	Configures unavailable servers to be skipped.
radius-server key *key-string*	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS environment.
radius-server host *ip-address* [**auth-port** *auth-port-number*] [**timeout** timeout] [**retransmit** *retries*] [**deadtime** *deadtime*] [**key** *key-string*] [**source** *source*] [**priority** *priority*]	Specifies a RADIUS server host.
show radius-servers	Displays the RADIUS server settings.

The following is an example of 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 127
timeout 20

Console# show radius-servers

IP address  Auth   Acct TimeOut   Retransmit  Deadtime   Source IP  Priority

--------    ---- ----  ------    ---------  -------    -------    ------

172.16.1.1   164    51646  3        3            0                  01
172.16.1.2   164    51646  3        3            0                  02
```

Defining SNMP Parameters

Simple Network Management Protocol (SNMP) provides a method for managing network devices. The switch supports the following SNMP versions:

- SNMPv1 (version 1)
- SNMPv2 (version 2)
- SNMPv3 (version 3)

SNMP v1 and v2

The SNMP agents maintains a list of variables, which are used to manage the switch. 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.

SNMPv1 and v2 are enabled by default.

SNMP v3

SNMP v3 also applies access control and a new traps mechanism to SNMPv1 and SNMPv2 PDUs. In addition, a User Security Model (USM) is defined for SNMPv3, which includes:

- **Authentication** — Provides data integrity and data origin authentication.
- **Privacy** — Protects against disclosure message content. Cipher Block-Chaining (CBC) is used for encryption. Either authentication is enabled on an SNMP message, or both authentication and privacy are enabled on an SNMP message. However privacy cannot be enabled without authentication.
- **Timeliness** — Protects against message delay or message redundancy. The SNMP agent compares incoming message to the message time information.
- **Key Management** — Defines key generation, key updates, and key use.

The switch supports SNMP notification filters based on Object IDs (OID). OIDs are used by the system to manage switch features. SNMP v3 supports the following features:

- Security
- Feature Access Control
- Traps

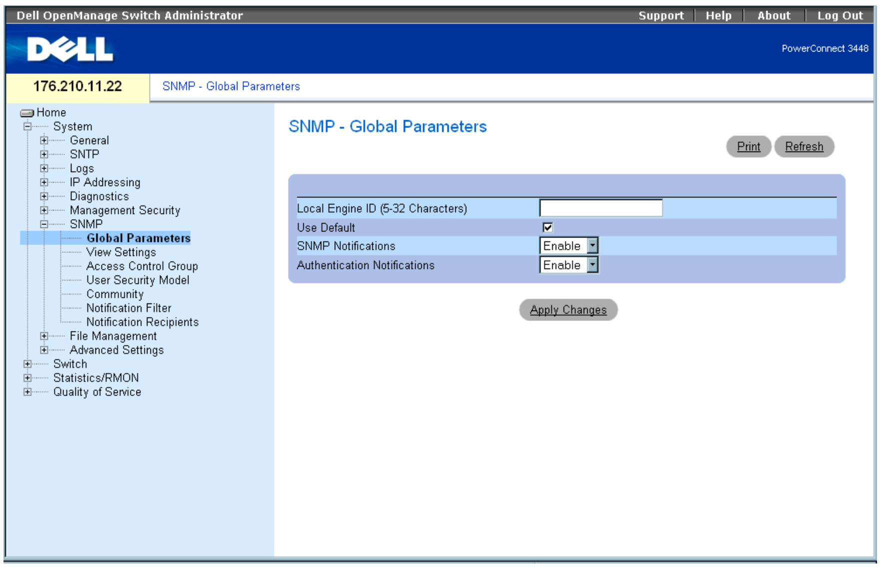
Authentication or Privacy Keys are modified in the **User Security Model (USM)**.

SNMPv3 can be enabled on if the Local Engine ID is enabled.

Defining SNMP Global Parameters

The **SNMP Global Parameters** page permits enabling both SNMP and Authentication notifications. To open the **SNMP Global Parameters** page, click **System →SNMP →Global Parameters** in the tree view.

Figure 6-57. SNMP Global Parameters



The **SNMP Global Parameters** page contains the following fields:

Local Engine ID — Indicates the local device engine ID. The field value is a hexadecimal string. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or a colon. The Engine ID must be defined before SNMPv3 is enabled.

For stand-alone devices select a default Engine ID that is comprised of Enterprise number and the default MAC address.

For a stackable system configure the Engine ID, and verify that the Engine ID is unique for the administrative domain. This prevents two devices in a network from having the same Engine ID.

Use Defaults — Uses the device generated Engine ID. The default Engine ID is based on the device MAC address and is defined per standard as:

> **First 4 octets** — first bit = 1, the rest is IANA Enterprise number = 674.
>
> **Fifth octet** — Set to 3 to indicate the MAC address that follows.
>
> **Last 6 octets** — MAC address of the device.

SNMP Notifications — Enables or disables the router sending SNMP notifications.

Authentication Notifications — Enables or disables the router sending SNMP traps when authentication fails.

Enabling SNMP Notifications

1. Open the **SNMP Global Parameters** page.
2. Select **Enable** in the **SNMP Notifications** field.
3. Click **Apply Changes**.

   SNMP notifications are enabled, and the device is updated.

Enabling Authentication Notifications

1. Open the **SNMP Global Parameters** page.
2. Select **Enable** in the **Authentication Notifications** field.
3. Click **Apply Changes**.

Enabling SNMP Notifications Using CLI Commands

The following table summarizes the equivalent CLI commands for viewing fields displayed in the SNMP Global Parameters page.

Table 6-48. SNMP Notification Commands

CLI Command	Description
snmp-server enable traps	Enables the router to send Simple Network Management Protocol traps
snmp-server trap authentication	Enables the router to send Simple Network Management Protocol traps when authentication fails
show snmp	Checks the status of SNMP communications.
snmp-server engine ID local {*engineid-string* | **default**}	Indicates the local device engine ID. The field values is a hexadecimal string. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon. The Engine ID must be defined before SNMPv3 is enabled.

The following is an example of the CLI commands:

```
Console(config)# snmp-server enable traps
Console(config)# snmp-server trap authentication
Console# show snmp

Community-String  Community-Access    View name     IP address
----------------  -----------------   ---------     ----------
public            read only           view-1        All

Community-String  Group name          IP address    Type
----------------  ----------          ----------    ----


Traps are enabled.
Authentication-failure trap is enabled.

Version 1,2 notifications
Target    Type    Community  Version   Udp   Filter  To    Retries
Address                                Port  name    Sec
-------   ----    ---------  -------   ----  ------  ---   -------


Version 3 notifications
Target    Type    Username   Security  Udp   Filter  To    Retries
Address                      Level     Port  name    Sec
--------  ----    ---------  --------  ----  ------  ---   -------
                                       -     -


System Contact: Robert
System Location: Marketing
```

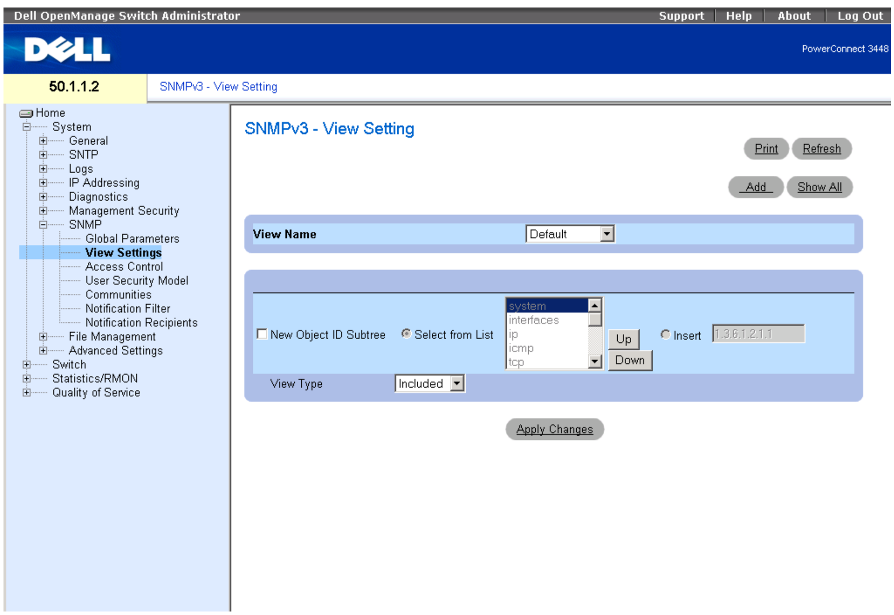
Defining SNMP View Settings

SNMP Views provide access or block access to device features or feature aspects. For example, a view can be defined which states that SNMP group A has read only (R/O) access to Multicast groups, while SNMP group B has read-write (R/W) access to Multicast groups. Feature access is granted via the MIB name, or MIB Object ID.

The Up and Down arrows allow navigating through the MIB tree, and MIB branches.

To open the **SNMPv3 View Settings** page, click **System** →**SNMP** →**View Settings** in the tree view.

Figure 6-58. SNMPv3 View Settings



The **SNMPv3 View Settings** page contains the following fields:

View Name — Contains a list of user-defined views. The view name can contain a maximum of 30 alphanumeric characters.

New Object ID Subtree — Indicates the device feature OID included or excluded in the selected SNMP view.

> **Selected from List** — Select the device feature OID by using the **Up** and **Down** buttons to scroll through a list of all device OIDs.
>
> **Insert** — Specify the device feature OID.

View Type — Indicates if the defined OID branch will be included or excluded in the selected SNMP view.

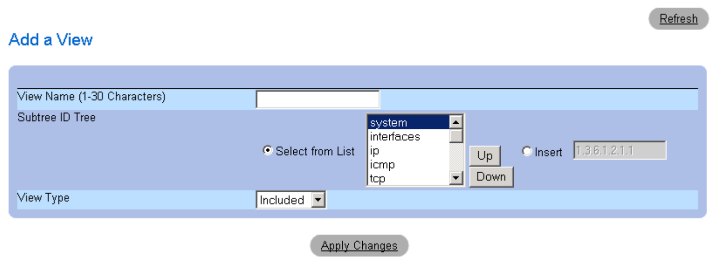
Adding a View

1 Open the **SNMPv3 View Settings** page.

2 Click **Add**.

The **Add A View** page opens:

Figure 6-59. Add A View



3 Define the field.

4 Click **Apply Changes**.

The SNMP View is added, and the device is updated.

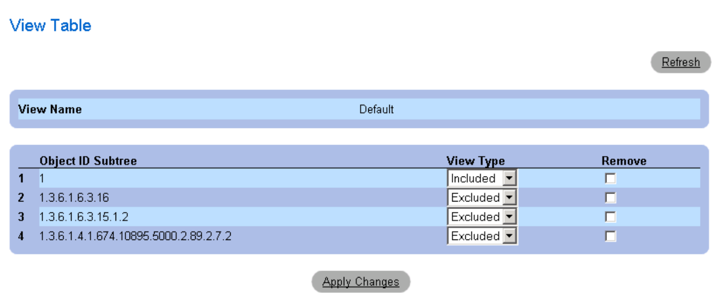
Displaying the View Table

1 Open the **SNMPv3 View Settings** page.

2 Click **Show All**.

The **View Table** page opens:

Figure 6-60. View Table



Defining SNMPv3 Views Using CLI Commands

The following table summarizes the equivalent CLI commands for defining fields displayed in the **SNMPv3 View Settings** page.

Table 6-49. SNMP View CLI Commands

CLI Command	Description
snmp-server view *view-name oid-tree* {**included** | **excluded**}	Creates or updates a view entry.
show snmp views [*viewname*]	Displays the configuration of views.

The following is an example of CLI commands:

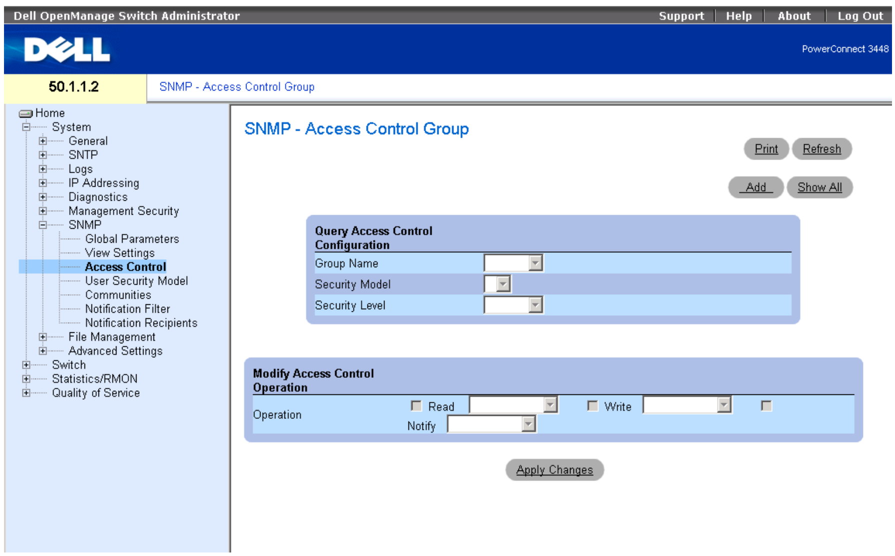
```
Console(config)# snmp-server view user1 1 included

Console(config)# end

Console# show snmp views


Name                 OID Tree               Type
-------------        -----------------      --------
user1                iso                    included
Default              iso                    included
Default              snmpVacmMIB            excluded
Default              usmUser                excluded
Default              rndCommunityTable      excluded
DefaultSuper         iso                    included
```

Defining SNMP Access Control

The **Access Control** page provides information for creating SNMP groups, and assigning SNMP access control privileges to SNMP groups. Groups allow network managers to assign access rights to specific device features, or features aspects.

To open the **Access Control Group** page, click **System →SNMP →Access Control** in the tree view.

Figure 6-61. Access Control Group



The **Access Control Group** contains the following fields:

Group Name — The user-defined group to whom access control rules are applied. The field range is up to 30 characters.

SNMP Version — Defines the SNMP version attached to the group. The possible field values are:

- **SNMPv1** — SNMPv1 is defined for the group.
- **SNMPv2** — SNMPv2 is defined for the group.
- **SNMPv3** — SNMPv3 is defined for the group.

Security Level — The security level attached to the group. Security levels apply to SNMPv3 only. The possible field values are:

- **No Authentication** — Neither the Authentication nor the Privacy security levels are assigned to the group.
- **Authentication** — Authenticates SNMP messages, and ensures the SNMP messages origin is authenticated.
- **Privacy** — Encrypts SNMP message.

Operation — Defines the group access rights. The possible field values are:

Read — The management access is restricted to read-only, and changes cannot be made to the assigned SNMP view.

Write — The management access is read-write and changes can be made to the assigned SNMP view.

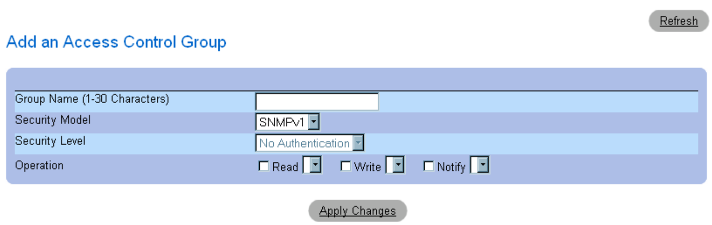
Notify — Sends traps for the assigned SNMP view.

Defining SNMP Groups

1. Open the **Access Control Group** page.
2. Click **Add**.

   The **Add an Access Control Group** page opens:

Figure 6-62. Add an Access Control Group



3. Define the fields in the **Add an Access Control Group** page.
4. Click **Apply Changes**.

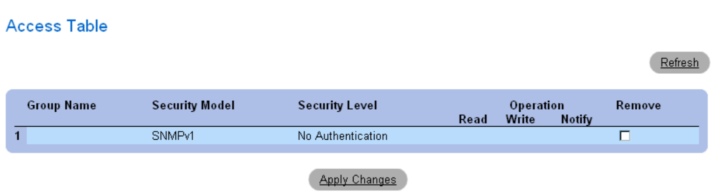
   The group is added, and the device is updated.

Displaying the Access Table

1. Open the **Access Control Group** page.
2. Click **Show All**.

   The **Access Table** opens:

Figure 6-63. Access Table



Removing SNMP Groups

1 Open the **Access Control Group** page.

2 Click **Show All**.

The **Access Table** opens.

3 Select a SNMP group.

4 Check the **Remove** checkbox.

5 Click **Apply Changes**.

The SNMP group is deleted, and the device is updated.

Defining SNMP Access Control Using CLI Commands

The following table summarizes the equivalent CLI commands for defining fields displayed in the **Access Control Group** page.

Table 6-50. SNMP Access Control CLI Commands

CLI Command	Description
snmp-server group *groupname* {**v1** | **v2** | **v3** {**noauth** | **auth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*]	Configure a new Simple Network Management Protocol (SNMP) group, or a table that maps SNMP users to SNMP views.
show snmp groups [*groupname*]	Displays the configuration of groups

The following is an example of the CLI commands:

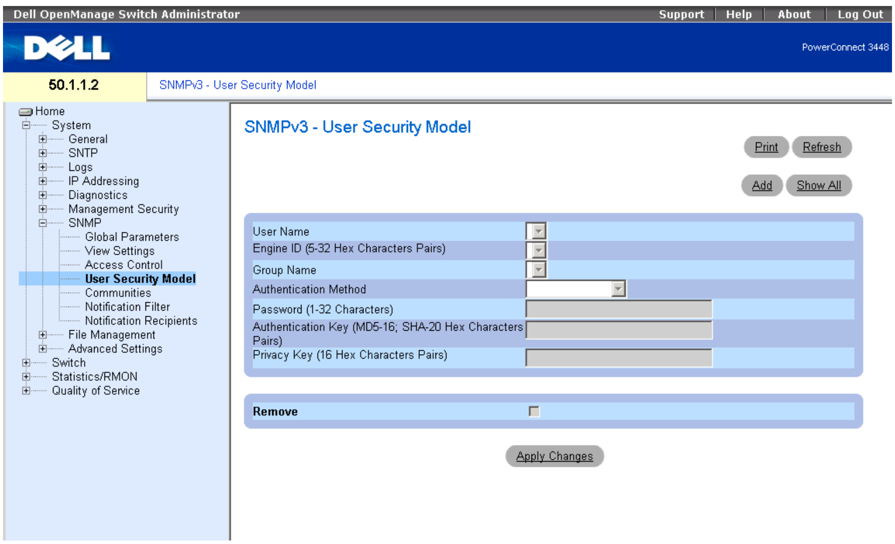
```
console (config)# snmp-server group user-group v3 priv read user-
view
```

Assigning SNMP User Security

The **SNMPv3 User Security Model (USM)** page enables assigning system users to SNMP groups, as well as defining the user authentication method.

To open the **SNMPv3 User Security Model (USM)** page, click **System→SNMP →User Security Model** in the tree view.

Figure 6-64. SNMPv3 User Security Model (USM)



The **SNMPv3 User Security Model (USM)** page contains the following fields:

User Name — Contains a list of user-defined user names. The field range is up to 30 alphanumeric characters.

Engine ID — Indicates either the local or remote SNMP entity, to which the user is connected. Changing or removing the local SNMP Engine ID deletes the SNMPv3 User Database.

> **Local** — Indicates that the user is connected to a local SNMP entity.
>
> **Remote** — Indicates that the user is connected to a remote SNMP entity. If the Engine ID is defined, remote devices receive inform messages.

Group Name — Contains a list of user-defined SNMP groups. SNMP groups are defined in the **Access Control Group** page.

Authentication Method — The authentication method used to authenticate users. The possible field values are:

> **MD5 Key**— Users are authenticated using the HMAC-MD5 algorithm.
>
> **SHA Key** — Users are authenticated using the HMAC-SHA-96 authentication level.

MD5 Password — Indicates that HMAC-MD5-96 password is used for authentication. The user should enter a password.

SHA Password — Users are authenticated using the HMAC-SHA-96 authentication level. The user should enter a password.

None — No user authentication is used.

Password (0-32 Characters) — Modifies the user-defined password for a group. Passwords can contain a maximum of 32 alphanumeric characters.

Authentication Key (MD5-16; SHA-20 hexa chars) — Defines the HMAC-MD5-96 or HMAC-SHA-96 authentication level. The authentication and privacy keys are entered to define the authentication key. If only authentication is required, 16 bytes are defined for MD5. If both privacy and authentication are required, 32 bytes are defined for MD5. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or a colon.

Privacy Key (16 hexa characters) — If only authentication is required, 20 bytes are defined. If both privacy and authentication are required, 16 bytes are defined. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon.

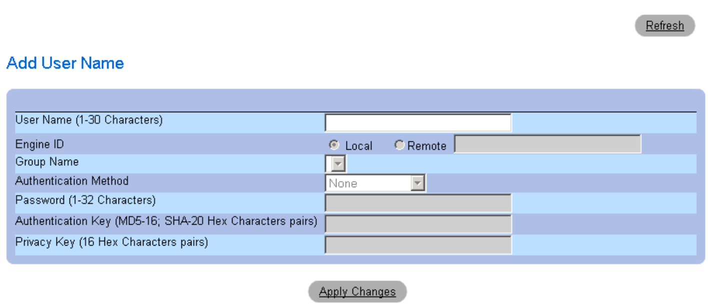
Remove — When checked, removes users from a specified group.

Adding Users to a Group

1. Open the **SNMPv3 User Security Model (USM)** page.
2. Click **Add**.

   The **Add SNMPv3 User Name** page opens:

Figure 6-65. Add SNMPv3 User Name



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

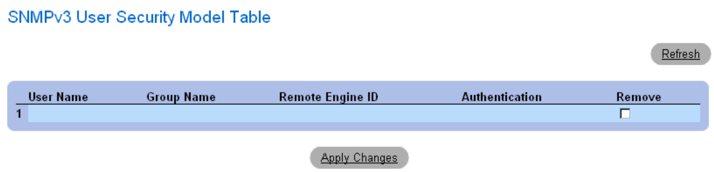
   The user is added to the group, and the device is updated.

Displaying the User Security Model Table

1. Open the **SNMPv3 User Security Model (USM)** page.
2. Click **Show All**.

   The **User Security Model Table** opens:

Figure 6-66. User Security Model Table



Deleting an User Security Model Table Entry

1. Open the **SNMPv3 User Security Model (USM)** page.
2. Click **Show All**.

   The **User Security Model Table** opens.

3. Select a **User Security Model Table** entry.
4. Check the **Remove** checkbox.
5. Click **Apply Changes**.

   The **User Security Model Table** entry is deleted, and the device is updated.

Defining SNMPv3 Users Using CLI Commands

The following table summarizes the equivalent CLI commands for defining fields displayed in the **SNMPv3 User Security Model (USM)** page.

Table 6-51. SNMPv3 User CLI Commands

CLI Command	Description
snmp-server user *username groupname* [**remote** *engineid-string*] [**auth-md5** *password* | **auth-sha** *password* | **auth-md5-key** *md5-des-key* | **auth-sha-key** *sha-des-key*]	Configures a new SNMP V3 user.
show snmp users [*username*]	Displays the configuration of users.

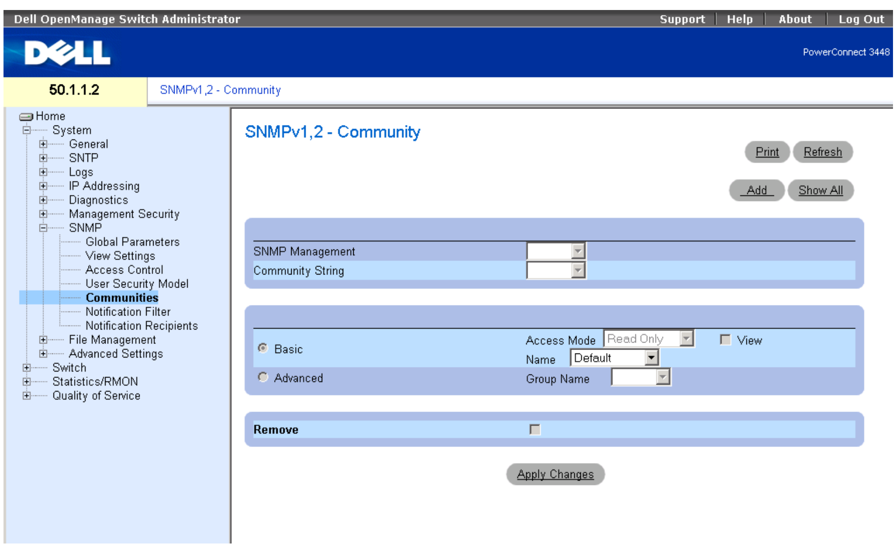
The following is an example of the CLI commands:

```
console (config)# snmp-server user John user-group auth-md5 1234
console (config)# end
console# show snmp users

Name         Group Name    Auth Method     Remote
-------      ----------    -----------     ------
John         user-group    md5
```

Defining SNMP Communities

Access rights are managed by defining communities on the **SNMPv1,2 Community** page. When the community names are changed, access rights are also changed. SNMP Communities are defined only for SNMP v1 and SNMP v2. To open the **SNMPv1,2 Community** page, click **System→ SNMP→Communities** in the tree view.

Figure 6-67. SNMPv1,2 Community



The **SNMPv1,2 Community** page contains the following fields:

SNMP Management Station — The management station IP address for which the SNMP community is defined.

Community String — Functions as a password and used to authenticate the management station to the device.

Basic — Enables SNMP Basic mode for a selected community. The possible field values are:

Access Mode — Defines the access rights of the community. The possible field values are:

Read-Only — Management access is restricted to read-only, and changes cannot be made to the community.

Read-Write — Management access is read-write and changes can be made to the device configuration, but not to the community.

SNMP-Admin — User has access to all device configuration options, as well as permissions to modify the community.

View Name — Contains a list of user-defined SNMP views

Name — Specifies the name of the community used for SNMPv1,v2.

Advanced — Contains a list of user-defined groups. When SNMP Advanced mode is selected, the SNMP access control rules comprising the group are enabled for the selected community. The Advanced mode also enables SNMP groups for specific SNMP communities. The SNMP Advanced mode is defined only with SNMPv3. The possible field value is:

Group Name — Specifies the name of the group when working in SNMP Advanced mode.

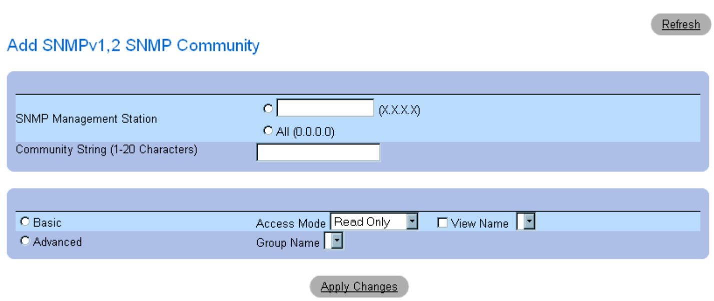
Remove — When checked, removes a community.

Defining a New Community

1. Open the **SNMPv1,2 Community** page.
2. Click **Add**.

The **Add SNMP Community** page opens:

Figure 6-68. Add SNMP Community



3. Complete the relevant fields.
4. Click **Apply Changes**.

   The new community is saved, and the device is updated.

Deleting Communities

1. Open the **SNMPv1,2 Community** page.
2. Click **Show All**.

   The **Community Table** page opens.
3. Select a community and check the **Remove** check box.
4. Click **Apply Changes**.

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

Configuring Communities Using CLI Commands

The following table summarizes the equivalent CLI commands for viewing fields displayed in the **SNMPv1,2 Community**.

Table 6-52. SNMP Community CLI Commands

CLI Command	Description
snmp-server community *community* [**ro** | **rw** | **su**] [*ip-address*][**view** *view-name*]	Sets up the community access string to permit access to the SNMP protocol.
snmp-server community-group *community group-name* [*ip-address*]	Sets up community access string to permit limited access to the SNMP protocol based on group access rights.
show snmp	Displays the current SNMP device configuration.

The following is an example of the CLI commands:

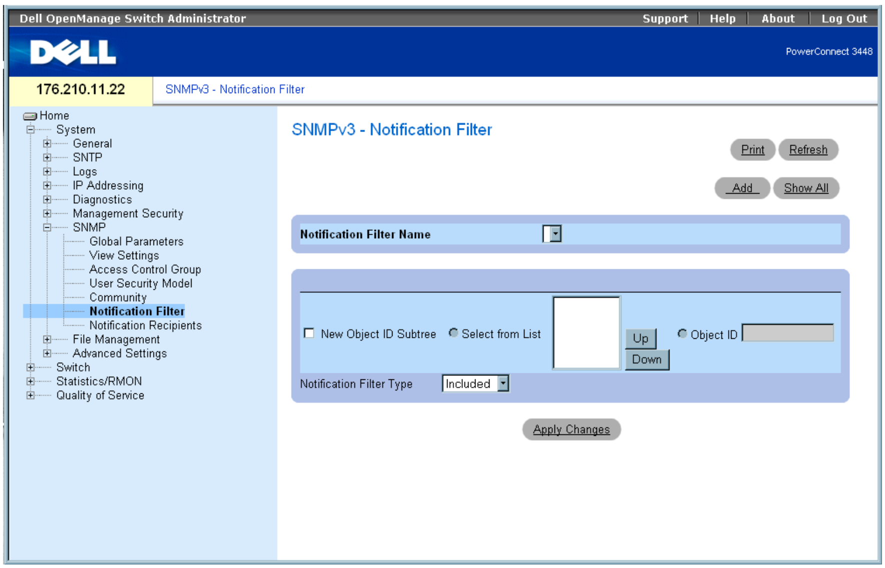
```
Console (config)# snmp-server community dell ro 10.1.1.1
```

Defining SNMP Notification Filters

The **Notification Filter** page permits filtering traps based on OIDs. Each OID is linked to a device feature or a feature aspect. The **Notification Filter** page also allows network managers to filter notifications.

To open the **Notification Filter** page, click **System→SNMP →Notification Filters** in the tree view.

Figure 6-69. Notification Filter



The **Notification Filter** page contains the following fields:

Notification Filter Name — The user-defined notification filter.

New Object Identifier Tree — The OID for which notifications are sent or blocked. If a filter is attached to an OID, traps or informs are generated and sent to the trap recipients. Object IDs are selected from either the **Select from List** or the **Object ID List**.

Notification Filter Type — Indicates whether informs or traps are sent regarding the OID to the trap recipients.

Excluded — Restricts sending OID traps or informs.

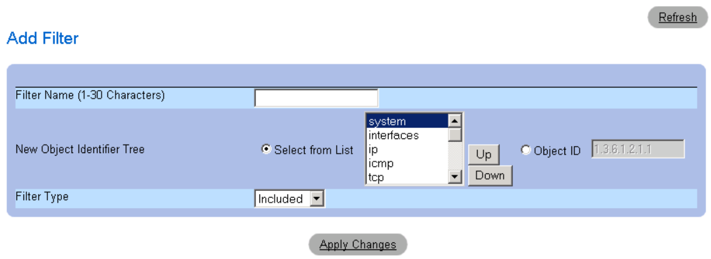
Included — Sends OID traps or informs.

Adding SNMP Filters

1. Open the **Notification Filter** page.
2. Click **Add**.

   The **Add Filter** page opens:

Figure 6-70. Add Filter



3 Define the relevant fields.

4 Click **Apply Changes**.

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

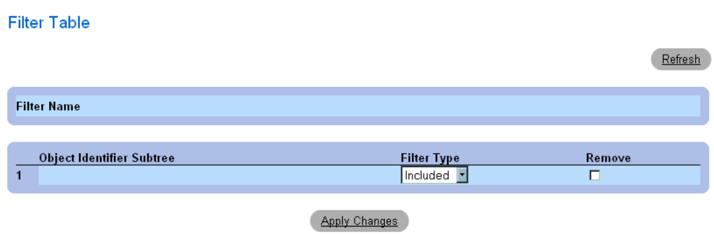
Displaying the Filter Table

1 Open the **Notification Filter** page.

2 Click **Show All**.

The **Filter Table** opens:

Figure 6-71. Filter Table



Removing a Filter

1 Open the **Notification Filter** page.

2 Click **Show All**.

The **Filter Table** opens.

3 Select a **Filter Table** entry.

4 Check the **Remove** checkbox.

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

Configuring Notification Filters Using CLI Commands

The following table summarizes equivalent CLI commands for defining fields displayed in the **Notification Filter** page.

Table 6-53. SNMP Notification Filter CLI Commands

CLI Command	Description
snmp-server filter *filter-name oid-tree* {**included** | **excluded**}	Creates or updates an SNMP notification filter.
show snmp filters [*filtername*]	Displays the configuration of SNMP notification filters

The following is an example of CLI commands:

```
Console (config)# snmp-server filter user1 iso included
Console(config)# end
Console # show snmp filters

Name             OID Tree          Type
-----------      -------------     --------
user1            iso               Included
```

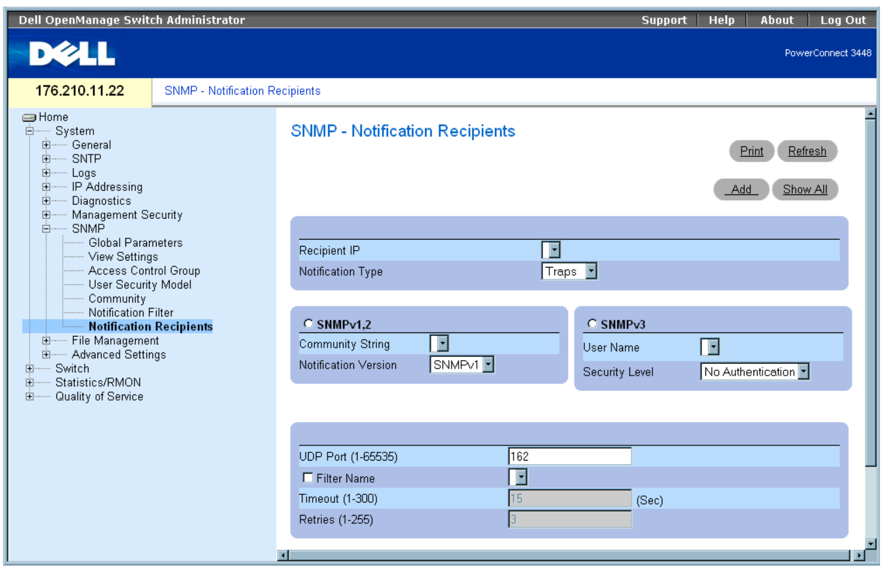
Defining SNMP Notification Recipients

The **Notification Recipients** page contains information for defining filters that determine whether traps are sent to specific users, and the trap type sent. SNMP notification filters provide the following services:

- Identifying Management Trap Targets
- Trap Filtering
- Selecting Trap Generation Parameters
- Providing Access Control Checks

To open the **Notification Recipients** page, click **System→SNMP→Notification Recipient** in the tree view.

Figure 6-72. Notification Recipients



The **Notification Recipients** page contains the following fields:

Recipient IP — Indicates the IP address to whom the traps are sent.

Notification Type — The notification sent. The possible field values are:

> **Trap** — Traps are sent.
>
> **Inform** — Informs are sent.

SNMPv1,2 — SNMP versions 1 and 2 are enabled for the selected recipient. Define the following fields for SNMPv1 and SNMPv2:

Community String (1-20 Characters) — Identifies the community string of the trap manager.

Notification Version — Determines the trap type. The possible field values are:

SNMP V1 — SNMP Version 1 traps are sent.

SNMP V2 — SNMP Version 2 traps are sent.

SNMPv3 — SNMPv3 is used to send and receive traps. Define the following fields for SNMPv3:

User Name — The user to whom SNMP notifications are sent.

Security Level — Defines the means by which the packet is authenticated. The possible field values are:

No Authentication — The packet is neither authenticated nor encrypted.

Authentication — The packet is authenticated.

Privacy — The packet is both authenticated and encrypted.

UDP Port (1-65535) — The UDP port used to send notifications. The default is 162.

Filter Name — Includes or excludes SNMP filters.

Timeout (1-300) — The amount of time (seconds) the device waits before resending informs. The default is 15 seconds.

Retries (1-255) — The amount of times the device resends an inform request. The default is 3.

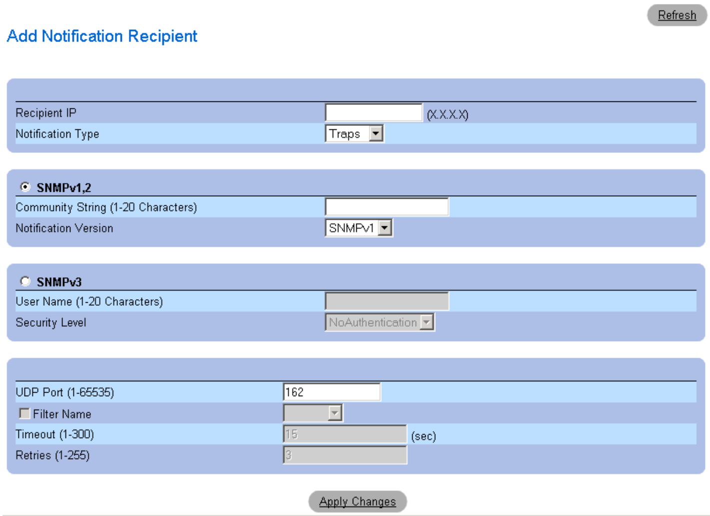
Remove Notification Recipient — When checked, removes selected notification recipients.

Adding a new Trap Recipients

1. Open **Notification Recipients** page.
2. Click **Add.**

   The **Add Notification Recipients** page opens:

Figure 6-73. Add Notification Recipients



3 Define the relevant fields.

4 Click **Apply Changes**.

The notification recipient is added, and the device is updated.

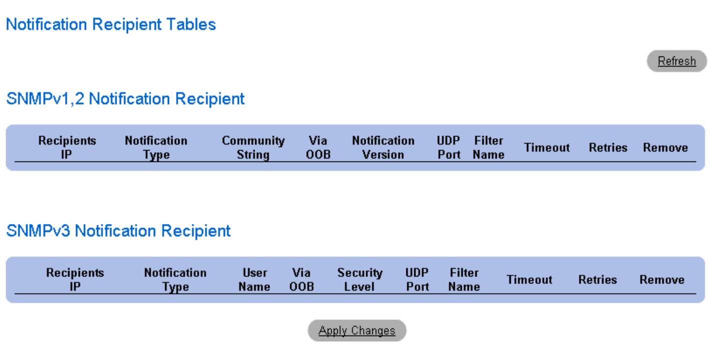
Displaying Notification Recipients Tables

1 Open **Notification Recipients** page.

2 Click **Show All**.

The **Notification Recipients Tables** page opens:

Figure 6-74. Notification Recipients Tables



Deleting Notification Recipients

1. Open **Notification Recipients** page.
2. Click **Show All**.

   The **Notification Recipients Tables** page opens.
3. Select a notification recipient in either the **SNMPV1,2 Notification Recipient** or **SNMPv3 Notification Recipient Tables**.
4. Check the **Remove** checkbox.
5. Click **Apply Changes**.

   The recipient is deleted, and the device is updated.

Configuring SNMP Notification Recipients Using CLI Commands

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

Table 6-54. SNMP Community CLI Commands

CLI Command	Description
snmp-server host {*ipaddress* | *hostname*} *community-string* [**traps** | **informs**] [**1** | **2**] [**udp-port** *port*] [**filter** *filtername*] [**timeout** *seconds*] [**retries** *retries*]	Creates or updates a notification recipient receiving notifications in SNMP version 1 or 2.
snmp-server v3-host {ip-*address* | *hostname*} *username* [**traps** | **informs**] {**noauth** | **auth** | **priv**} [**udp-port** *port*] [**filter** *filtername*] [**timeout** *seconds*] [**retries** *retries*]	Creates or updates a notification recipient receiving notifications in SNMP version 3.
show snmp	Shows the current SNMP configuration

The following is an example of the CLI commands:

```
console(config)# snmp-server host 172.16.1.1 private
console(config)# end
console# show snmp
Community-String  Community-Access  View name     IP address
----------------  ----------------  ---------     ----------
public            read only         user-view     All
private           read write        default       172.16.1.1
private           su                DefaultSuper  172.17.1.1
```

Managing Files

Use the **File Management** page to manage device software, the image file, and the configuration files. Files can be downloaded or uploaded via a TFTP server.

Management File Overview

The management file structure consists of the following files:

- **Startup Configuration File** — Contains the commands required to configure device at startup or after reboot. The startup configuration file is created by copying the configuration commands from the Running Configuration file or the Backup Configuration file to the Startup Configuration file.
- **Running Configuration File** — Contains all Startup Configuration 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 Configuration file are copied to the Running Configuration file and applied to the device. During the session, all new commands are added to the commands existing in the Running Configuration file. To update the Startup Configuration file, before powering down the device, the Running Configuration file must be copied to the Startup Configuration file.
- **Backup Configuration File** — Contains a backup copy of the device configuration. Up to five backup configuration files can be saved on the device, with user configured names. These files are generated when the user copies the Running Configuration file or the Startup Configuration file to a user-named file. The contents of the backup configuration files can be copied to either the Running Configuration or the Startup Configuration files.

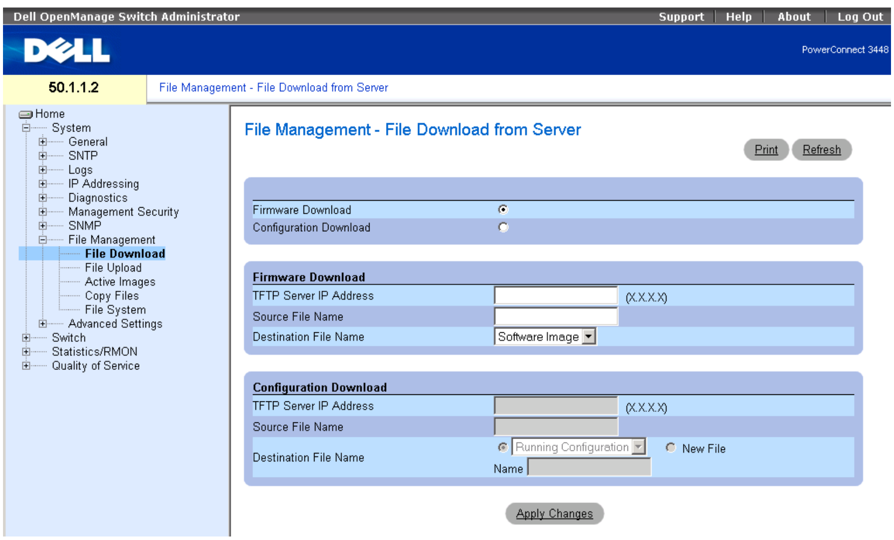
- **Image Files** — System file images are saved in two Flash Files called Image 1 and Image 2. The active image stores the active copy, while the other image stores a second copy. The device boots and runs from the active image. If the active image is corrupted, the system automatically boots from the 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.

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 6-75. File Download from Server



The **File Download from Server** page contains the following fields:

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 the firmware files are downloaded.
>
> **Source File Name** — Indicates the file to be downloaded.

Destination File Name — The destination file type to which the file is downloaded. The possible field values are:

Software Image — Downloads the Image file.

Boot Code — Downloads the Boot file.

Configuration Download

TFTP Server IP Address — The TFTP Server IP Address from which the configuration files are downloaded.

Source File Name — Indicates the configuration files to be downloaded.

Destination File Name— The destination file to which 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.

User Defined Backup Configuration — Downloads the user-defined Backup Configuration file, and overwrites it.

New **File Name** — Downloads a new backup configuration file can be specified as the destination file.

NOTE: The image file overwrites the non-active image. It is recommended to designate that the non-active image will become the active image after reset, and then to reset the device following the download.

During the Image file download a dialog box opens which displays the download progress. The window closes automatically when the download is complete.

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 **Switching Between Stack Masters**.

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 6-55. File Download CLI Commands

CLI Command	Description
copy *source-url destination-url*	Copies any file from a source to a destination.

The following is an example of the CLI commands:

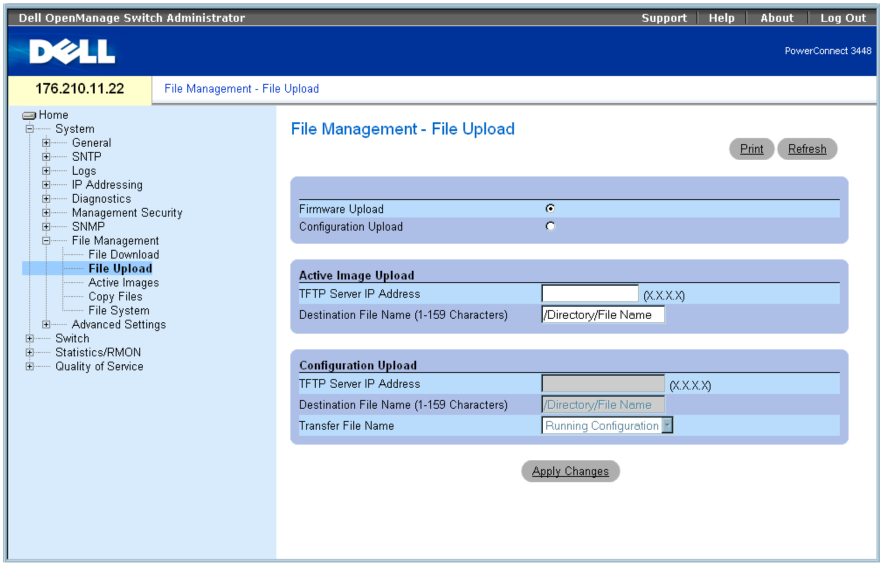
```
console# copy tftp://10.6.6.64/pp.txt startup-config

....!

Copy: 575 bytes copied in 00:00:06 [hh:mm:ss]

01-Jan-2000 06:41:55 %COPY-W-TRAP: The copy operation was
completed successfully
```

NOTE: Each exclamation mark (!) indicates that ten packets were successfully transferred.

Uploading Files

The **File Upload to Server** page contains fields for uploading the software to the TFTP server from 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 6-76. File Upload to Server



The **File Upload to Server** page contains the following fields:

Firmware Upload — The Firmware file is uploaded. If **Firmware Upload** is selected, the **Configuration Upload** fields become unavailable.

Configuration Upload — The Configuration file is uploaded. If **Configuration Upload** is selected, the **Active Image Upload** fields become unavailable.

Active Image Upload

> **TFTP Server IP Address** — The TFTP Server IP Address to which the Software Image is uploaded.
>
> **Destination File Name (1-159 Characters)** — Indicates 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.
>
> **Destination File Name (1-159 Characters)** — Indicates the Configuration file path to which the file is uploaded.
>
> **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.
> >
> > **List of User Defined Configuration Files** — Uploads a user-defined configuration file.

NOTE: This list of user-defined configuration files only appears if the user had created backup configuration files. For example, if the user copied the running configuration file to a user-defined configuration file called BACKUP-SITE-1, this list appears on the **File Upload to Server** page and the BACKUP-SITE-1 configuration file appears in the list.

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 TFTP server.

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 6-56. File Upload CLI Commands

CLI Command	Description
copy *source-url destination-url*	Copies any file from a source to a destination.

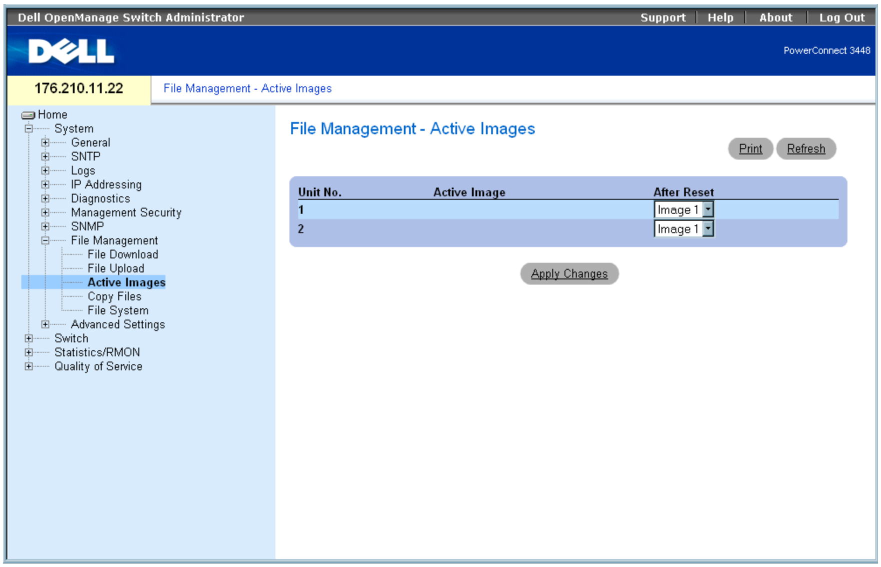
The following is an example of the CLI commands:

```
console# copy image tftp://10.6.6.64/uploaded.ros
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Copy: 4234656 bytes copied in 00:00:33 [hh:mm:ss]
01-Jan-2000 07:30:42 %COPY-W-TRAP: The copy operation was
completed successfully
```

Activating Image Files

The **Active Images** page allows network managers to select and reset the Image files. The Active Image file for each unit in a stacking configuration can be individually selected. To open the **Active Images** page, click **System →File Management →Active Images** in the tree view.

Figure 6-77. Active Images



The **Active Images** page contains the following fields:

Unit No. — The unit number for which the Image file is selected.

Active Image — The Image file which is currently active on the unit.

After Reset — The Image file which is active on the unit after the device is reset. The possible field values are:

> **Image 1** — Activates Image file 1 after the device is reset.
>
> **Image 2** — Activates Image file 2 after the device is reset.

Selecting an Image File

1. Open the **Active Images** page.
2. Select an Image file for a specific unit in the **After Reset** field.
3. Click **Apply Changes**.

   The Image file is selected. The Image file reloads only after the next reset. The currently selected Image file continue to run until the next device reset.

Working with the Active Image File Using CLI Commands

The following table summarizes the equivalent CLI commands for viewing fields displayed in the **Active Images**.

Table 6-57. File Upload CLI Commands

CLI Command	Description
boot system [**unit** | *unit*] {**image-1** | **image-2**}	Indicates the system image that the device loads at startup.
show version [**unit** *unit*]	Displays version information for the system

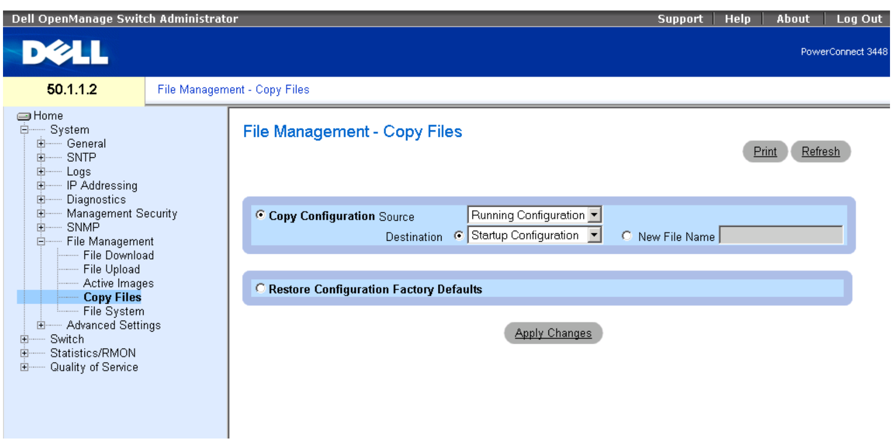
The following is an example of the CLI commands:

```
Console# boot system image-1
```

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



The **Copy Files** page contains the following fields:

Copy Configuration — When selected, copies either the running, startup or backup configuration file of the Master file to the destination file.

> **Source** — Indicates the type of file to be copied to the destination file. Select either the Running Configuration, Startup Configuration or one of the user-defined Backup Configuration files.

Destination — Indicates the destination configuration file to which the source file is copied. Files cannot be copied to the Backup Master's backup file. Backup files appear in the **Destination Unit** field only if backup files have been defined. Select the **New File Name** checkbox and indicate the name of the new file to copy the source file to a new backup configuration file.

New File Name — Indicates the name of the newly created backup configuration file.

Restore Configuration Factory Defaults — When selected, indicates that the current configuration settings should be replaced by the factory configuration default settings. When clear, indicates that the current configuration settings should be maintained.

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 Configuration 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 6-58. Copy Files CLI Commands

CLI Command	Description
copy *source-url destination-url*	Copies any file from a source to a destination.
delete startup-config	Deletes the startup-config file.

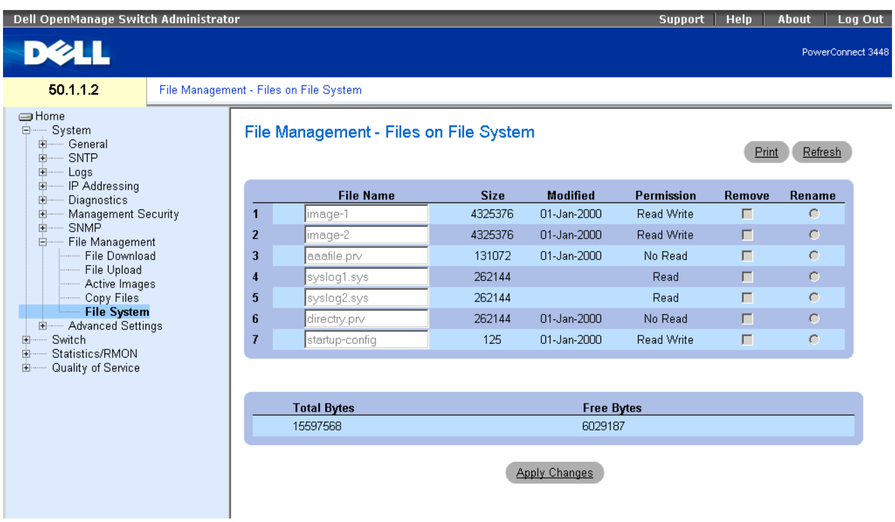
The following is an example of the CLI commands:

```
console# delete startup-config
Startup file was deleted
console#
console# copy running-config startup-config
01-Jan-2000 06:55:32 %COPY-W-TRAP: The copy operation was
completed successfully
Copy succeeded
console#
```

Managing Device Files

The **Files on File System** page provides information about files currently stored on the system, including file names, file sizes, files modifications, and file permissions. The files system permits managing up to five files and a total file size of 3MB. To open the **Files on File System** page, click **System→File Management→File System** in the tree view.

Figure 6-79. Files on File System



The **Files on File System** page contains the following fields:

File Name — Indicates the file currently stored in the file management system.

Size — Indicates the file size.

Modified — Indicates the date the file was last modified.

Permission — Indicates the permission type assigned to the file. The possible field values are:

Read Only — Indicates a read-only file.

Read Write — Indicates a read-write file.

Remove — Deletes the file, when checked.

Rename — Permits renaming the file. The file name is renamed in the **File Name** field.

Total Bytes — Indicates the total amount of the space currently used.

Free Bytes — Indicates the remaining amount of the space currently free.

Managing Files Using CLI Commands

The following table summarizes the equivalent CLI commands for managing system files.

Table 6-59. Copy Files CLI Commands

CLI Command	Description
dir	Display list of files on a flash file system

The following is an example of the CLI commands:

```
console# dir
Directory of flash:

File Name         Permis-   Flash     Data      Modified
                  sion      Size      Size
--------------    ------    ------    ------    --------------------
3.txt             rw        524288    523776    22-Feb-2005 18:49:27
setup             rw        524288    95        22-Feb-2005 15:58:19
setup2            rw        524288    95        22-Feb-2005 15:58:35
image-1           rw        4325376   4325376   06-Feb-2005 17:55:32
image-2           rw        4325376   4325376   06-Feb-2005 17:55:31
test.txt          rw        524288    95        22-Feb-2005 12:16:44
aaafile.prv       --        131072    --        06-Feb-2005 19:09:02
```

```
syslog1.sys      r-       262144   --       22-Feb-2005 18:49:27
syslog2.sys      r-       262144   --       22-Feb-2005 18:49:27
directory.prv    --       262144   --       06-Feb-2005 17:55:31
startup-config   rw       524288   347      22-Feb-2005 11:56:03

Total size of flash: 16646144 bytes
Free size of flash: 4456448 bytes
```

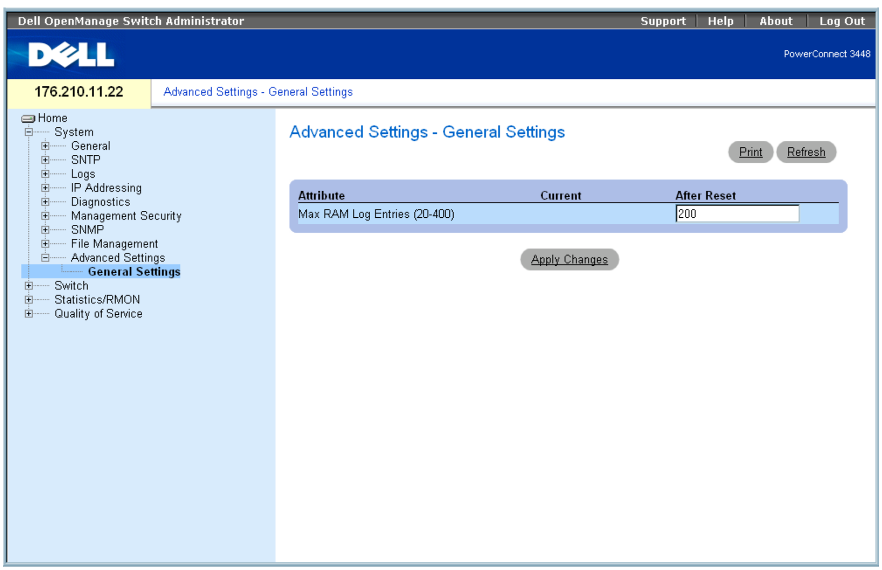
Configuring General Settings

Use Advanced Settings to set miscellaneous global attributes of the switch. The changes to these attributes are applied only after the switch is reset. Click **System→Advanced Settings** in the tree view to open the **Advanced Settings** page.

The the **Advanced Settings** page contains a link for configuring general settings.

The **General Settings** page provides information for defining general device parameters. To open the **General Settings** page, click **System→Advanced Settings→General Settings** in the tree view.

Figure 6-80. General Settings



The **General Settings** page contains the following information:

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.

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 6-60. General Settings CLI Commands

CLI Command	Description
logging buffered size *number*	Sets the number of syslog messages stored in the internal buffer (RAM).

The following is an example of the CLI commands:

```
console(config)# logging buffered size 300
```

7

Configuring Switch 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

Use the **Network Security** page to set network security through both access control lists and locked ports. To open the **Network Security** page, select **Switch →Network Security**.

Port Based Authentication

Port based authentication enables authenticating system users on a per-port basis via an external server. Only authenticated and approved system users can transmit and receive data. Ports are authenticated via the RADIUS server using the Extensible Authentication Protocol (EAP). Port Authentication includes:

- **Authenticators** — Specifies the device port which 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 supplicant is authorized to access system services.

Port based authentication creates two access states:

- **Controlled Access** — Permits communication between the supplicant and the system, if the supplicant 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.
- 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.

- Enables user based authentication. Specific VLANs in the device are always available, even if specific ports attached to the VLAN are unauthorized.
  - For example, Voice over IP does not require authentication, while data traffic requires authentication. VLANs for which authorization is not required can be defined. Unauthenticated VLANs are available to users, even if the ports attached to the VLAN are defined as authorized.

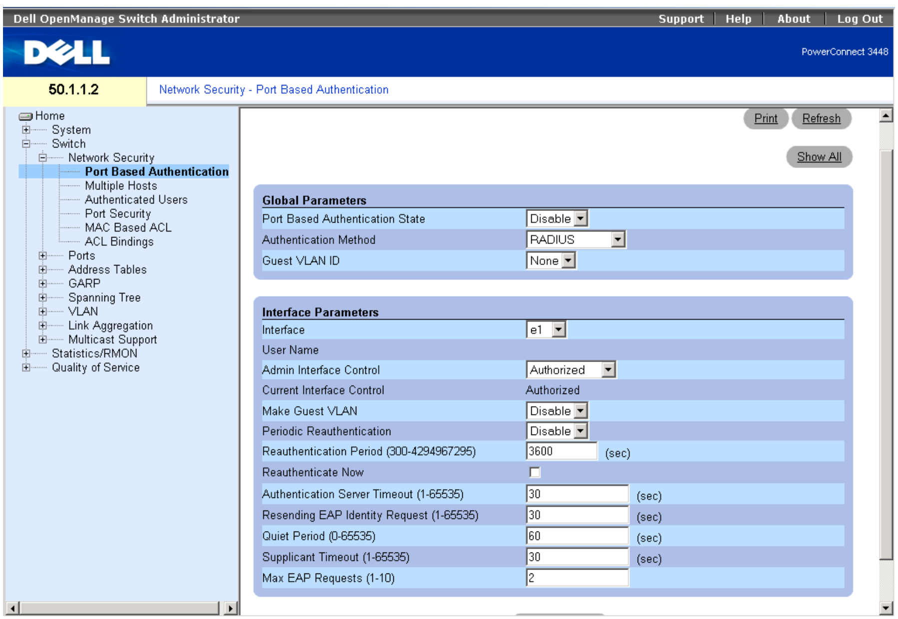
Advanced Port Based Authentication is implemented in the following modes:

- **Single Host Mode** — Only the authorized host can access the port.
- **Multiple Host Mode** — Multiple hosts can be attached to a single port. Only one host must be authorized for all hosts to access the network. If the host authentication fails, or an EAPOL-logoff message is received, all attached clients are denied access to the network.
- **Guest VLANs** — Provides limited network access authorized to ports. If a port is denied network access via port based authorization, but the Guest VLAN is enabled, the port receives limited network access. For example, a network administrator can use Guest VLANs to deny network access via port based authentication, but grant Internet access to unauthorized users.

Configuring Port Based Authentication

The **Port Based Authentication** page allows network managers to configure port based authentication. To open the **Port Based Authentication** page, click **Switch →Network Security → Port Based Authentication.**

Figure 7-1. Port Based Authentication



The **Port Based Authentication** page contains the following fields:

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 — Indicates the Authentication method used. The possible field values are:

> **None** — Indicates that no authentication method is used to authenticate the port.
>
> **RADIUS** — Indicates that port authentication is performed via RADIUS server.
>
> **RADIUS, None** — Indicates that port authentication is performed first via the RADIUS server. If the port is not authenticated, then no authentication method is used, and the session is permitted.

Guest VLAN — Enables using a guest VLAN for unauthorized ports. If a Guest VLAN is enabled, the unauthorized port automatically joins the VLAN selected in **VLAN List** field. The field default is disabled.

Interface — Contains an interface list for which port based authentication is enabled.

User Name — Indicates the supplicant user-name.

Admin Interface Control — Defines the port authorization state. The possible field values are:

> **Auto** — Enables port based authentication on the device. The interface moves between an authorized or unauthorized state based on the authentication exchange between the device and the client.
>
> **Authorized** — Places the interface into an authorized state without being authenticated. The interface resends and receives normal traffic without client port based authentication.
>
> **Unauthorized** — Denies the selected interface system access by moving the interface into unauthorized state. The device cannot provide authentication services to the client through the interface.

Current Interface Control — The current port authorization state.

Make Guest VLAN — If enabled, indicates that unauthorized users connected to this interface can access the Guest VLAN.

Periodic Reauthentication — Permits immediate port reauthentication.

Reauthentication Period (300-4294967295) — Indicate the time span in which the selected port is reauthenticated. The field value is seconds. The field default is 3600 seconds.

Reauthenticate Now — Permits immediate port reauthentication, when checked.

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 specified 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) — Indicates 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) — Indicates the amount of time that lapses before EAP requests are resent to the supplicant. The field value is in seconds. The field default is 30 seconds.

Max EAP Requests (1-10) — Indicates that 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.

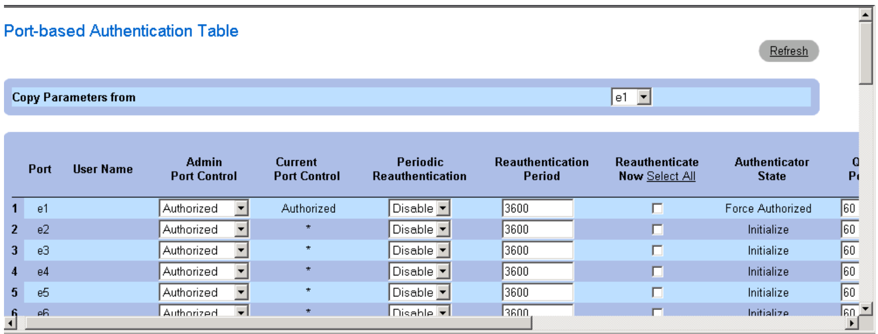
Displaying the Port Based Authentication Table

1 Open the **Port Based Authentication** page.

2 Click **Show All**.

The **Port Based Authentication Table** opens:

Figure 7-2. Port Based Authentication Table



In addition to the fields in the **Port Based Authentication Table** also displays the following fields:

Unit No. — Selects a stacking member.

Copy Parameters from Port No. — Copies parameters a the selected port.

Copying parameters in the Port Based Authentication Table

1 Open the page.

2 Click **Show All**.

The **Port Based Authentication Table** opens.

3 Select the interface in the **Copy Parameters from Port No.** field.

4 Select an interface in the **Port Based Authentication Table**.

5 Check the **Copy to** check box to define the interfaces to which the Port based authentication parameters are copied.

6 Click **Apply Changes**.

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** table.

Table 7-61. 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.
dot1x guest-vlan enable	Enables using a guest VLAN for unauthorized ports. If a Guest VLAN is enabled, the unauthorized port automatically joins the VLAN selected in **VLAN List** field. The field default is disabled.
dot1x guest-vlan	Contains a list of VLANs. The guest VLAN is selected from the **VLAN List**

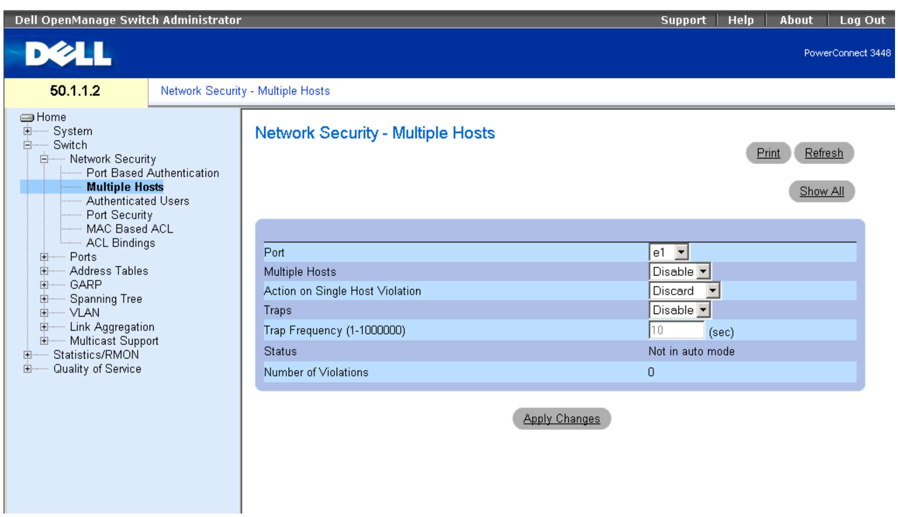
The following is an example of the CLI commands:

```
Console# show dot1x

Interface  Admin Mode  Oper Mode     Reauth    Reauth   Username
                                     Control   Period
---------  ----------  ----------    --------  ------   --------
1/e1       Auto        Authorized    Ena       3600     Bob
1/e2       Auto        Authorized    Ena       3600     John
1/e3       Auto        Unauthorized  Ena       3600     Clark
1/e4       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 and VLANs. For more information on Advanced Port Based Authentication, see **Advanced Port Based Authentication**. To open the **Multiple Hosts**, click **Switch →Network Security →Multiple Hosts**.

Figure 7-3. Multiple Hosts



The **Multiple Hosts** page contains the following fields:

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 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 shuts down the port. Ports remain shut down until they are activated, or the switch 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** — Indicates that the port control is *Force Unauthorized*, the port link is down or the port control is Auto, but a client has not been authenticated via the port.
>
> **Not in Auto Mode** — Indicates that the port control is *Forced Authorized*, and clients have full port access.
>
> **Single-host Lock** — Indicates that the port control is *Auto* and a single client has been authenticated via the port.
>
> **No Single Host** — Indicates that Multiple Host is enabled.

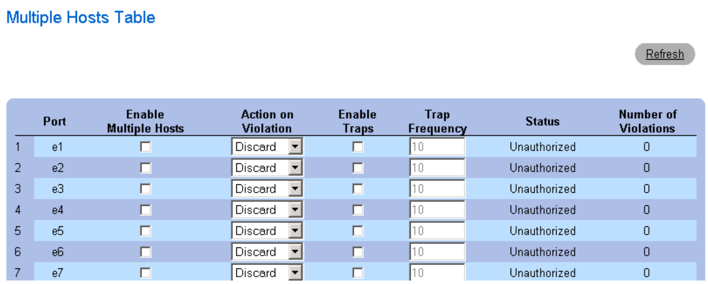
Number of Violations — The number of packets that arrived on the interface in single-host mode, from a host whose MAC address is not the client (supplicant) MAC address.

Displaying the Multiple Hosts Table

1. Open the **Multiple Hosts** page.
2. Click **Show All**.

   The **Multiple Hosts Table** opens.

Figure 7-4. Multiple Hosts Table



Multiple Hosts Table

Refresh

	Port	Enable Multiple Hosts	Action on Violation	Enable Traps	Trap Frequency	Status	Number of Violations
1	e1	☐	Discard	☐	10	Unauthorized	0
2	e2	☐	Discard	☐	10	Unauthorized	0
3	e3	☐	Discard	☐	10	Unauthorized	0
4	e4	☐	Discard	☐	10	Unauthorized	0
5	e5	☐	Discard	☐	10	Unauthorized	0
6	e6	☐	Discard	☐	10	Unauthorized	0
7	e7	☐	Discard	☐	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 7-62. 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-shutdown}[**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.

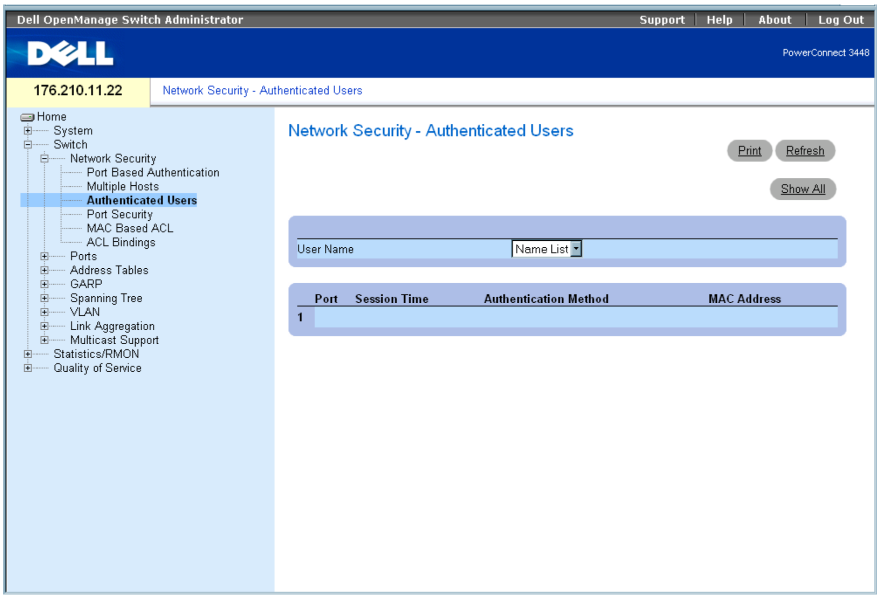
The following is an example of the CLI Command.

```
Console(config)# interface ethernet 1/e1
Console(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 7-5. Authenticated Users



The **Authenticated Users** page contains the following fields:

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.

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 supplicant MAC address.

Displaying the Authenticated Users Table

1 Open the **Authenticated Users** page.

2 Click **Show All**.

The **Authenticated Users Table** opens:

Figure 7-6. Authenticated Users Table

Authenticating Users Using the CLI Commands

The following table summarizes the equivalent CLI commands for authenticating users as displayed in the **Authenticated Users** page.

Table 7-63. 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

Port   Username Session Time Auth Method MAC Address

-----------------------------------------------------------------

1/e11 gili   00:09:27   Remote 00:80:c8:b9:dc:1d
```

Configuring Port Security

Network security can be enhanced 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 it 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 port is shut down

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.

NOTE: In order to enable port security, enable the **Multiple Hosts** feature on the required ports.

Disabled ports are activated from the **Port Security** page. The **Ports** page provides links for configuring port functionality including advanced features such as storm control and port mirroring, and for performing virtual port tests. To open the **Port Security** page, click **Switch→ Network Security→Port Security**.

Figure 7-7. Port Security

The **Port Security** page contains the following fields:

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.

Learning Mode — Defines the locked port type. The **Learning Mode** field is enabled only if **Locked** is selected in the **Set Port** field.The possible field values are:

> **Classic Lock** — Locks the port using the classic lock mechanism. The port is immediately locked, regardless of the number of addresses that have already been learned.
>
> **Limited Dynamic Lock** — Locks the port by deleting the current dynamic MAC addresses associated with the port. The port learns up to the maximum addresses allowed on the port. Both relearning and aging MAC addresses are enabled.

Max Entries — Specifies the number of MAC address that can be learned on the port. The **Max Entries field** is enabled only if **Locked** is selected in the **Set Port** field. In addition, the Limited Dynamic Lock mode is selected. The default is 1.

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 shuts down the port. Ports remained shut down until they are reactivated, 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. 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.

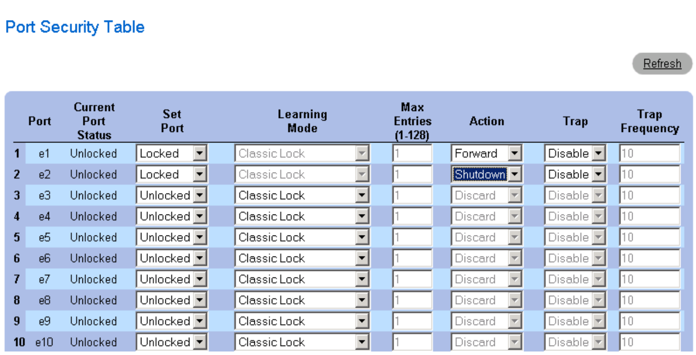
Displaying the Port Security Table

1. Open the **Port Security** page.
2. Click **Show All.**

   The **Port Security Table** opens:

   NOTE: Locked Ports are defined in the **Port Security Table.**

Figure 7-8. Port Security Table



Port Security Table

Refresh

	Port	Current Port Status	Set Port	Learning Mode	Max Entries (1-128)	Action	Trap	Trap Frequency
1	e1	Unlocked	Locked	Classic Lock	1	Forward	Disable	10
2	e2	Unlocked	Locked	Classic Lock	1	Shutdown	Disable	10
3	e3	Unlocked	Unlocked	Classic Lock	1	Discard	Disable	10
4	e4	Unlocked	Unlocked	Classic Lock	1	Discard	Disable	10
5	e5	Unlocked	Unlocked	Classic Lock	1	Discard	Disable	10
6	e6	Unlocked	Unlocked	Classic Lock	1	Discard	Disable	10
7	e7	Unlocked	Unlocked	Classic Lock	1	Discard	Disable	10
8	e8	Unlocked	Unlocked	Classic Lock	1	Discard	Disable	10
9	e9	Unlocked	Unlocked	Classic Lock	1	Discard	Disable	10
10	e10	Unlocked	Unlocked	Classic Lock	1	Discard	Disable	10

The **Port Security Table** contains the additional following fields:

Unit No. — Specifies the stacking unit for which locked port information is displayed.

Copy Parameters from — Copies parameters to the selected unit number.

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 7-64. 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 learning {disabled | dynamic}	Defines the locked port type.
port security max *max-addr*	Specifies the number of MAC address that can be learned on the port.
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
-----  -------     -------      -------   ---------  --------
1/e1   locked      Discard      Enable    100        88
1/e2   locked      Discard,     Disable
                   Shutdown
1/e3   Unlocked    -            -         -          -
```

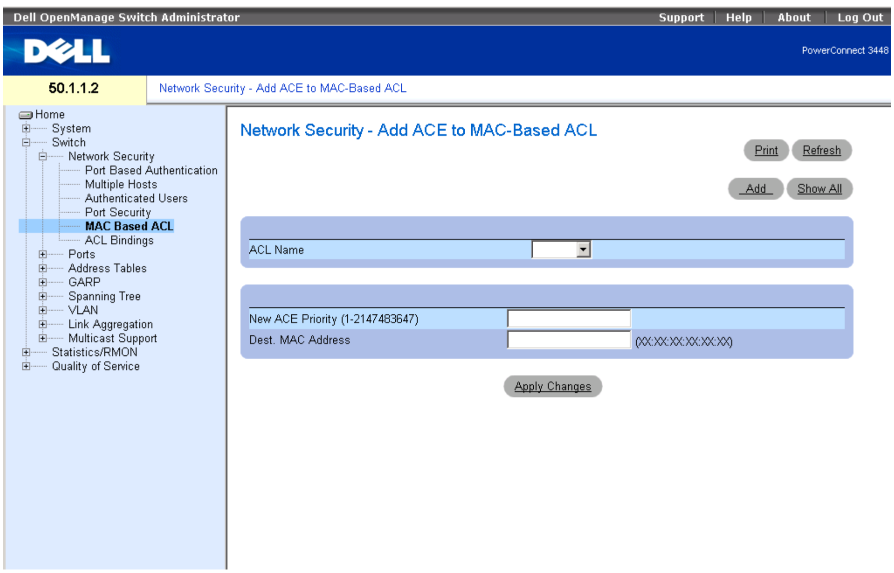
Defining MAC Based ACLs

Access Control Lists (ACL) allow network managers to define classification actions and rules for specific ingress ports. ACLs contain multiple classification rules and actions. Each classification rule and action are called *Access Control Element* (ACE). ACEs are the filters that determine traffic classifications. MAC based ACLs are applied to any packet, including non IP. Classification fields are based on L2 fields only.

The **MAC Based ACL** page allows a MAC- based ACL to be defined. For an explanation of ACLs, see "Defining MAC Based ACLs."

To open the **MAC Based ACL** page, select **Switch→Network Security→MAC based ACL**.

Figure 7-9. MAC Based ACL



The **MAC Based ACL** page contains the following fields:

ACL Name — User-defined ACL.

New ACE Priority (1-2147483647) — Index of the ACE rule in the ACL field.

Destination MAC Address — Matches the destination MAC address to which packets are addressed to the ACE.

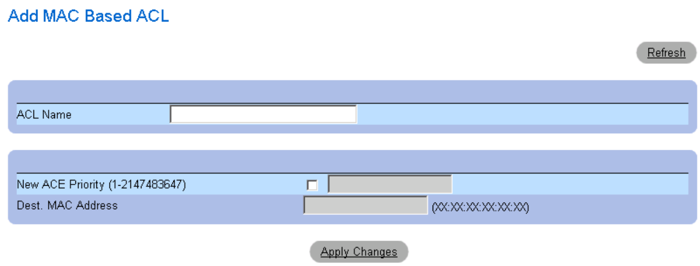
Adding a MAC-Based ACL:

1 Open the **MAC Based ACL** page.

2 Click **Add**.

The **Add MAC Based ACLs** page opens.

Figure 7-10. Add MAC Based ACLs



3 Define the fields.

4 Click **Apply Changes**.

The MAC-based ACL is defined, and the device is updated.

Displaying ACL-Specific ACEs

1 Open the **MAC Based ACL** page.

2 Select an ACL.

3 Click **Show All.**

The **ACEs Associated with MAC ACL** page opens.

Removing ACLs

1 Open the **MAC Based ACL** page.

NOTE: ACLs can be removed only if they are not bound to an interface.

2 Select an ACL.

3 Click **Show All**.

The **ACEs Associated with MAC ACL** page opens.

4 Check the **Remove ACL** checkbox.

Assigning MAC based ACEs to ACLs Using the CLI Commands

The following table summarizes the equivalent CLI commands for assigning MAC based ACEs to ACLs, as displayed in the **MAC Based ACL** page.

Table 7-65. MAC-Based ACE CLI Commands

CLI Command	Description
`mac access-list` ***`name`***	Creates Layer 2 MAC ACLs, and enters to MAC-Access list configuration mode.
`deny` *`destination`*	Denies traffic if the conditions defined in the MAC based ACL are matched.
`show access-lists` `[`*`name`*`]`	Displays Access Control Lists configured on the device.

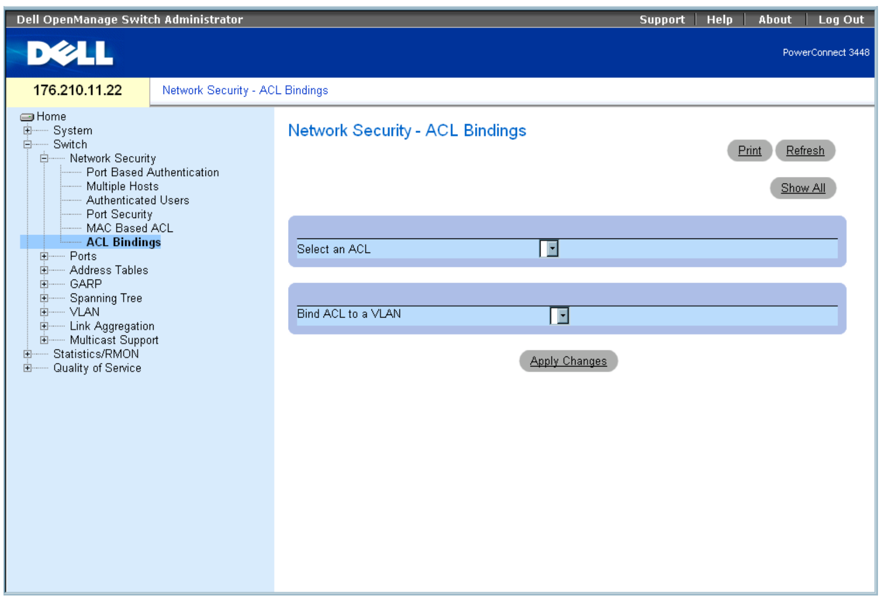
The following is an example of the CLI commands:

```
console (config)# mac access-list dell
console (config-mac-al)# deny 00-10-B5-F4-00-01
```

Configuring ACL Binding

When an ACL is bound to an interface, the ACL is applied to the selected interface. Use the **ACL Bindings** page to assign ACL Lists to classification methods and interfaces. To open the **ACL Bindings** page, select **Switch→Network Security→ACL Binding**.

Figure 7-11. ACL Bindings



The **ACL Bindings** page contains the following fields:

Select an ACL — The ACL type to which incoming packets are matched.

Bind ACL to VLAN — The VLAN to which the ACL is attached.

Assigning an ACL to an Interface

1. Open the **ACL Bindings** page.
2. Select the ACL type in the **Select an ACL** field.
3. Select the VLAN to which the ACL is attached in the **Bind ACL to an VLAN** field.
4. Click **Apply Changes**.

   The ACL is attached to the interface.

Removing an Entry from the ACL Bindings Table

1 Open the **ACL Bindings** page.

2 Click **Show All**.

The **ACL Bindings Table** opens.

3 Check the **Remove** check box for the entry that needs to be removed.

4 Click **Apply Changes**.

The selected entry is removed from the table, and the device is updated.

Displaying the ACL Bindings Table

1 Open the **ACL Bindings** page.

2 Click **Show All** to open the **ACL Bindings Table**.

The fields in the **ACL Bindings Table** are the same as the fields on the **ACL Bindings** page.

Copying Parameters in the ACL Bindings Table

1 Open the **ACL Bindings** page.

2 Click **Show All**.

The **ACL Bindings Table** opens.

3 Select an interface in the **Copy Parameters from** field.

4 Select a VLAN from the **VLAN** drop-down menu.

The definitions for this interface are copied to the selected target ports/trunks.

5 Check the **Copy to** check box for the entry to be edited, or to copy the definitions to all available ports/trunks.

6 Click **Select All**.

7 Click **Apply Changes**.

The parameters are copied to the target ports/trunks in the **ACL Bindings Table**, and the device is updated.

Assigning ACL Membership Using the CLI Commands

The following table summarizes the equivalent CLI commands for assigning ACL membership as displayed in the **ACL Binding** page.

Table 7-66. ACL Binding CLI Commands

CLI Command	Description
service-acl {**input** *acl-name*}	Applies an access-list to the interface input.

The following is an example of the CLI commands:

```
console(config)# interface vlan 123
console(config-if)# service-acl input dell
```

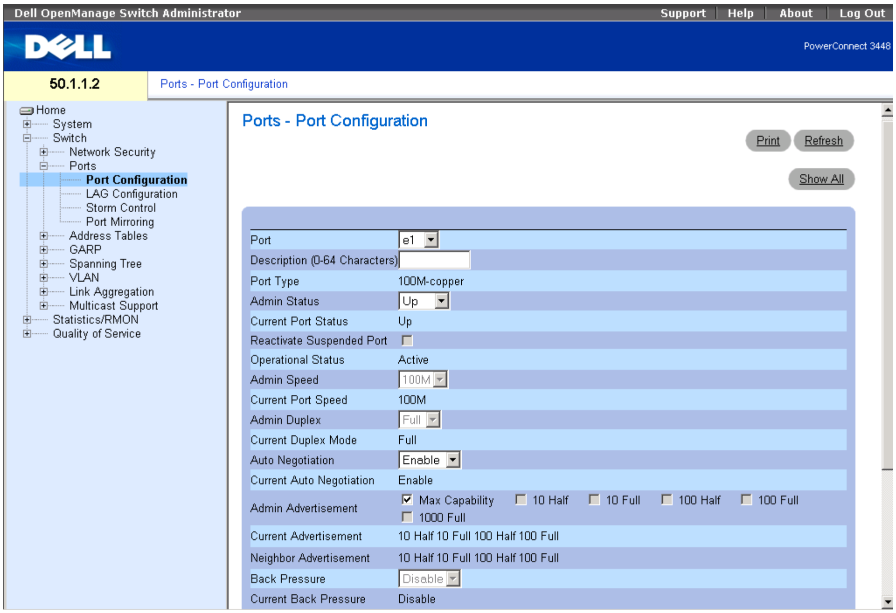
Configuring Ports

The **Ports** page provides links for configuring port functionality including advanced features such as storm control and port mirroring, and for performing virtual port tests. To open the **Ports** page Select **Switch→Ports**.

Defining Port Configuration

Use the **Port Configuration** page to define port parameters. 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. To open the **Port Configuration** page, click **Switch→Ports→Port Configuration** in the tree view.

Figure 7-12. Port Configuration



The **Port Configuration** page contains the following fields:

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.

Current Port Status — Specifies whether the port is currently operational or non-operational.

Reactivate Suspended Port — Reactivates a port if the port has been disabled through the locked port security option.

Operational Status — Indicates the port operational status. Possible field values are:

- **Suspended** — The port is currently active, and is not receiving or transmitting traffic.
- **Active** — The port is currently active and is receiving and transmitting traffic.
- **Disable** — The port is currently disabled, and is not 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 the port is disabled.

Current Port Speed — The actual synchronized port speed (bps).

Admin Duplex — The port duplex mode in bps. **Full** indicates that the interface supports transmission between the device and the client 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 synchronized 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 current Auto Negotiation setting.

Admin Advertisement — Defines the auto-negotiation setting the port advertises. The possible field values are:

Max Capability — Indicates that all port speeds and Duplex mode settings are accepted.

10 Half — Indicates that the port advertises for a 10 mbps speed port and half duplex mode setting.

10 Full — Indicates that the port advertises for a 10 mbps speed port and full duplex mode setting.

100 Half — Indicates that the port advertises for a 100 mbps speed port and half duplex mode setting.

100 Full — Indicates that the port advertises for a 100 mbps speed port and full duplex mode setting.

1000 Full — Indicates that the port advertises for a 1000 mbps speed port and full duplex mode setting.

Current Advertisement — The port advertises its speed to its neighbor port to start the negotiation process. The possible field values are those specified in the **Admin Advertisement** field.

Neighbor Advertisement — Indicates the neighboring port's advertisement settings. The field values are identical to the **Admin Advertisement** field values.

Back Pressure — Enables Back Pressure mode on the port. Back Pressure mode is used with Half Duplex mode to disable ports from receiving messages. Back Pressure is not supported in OOB ports.

Current Back Pressure — The current Back Pressure setting.

Flow Control — Enables or disables flow control or enables the auto negotiation of flow control on the port.

Current Flow Control — The current 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. Auto MDIX does not operate on FE ports if auto negotiation is disabled. The possible field values are:

Auto — Use to automatically detect the cable type.

MDIX — Use for hubs and switches.

MDI — Use for end stations.

Current MDI/MDIX — Indicates the current device MDIX settings. The possible field values are:

MDI — The current MDI setting is MDI.

MDIX — The current MDI setting is MDIX.

LAG — Specifies if the port is part of a LAG.

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.

Defining Port Parameters

1. Open the **Port Configuration** page.
2. Select a port in the **Port** Field.
3. Define the available fields in the dialog.
4. Click **Apply Changes**.

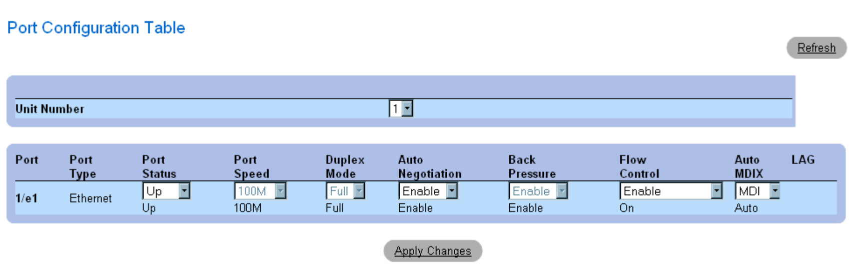
   The port parameters are saved to the device.

Displaying the Port Table

1. Open the **Port Configuration** page.
2. Click **Show All**.

   The **Port Configuration Table** opens.

Figure 7-13. Port Configuration Table



Configuring Ports with CLI Commands

The following table summarizes the equivalent CLI commands for configuring ports as displayed in the **Port Configuration** page.

Table 7-67. 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.
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 *Mbps*	Configures the speed of a given ethernet interface when not using auto negotiation.
duplex {**half** | **full**}	Configures the full/half duplex operation of a given ethernet interface when not using auto negotiation.
negotiation [capability1 [capability2…capability5]	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**}	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 interface advertise	Displays the interface's negotiation advertisement settings.
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 1/e3
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)# end
console# show interfaces configuration ethernet 1/e3

Port   Type   Duplex  Speed   Neg      Flow     Admin    Back      Mdix
                                       Control  State    Pressure  
                                                                   Mode
----   -----  ------  ------  ----     ------   -----    ------    ----
1/e3   100    Full    100     Enabled  On       Up       Enable    Auto

Console# show interfaces status
```

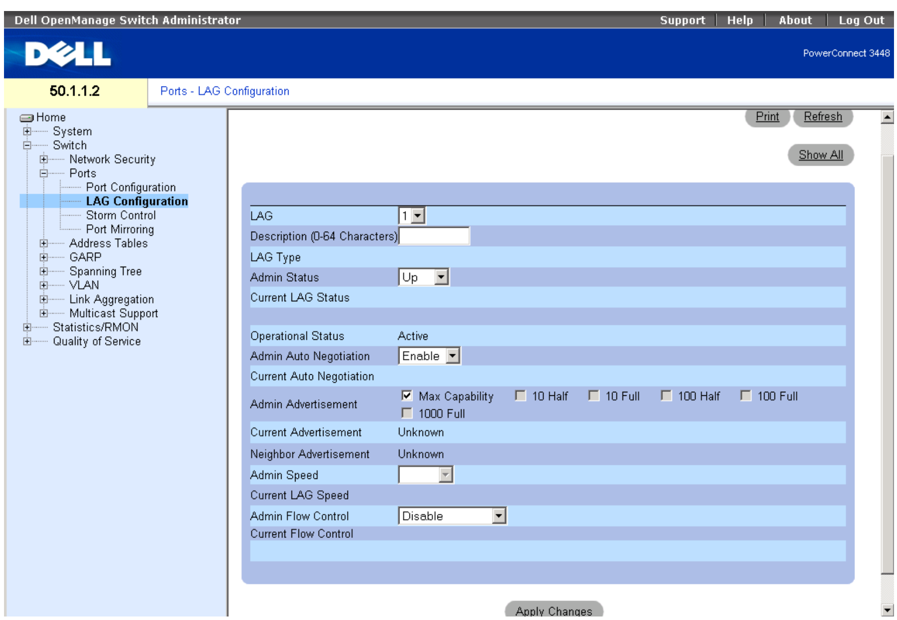
```
Port   Type   Duplex  Speed   Neg    Flow     Link    Back      Mdix
                                     Control  State   Pressure  Mode
----   -----  ------  ------  ----   ------   -----   ------    ----
1/e3   100    Full    100     Auto   On       Up      Enable    On
1/e4   100    Full    1000    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, see **Aggregating Ports**.

To open the **Port Configuration** page, click **Switch→Ports→LAG Configuration** in the tree view.

Figure 7-14. LAG Configuration



The **LAG Configuration** page contains the following fields:

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 the selected LAG.

Current LAG Status — Indicates if the LAG is currently operating.

Operational Status — Enables or disables traffic forwarding through the selected 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 Advertisement — Defines the auto-negotiation setting the LAG advertises. The possible field values are:

- **Max Capability** — Indicates that all LAG speeds and Duplex mode settings are accepted.
- **10 Half** — Indicates that the LAG advertises for a 10 mbps speed LAG and half duplex mode setting.
- **10 Full** — Indicates that the LAG advertises for a 10 mbps speed LAG and full duplex mode setting.
- **100 Half** — Indicates that the LAG advertises for a 100 mbps speed LAG and half duplex mode setting.
- **100 Full** — Indicates that the LAG advertises for a 100 mbps speed LAG and full duplex mode setting.
- **1000 Full** — Indicates that the LAG advertises for a 1000 mbps speed LAG and full duplex mode setting.

Current Advertisement — The LAG advertises its speed to its neighbor LAG to start the negotiation process. The possible field values are those specified in the **Admin Advertisement** field.

Neighbor Advertisement — Indicates the neighboring LAG advertisement settings. The field values are identical to the **Admin Advertisement** field values.

Admin Speed — The speed at which the LAG is operating.

Current LAG Speed — The current speed at which the LAG is operating.

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**.

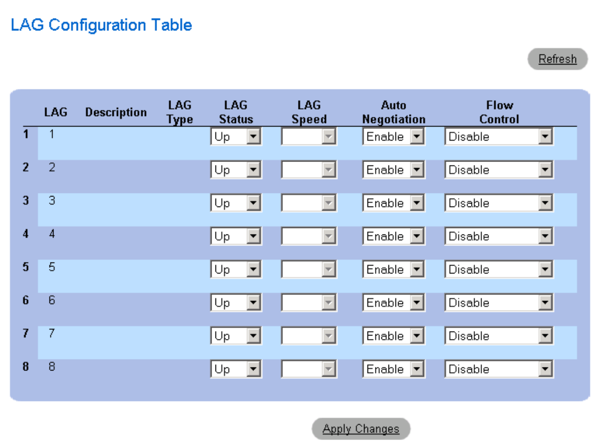
   The LAG parameters are saved to the device.

Displaying the LAG Configuration Table:

1. Open the **LAG Configuration** page.
2. Click **Show All.**

   The **LAG Configuration Table** opens:

Figure 7-15. LAG Configuration Table



Configuring LAGs with CLI Commands

The following table summarizes the equivalent CLI commands for configuring LAGs as displayed in the **LAG Configuration** page.

Table 7-68. 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.
negotiation [capability1 [capability2…capability5]	Enables interface speed auto negotiation operation.
back-pressure	Enables Back Pressure on a given interface.
flowcontrol {**auto** | **on** | **off** }	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)# interface port-channel 2
console(config-if)# no negotiation
console(config-if)# speed 100
console(config-if)# flowcontrol on
console(config-if)# exit
console(config)# interface port-channel 3
console(config-if)# shutdown
console(config-if)# exit
console(config)# interface port-channel 4
console(config-if)# back-pressure
console(config-if)# description p4
console(config-if)# end
console# show interfaces port-channel
Channel               Ports
---------             ---------
ch1                   Inactive: 1/e(11-13)
ch2                   Active: 1/e14
```

Enabling Storm Control

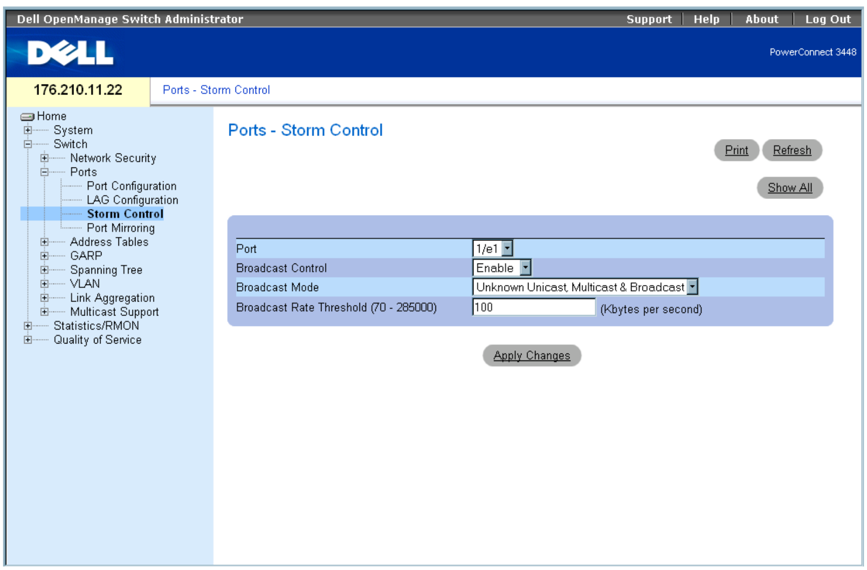
A Broadcast Storm is a result of an excessive amount of Broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses are heaped onto the network, straining network resources or causing the network to time out.

Storm Control is enabled per port by defining the packet type and the rate the packets are transmitted.

The system measures the incoming Broadcast, Unicast, 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 7-16. Storm Control



The **Storm Control** page contains the following fields:

Port — The port from which storm control is enabled.

Broadcast Control — Enables or disables forwarding Broadcast packet types on the specific interface.

Broadcast Mode — Specifies the Broadcast mode currently enabled on the device or stack. The possible field values are:

> **Unknown Unicast, Multicast & Broadcast** — Counts Unicast, Multicast, and Broadcast traffic.
>
> **Multicast & Broadcast** — Counts Broadcast and Multicast traffic together.
>
> **Broadcast Only** — Counts only Broadcast traffic.

Broadcast Rate Threshold (70-285000) — The maximum rate (kilobytes per second) at which unknown packets are forwarded. The field range is 70-285000 kilobytes per second.

Enabling Storm Control

1 Open the **Storm Control** page.

2 Select an interface on which to implement storm control.

3 Define the fields.

4 Click **Apply Changes**.

Storm Control is enabled.

Modifying Storm Control Port Parameters

1 Open the **Storm Control** page.

2 Modify the fields.

3 Click **Apply Changes**

The Storm Control port parameters are saved to the device.

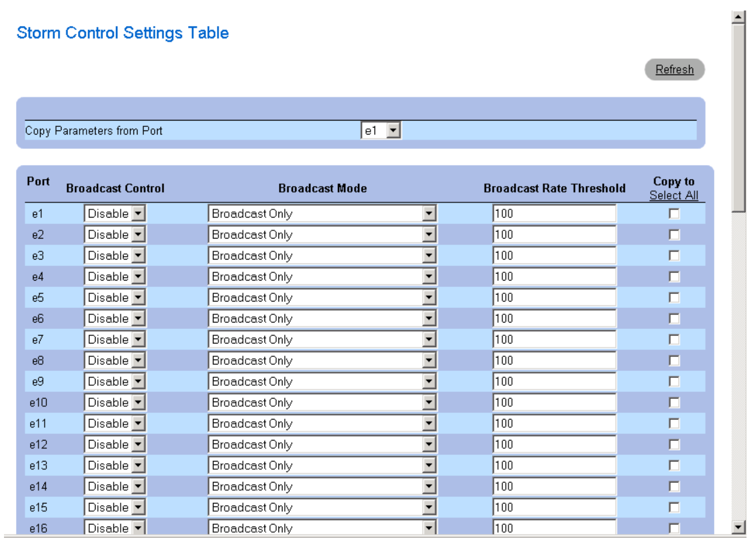
Displaying the Port Parameters Table

1 Open the **Storm Control** page.

2 Click **Show All.**

The **Storm Control Settings Table** opens:

Figure 7-17. Storm Control Settings Table



Port	Broadcast Control	Broadcast Mode	Broadcast Rate Threshold	Copy to Select All
e1	Disable	Broadcast Only	100	
e2	Disable	Broadcast Only	100	
e3	Disable	Broadcast Only	100	
e4	Disable	Broadcast Only	100	
e5	Disable	Broadcast Only	100	
e6	Disable	Broadcast Only	100	
e7	Disable	Broadcast Only	100	
e8	Disable	Broadcast Only	100	
e9	Disable	Broadcast Only	100	
e10	Disable	Broadcast Only	100	
e11	Disable	Broadcast Only	100	
e12	Disable	Broadcast Only	100	
e13	Disable	Broadcast Only	100	
e14	Disable	Broadcast Only	100	
e15	Disable	Broadcast Only	100	
e16	Disable	Broadcast Only	100	

In addition to the fields in the **Storm Control** page, the **Storm Control Settings Table** contains the following additional fields:

Copy Parameters from Port — Indicates the specific port from which storm control parameters are copied.

Copying Parameters in the Storm Control Settings Table

1. Open the **Storm Control** page.
2. Click **Show All**.

   The **Storm Control Settings Table** opens.

3. Select the port from which settings are copied from the **Copy Parameters from Port** field.
4. Check the **Copy to** check box to define the interfaces to which the storm control definitions are copied, or click **Select All** to copy the definitions to all ports.
5. Click **Apply Changes**.

   The parameters are copied to the selected ports in the **Storm Control Settings Table**, and the device is updated.

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 7-69. Storm Control CLI Commands

CLI Command	Description
port storm-control include-multicast	Enables the device to count Multicast, Unicast, and Broadcast packets together.
port storm-control broadcast enable	Enables broadcast storm control.
port storm-control broadcast rate	Configures the maximum broadcast rate.
show ports storm-control *port*	Displays the storm control configuration.

The following is an example of the CLI commands:

```
console(config)# port storm-control include-multicast
console(config)# interface ethernet 1/e1
console(config-if)# port storm-control broadcast enable
console(config-if)# port storm-control broadcast rate 100000
console(config-if)# end
console# show ports storm-control
Port                 Broadcast Storm control [kbyes/sec]
-----                -------------------------------------
1/e1                 8000
2/e1                 Disabled
3/e2                 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.
- Can be used as a diagnostic tool and/or a debugging feature.
- Enables device performance and monitoring.

Port mirroring is configured by selecting a specific port to copy all packets, and different ports from which the packets are copied.

Before configuring Port Mirroring, note the following:

- Port mirroring monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets, from a monitored port to a monitoring port.
- 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.

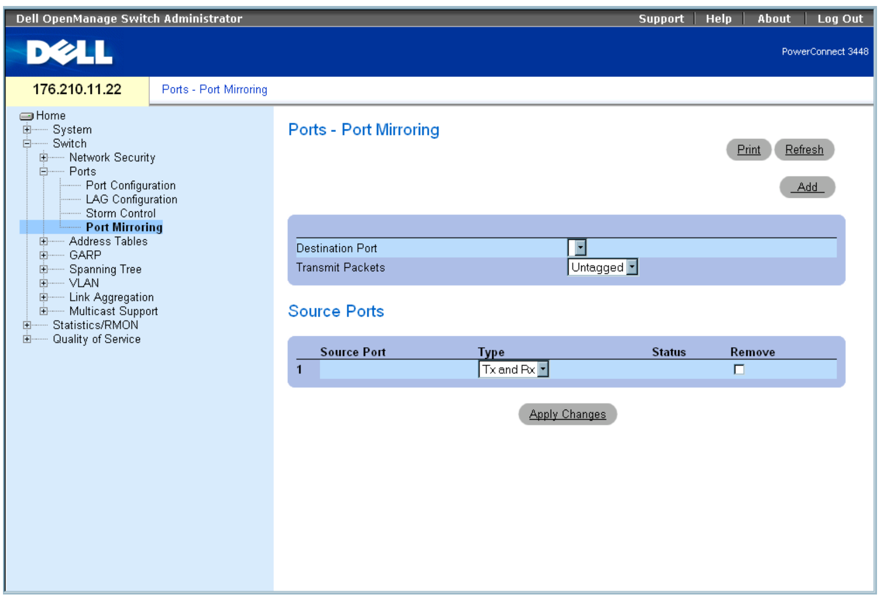
The following restrictions apply to ports configured to be source ports:

- Source Ports cannot be a LAG member.
- Ports cannot be configured as a destination port.
- Up to 8 source ports are supported.

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 7-18. Port Mirroring



The **Port Mirroring** page contains the following fields:

Destination Port — The port number to which port traffic is copied.

Transmit Packets — Defines the how the packets are mirrored. The possible field values are:

Untagged — Mirrors packets as untagged vlan packets. This is the default value.

Tagged — Mirrors packets as tagged vlan packets.

Type — Indicates if the mirrored packets are 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 Define the **Source Port** and the **Type** fields.
4 Click **Apply Changes**.
5 Select the destination port from the **Destination Port** drop-down menu.
6 Click the **Refresh** button **Port Mirroring** page.
7 Define the **Tagged Packets** field.
8 Define the **Type** field.
9 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 7-70. 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 1/e1
console(config-if)# port monitor 1/e2
console (config-if)# end
console# show ports monitor

Source Port   Destination Port    Type            Status      VLAN Tagging
-----------   ----------------    ------------    -------     ------------
1/e2          1/e1                RX, TX          Active      No
```

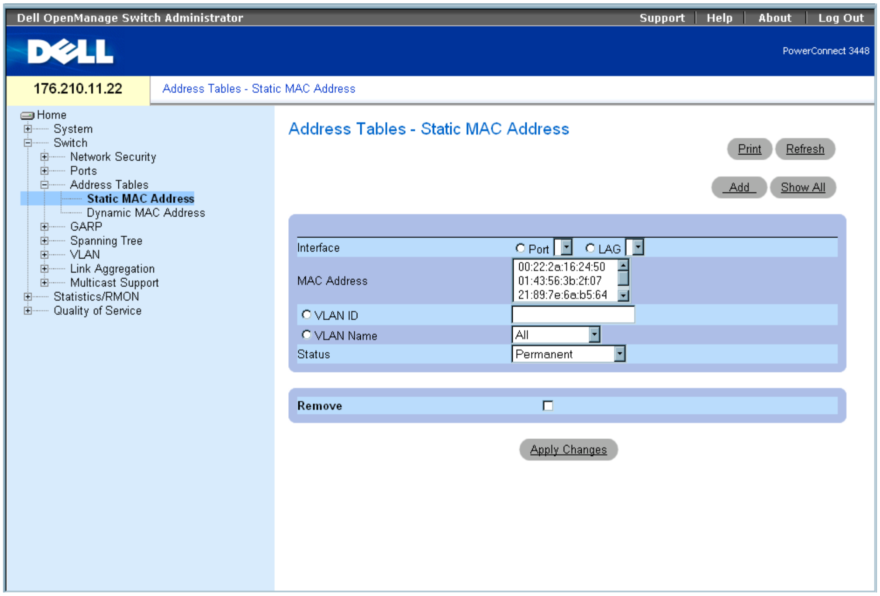
Configuring Address Tables

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 Dynamic Address Table can be sorted by interface, VLAN, and MAC Address. MAC addresses are dynamically learned as packets from sources arrive at the device. Addresses are associated with ports by learning the ports from the frames 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 Tables** in the tree view.

Defining Static Addresses

The **Static MAC Address Table** page contains a list of static MAC addresses. Static Address can be added and removed from the **Static MAC Address Table** page. In addition, several MAC Addresses can be defined for a single port. To open the **Static MAC Address Table** page, click **Switch →Address Tables →Static Address Table** in the tree view.

Figure 7-19. Static MAC Address Table



The **Static MAC Address Table** page contains the following fields:

Interface — The specific port or LAG to which the static MAC address is applied.

MAC Address — The MAC addresses listed in the current static addresses list.

VLAN ID — The VLAN ID attached to the MAC.

VLAN Name — User-defined VLAN name.

Status — MAC address status. Possible values are:

- **Secure** — Used for defining static MAC Addresses for Locked ports.
- **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.

NOTE: To prevent Static MAC addresses from being deleted when the Ethernet device reset, ensure the port attached to the MAC address is locked.

Remove — When selected, removes the selected MAC address from the MAC Address Table.

Adding a Static MAC Address

1. Open the **Static MAC Address Table** 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 Setting in the Static MAC Address Table

1. Open the **Static MAC Address Table** page.
2. Select an interface.
3. Modify the fields.
4. 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 Table** page.
2. Choose an interface.
3. Click **Show All**.

   The **Static MAC Address Table** opens.
4. Select a table entry.
5. Select the **Remove** check box.
6. 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 Table** page.

Table 7-71. Static Address CLI Commands

CLI Command	Description
bridge address *mac-address* [**permanent** | **delete-on-reset** | **delete-on-timeout** | **secure**] {**ethernet** *interface* | **port-channel** *port-channel-number*}	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.

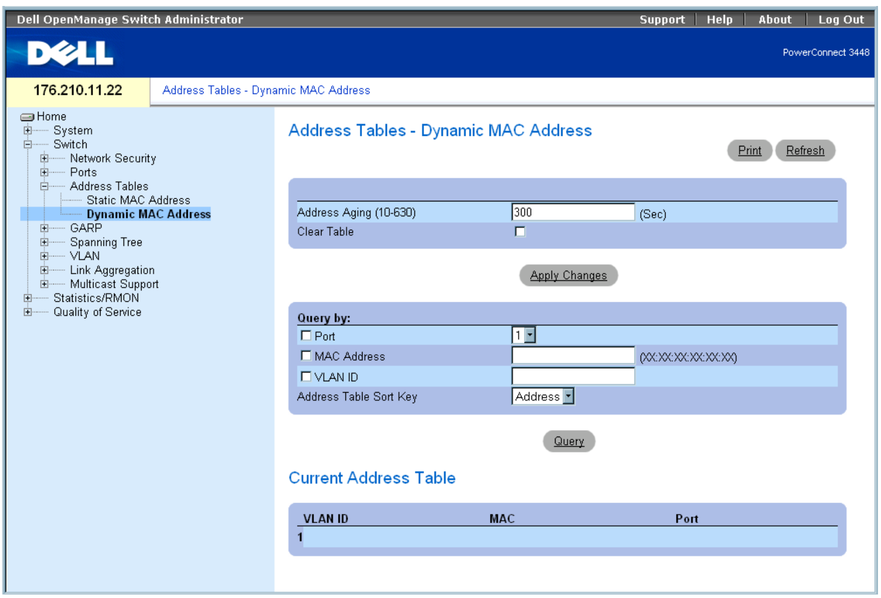
```
console(config-if)#bridge address 00:60:70:4C:73:FF permanent
ethernet g8

console# show bridge address-table

Aging time is 300 sec


vlan    mac address          port    type
----    ------------         ----    --------
1       00:60:70:4C:73:FF    1/e8    dynamic
1       00:60:70:8C:73:FF    1/e8    dynamic
200     00:10:0D:48:37:FF    1/e9    static
```

Viewing Dynamic Addresses

The **Dynamic MAC Address** contains information 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 MAC Address** page 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 MAC Address** page, click **Switch →Address Tables →Dynamic MAC Address** in the tree view.

Figure 7-20. Dynamic MAC Address



The **Dynamic MAC Address** page contain the following fields:

Address Aging (10-630) — Specifies the amount of time the MAC Address remains in the **Dynamic MAC Address** before it is timed out if no traffic from the source is detected. The default value is 300 seconds.

Clear Table — Clears the Dynamic Address table, when checked.

Port — Specifies the interface for which the table is queried. There are two interface types from which to select.

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. The address table can be sorted by address, VLAN or interface.

Redefining the Aging Time

1. Open the **Dynamic MAC Address**.
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 MAC Address**.
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 MAC Address** is queried.

Sorting the Dynamic Address Table

1. Open the **Dynamic MAC Address**.
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 MAC Address** is sorted.

Querying and Sorting Dynamic Addresses Using CLI Commands

The following table summarizes the equivalent CLI commands for aging, querying, and sorting dynamic addresses as displayed in the **Dynamic MAC Address**.

Table 7-72. 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)# end
console# show bridge address-table

Aging time is 250 sec

vlan      mac address         port     type
----      -----------         ----     ----
1         00:60:70:4C:73:FF   1/e8     dynamic
1         00:60:70:8C:73:FF   1/e8     dynamic
200       00:10:0D:48:37:FF   1/e8     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:

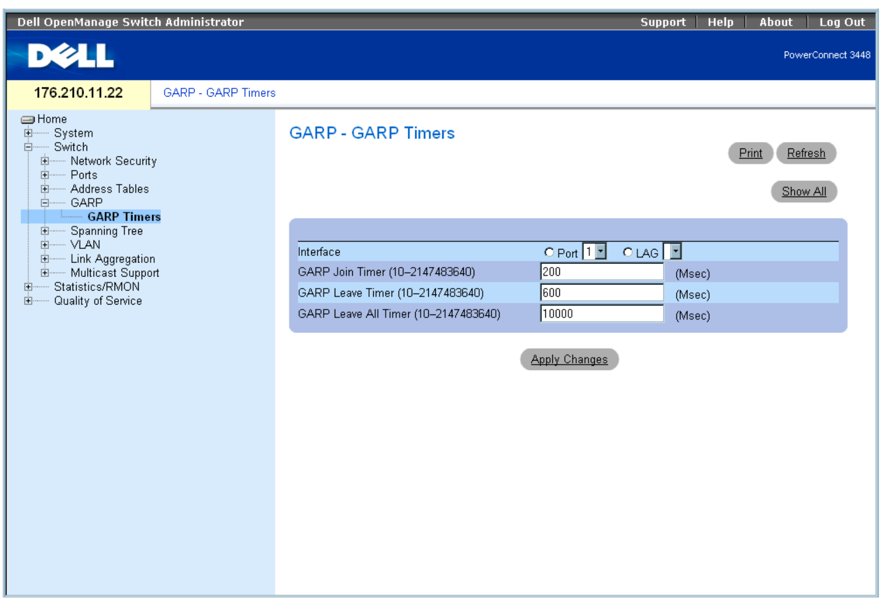
- The leave time must be greater than or equal to three times the join time.
- The leave-all time must be greater than the leave time.
- Set the same GARP timer values on all Layer 2-connected devices. If the GARP timers are set differently on the Layer 2-connected devices, GARP application does not 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 7-21. GARP Timers



The GARP Timers page contains the following fields:

Interface — To select a port or LAG for GARP Timers editing.

GARP Join Timer (10 - 2147483640) (Msec)— Time, in milliseconds, that PDUs are transmitted. The default value is 200 msec.

GARP Leave Timer (10 - 2147483640) (Msec)— 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 default value is 600 msec.

GARP Leave All Timer (10 - 2147483640) (Msec) — 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 default value is 10000 msec.

Defining GARP Timers

1 Open the **GARP Timers** page.

2 Select an interface.

3 Complete the fields.

4 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.

The definitions for this interface are copied to the selected interfaces. See step 6.

5 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.

6 Click **Apply Changes**.

The parameters are copied to the selected 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 7-73. 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 1/e1
console(config-if)# garp timer leave 900
console(config-if)# end
console# show gvrp configuration ethernet 1/e11

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
------- -------- ------------  ------------  -------  ------ ---------
1/e11   Disabled Normal        Enabled       200      900    10000
```

Configuring the Spanning Tree Protocol

Spanning Tree Protocol (STP) provides tree topography for any bridge arrangement. STP eliminates loops by providing one path between end stations on a network.

Loops occur when alternate routes exist between hosts. Loops in an extended network can cause bridges to forward traffic indefinitely, resulting in increased traffic and reducing network efficiency.

The device supports the following Spanning Tree versions:

- **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 convergence of the spanning tree, without creating forwarding loops. If RSTP is enabled on the device, but the neighboring device is STP enabled, the local device uses STP.

  For more information on configuring Rapid STP, see **Defining Rapid Spanning Tree**.
- **Multiple STP** — Provides full connectivity for packets allocated to any VLAN. Multiple STP is based on the RSTP. In addition, Multiple STP transmits packets assigned to different VLANs through different MST regions. MST regions act as a single bridge if MSTP is enabled on the device. However, if RSTP is enabled on the neighboring device and the local device uses STP, RSTP, and MSTP, then both the devices are interoperable.

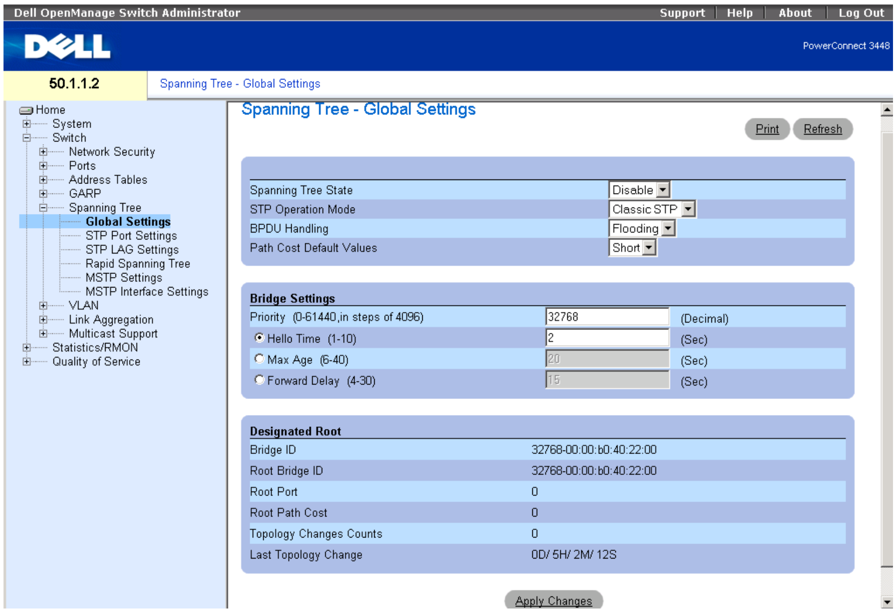
  For more information on configuring Multiple STP, see **Configuring Multiple Spanning Tree**.

To open the **Spanning Tree** page, click **Switch→Spanning Tree** in the tree view.

Defining STP Global Settings

The **Spanning Tree Global Settings** page contains parameters for enabling STP on the device. To open the **Spanning Tree Global Settings** page, click **Switch→Spanning Tree→Global Settings** in the tree view.

Figure 7-22. Spanning Tree Global Settings



The **Spanning Tree Global Settings** page contains the following fields:

Spanning Tree State — Enables or disables STP, Rapid STP, or MSTP on the device.

STP Operation Mode — Indicates 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.
>
> **Multiple STP** — Enables Multiple STP on the device.

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. This is the default value.
>
> **Flooding** — Floods BPDU packets when spanning tree is disabled on an interface.

Path Cost Default Values — Specifies the method used to assign default path costs to STP ports. The possible field values are:

Short — Specifies 1 through 65,535 range for port path costs. This is the default value.

Long — Specifies 1 through 200,000,000 range for port path costs.

The default path costs assigned to an interface vary according to the selected method:

Interface	Long	Short
LAG	20,000	4
1000 Mbps	20,000	4
100 Mbps	200,000	19
10 Mbps	2,000,000	100

Priority (0-65535) — Specifies the bridge priority value. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the device with the lowest priority value becomes the Root Bridge. The default value is 32768. The port priority value is provided in increments of 4096. For example, 4096, 8192, 12288, 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 10 seconds.

Bridge ID — Identifies the Bridge priority and MAC address.

Root Bridge ID — Identifies the Root Bridge priority and MAC address.

Root Port — Indicates 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.

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.

Last Topology Change — Indicates 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 D/H/M/S format, for example, 2D/5H/10M/4S.

Defining STP Global Parameters

1 Open the page.

2 Select **Enable** in the **Spanning Tree State** field.

3 Select the **STP** mode in the **STP Operation Mode** field, and define the bridge settings.

4 Click **Apply Changes**.

STP is enabled on the device.

Modifying STP Global Parameters

1 Open the 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 Spanning Tree Global Settings page.

Table 7-74. STP Global Parameter CLI Commands

CLI Command	Description
spanning-tree	Enables spanning tree functionality.
spanning-tree mode {**stp** | **rstp** | **mstp**}	Configures the mode of 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 devices.
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 7-74. STP Global Parameter CLI Commands *(continued)*

CLI Command	Description
show spanning-tree [**ethernet** *interface* | **port-channel** *port-channel-number*] [**instance** *instance-id*]	Displays spanning tree configuration.
show spanning-tree [**detail**] [**active** | **blockedports**] [**instance** *instance-id*]	Displays detailed spanning tree information on active or blocked ports.
show spanning-tree mst-configuration	Displays spanning tree MST configuration identifier.

The following is an example of the CLI commands:

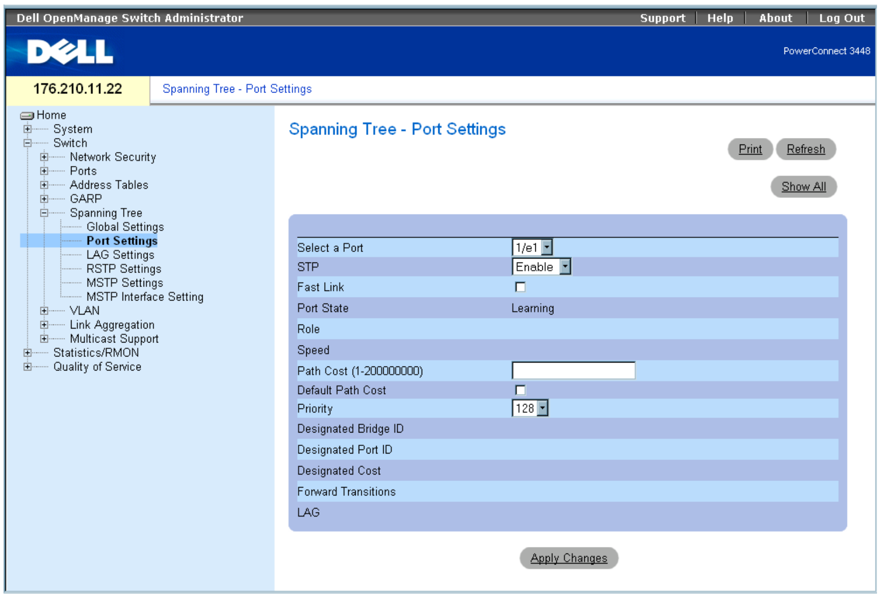
```
console(config)# spanning-tree
console(config)# spanning-tree mode rstp
console(config)# spanning-tree priority 12288
console(config)# spanning-tree hello-time 5
console(config)# spanning-tree max-age 12
console(config)# spanning-tree forward-time 25
console(config)# exit
console# show spanning-tree
Spanning tree enabled mode MSTP
Default port cost method: short

Gathering information ..........
###### MST 0 Vlans Mapped:  16-4094
 CST Root ID Priority 20480
      Address          00:30:ab:00:00:08
      Path Cost        4
      Root Port        ch2
      This switch is the IST master
      Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

 Bridge ID Priority              32768
      Address          00:00:00:16:00:64
      Max hops         20
 Name  State  Prio.Nbr Cost  Sts   Role  PortFast      Type
 ----  -----  -------  ----  ---   ----   -------      ----
 1/e2 enabled  128.2   100  DSBL  Dsbl     No        P2p Intr
 1/e3 enabled  128.3   100  DSBL  Dsbl     No        P2p Intr
 1/e4 enabled  128.4   100  DSBL  Dsbl     No        P2p Intr
 1/e5 enabled  128.5    19   FRW  Desg     Yes       P2p Intr
```

```
 1/e6  enabled  128.6   100  DSBL  Dsbl     No        P2p Intr
 1/e7  enabled  128.7   100  DSBL  Dsbl     No        P2p Intr
 1/e8  enabled  128.8   100  DSBL  Dsbl     No        P2p Intr
 1/e9  enabled  128.9   100  DSBL  Dsbl     No        P2p Intr
1/e10 enabled  128.10   100  DSBL  Dsbl     No        P2p Intr
1/e11 enabled  128.11    19  DSBL  Desg     Yes       P2p Intr

console# show spanning-tree active
Spanning tree enabled mode MSTP
Default port cost method: short
Gathering information ..........
###### MST 0 Vlans Mapped: 16-4094
 CST Root ID Priority 20480
      Address          00:30:ab:00:00:08
      Path Cost        4
      Root Port        ch2
      This switch is the IST master
      Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

 Bridge ID Priority           32768
      Address          00:00:00:16:00:64
      Max hops         20
 Name   State  Prio.Nbr Cost  Sts   Role  PortFast      Type
 ----   -----  -------- ----  ---   ----  -------       ----
 1/e5  enabled  128.2    19   FRW   Desg     Yes      P2p Intr
 1/e7  enabled  128.7    19   DSCR  Altn     No    P2p Bound (STP)
1/e11 enabled  128.11    19   FRW   Desg     Yes      P2p Intr
1/e15 enabled  128.15    19   FRW   Desg     No       P2p Intr
1/e22 enabled  128.22    19   FRW   Desg     Yes      P2p Intr
```

Defining STP Port Settings

Use the Spanning Tree Port Settings page to assign STP properties to individual ports. To open the Spanning Tree **Port Settings** page, click **Switch→Spanning Tree→Port Settings** in the tree view.

Figure 7-23. Spanning Tree Port Settings



The Spanning Tree Port Settings page contains the following fields:

Select a Port — Specifies the port number on which STP settings are to be to modified.

STP — Enables or disables STP on the port.

Fast Link — When checked, 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 — Indicates the current STP state of a port. If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are:

> **Disabled** — STP is currently disabled on the port. The port forwards traffic while learning MAC addresses.
>
> **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.

Role—Indicates the port role assigned by the STP algorithm that provides STP paths. The possible field values are:

Root—Provides the lowest cost path to forward packets to root switch.

Designated—Indicates that the port via which the designated switch is attached to the LAN.

Alternate—Provides an alternate path to the root switch 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 by a point-to-point link. Backup ports also occur when a LAN has two or more connections connected to a shared segment.

Disabled—Indicates the port is not participating in the Spanning Tree.

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. The default values for long path costs are:

Ethernet - 2,000,000

Fast Ethernet - 200,000

Gigabit Ethernet - 20,000

The default values for short path costs are:

Ethernet - 100

Fast Ethernet - 19

Gigabit Ethernet - 4

Priority (0-240, in steps of 16) — 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 designated port's priority and interface.

Designated Cost — 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 Transmission — Number of times the port has changed from the **Forwarding** state to **Blocking**.

LAG — The LAG to which the port is attached.

Enabling STP on a Port

1. Open the Spanning Tree **Port Settings** page.
2. Select the port.
3. Select **Enabled** in the **STP** field.
4. Define the **Fast Link**, **Path Cost**, and the **Priority** fields.
5. Click **Apply Changes**.

   STP is enabled on the port.

Modifying STP Port Properties

1. Open the Spanning Tree Port Settings page.
2. Select the port.
3. Modify the relevant fields.
4. Click **Apply Changes**.

   The STP port parameters are modified, and the device is updated.

Displaying the STP Port Table

1. Open the Spanning Tree 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 7-75. 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.
show **spanning-tree** [**ethernet** *interface* | **port-channel** *port-channel-number*][**instance** *instance-id*]	Displays spanning tree configuration.

Table 7-75. **STP Port Settings CLI Commands** *(continued)*

CLI Command	Description
spanning-tree portfast	Enables PortFast mode.
show spanning-tree [**detail**] [**active** | **blockedports**] [**instance** *instance-id*]	Displays detailed spanning tree information on active or blocked ports.
show spanning-tree mst-configuration	Displays spanning tree MST configuration identifier.

The following is an example of the CLI commands:

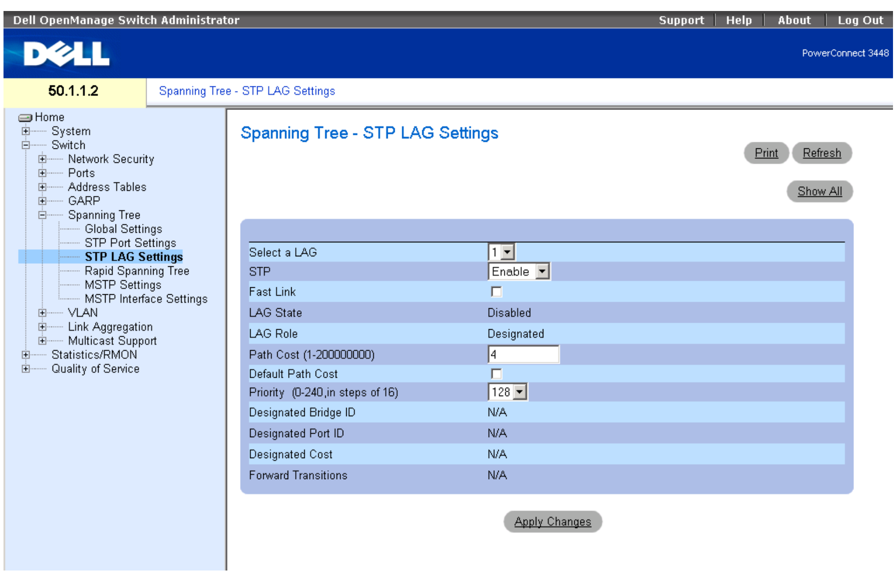
```
console> enable
console# configure
Console(config)# interface ethernet 1/e1
Console(config-if)# spanning-tree disable
Console(config-if)# spanning-tree cost 35000
Console(config-if)# spanning-tree port-priority 96
Console(config-if)# spanning-tree portfast
Console(config-if)# exit
Console(config)# exit
Console# show spanning-tree ethernet 1/e15
Port 1/e15 enabled
State: forwarding                  Role: designated
Port id: 128.15                    Port cost: 19
Type: P2p (configured: Auto) Internal Port Fast: No (configured:
No)
Designated bridge Priority : 32768 Address: 00:00:00:16:00:64
Designated port id: 128.15         Designated path cost: 4
Guard root: Disabled
Number of transitions to forwarding state: 2
BPDU: sent 483, received 1037
```

```
console# show spanning-tree ethernet 1/e15 instance 12
Port 1/e15 enabled
State: discarding                  Role: alternate
Port id: 128.15                    Port cost: 19
Type: P2p (configured: Auto) Internal Port Fast: No (configured:
No)
Designated bridge Priority : 32768 Address: 00:00:b0:07:07:49
Designated port id: 128.11         Designated path cost: 0
Guard root: Disabled
Number of transitions to forwarding state: 3
BPDU: sent 482, received 1035
```

Defining STP LAG Settings

Use the **Spanning Tree LAG Settings** page to assign STP aggregating ports parameters. To open the Spanning Tree **LAG Settings** page, click **Switch→Spanning Tree→LAG Settings** in the tree view.

Figure 7-24. Spanning Tree LAG Settings



The **Spanning Tree LAG Settings** page contains the following fields:

Select a LAG — The LAG number for which you want to modify STP settings.

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 — STP is currently disabled on the LAG. The LAG forwards traffic while learning MAC addresses.

Blocking — The LAG is blocked and cannot be used to forward traffic or learn MAC addresses.

RSTP Discarding State — In this state the port does not learn MAC addresses and do not forward frames.

This state is union of Blocking, and Listening state introduced in STP (802.1.D).

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.

LAG Role—Indicates the LAG role assigned by the STP algorithm that provides STP paths. The possible field values are:

Root—Provides the lowest cost path to forward packets to root switch.

Designated—Indicates that the via which the designated switch is attached to the LAN.

Alternate—Provides an alternate LAG to the root switch 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 by a point-to-point link. Backup ports also occur when a LAN has two or more connections connected to a shared segment.

Disabled—Indicates the LAG is not participating in the Spanning Tree.

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 is being rerouted. The path cost has a value of 1 to 200000000.

Default Path Cost — Indicates if the default path cost is used. The possible LAG path cost default_values are:

Long Method for LAG — 20,000

Short Method for LAG — 4

Priority (0-240, in steps of 16) — Priority value of the LAG. The priority value influences the LAG choice when a bridge has looped ports. The priority value is between 0-240, in steps of 16.

Designated Bridge ID — The priority and the MAC Address of the designated bridge.

Designated Port ID — The ID of the selected interface.

Designated Cost — 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 — Number of times the **LAG State** has changed from the **Forwarding** state to a **Blocking state**.

Modifying the LAG STP Parameters

1. Open the **Spanning Tree 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 contains the CLI commands for defining STP LAG settings.

Table 7-76. 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 7-76. STP LAG Settings CLI Commands *(continued)*

CLI Command	Description
show spanning-tree [**ethernet** *interface* | **port-channel** *port-channel-number*][**instance** *instance-id*]	Displays spanning tree configuration.
show spanning-tree [**detail**] [**active** | **blockedports**] [**instance** *instance-id*]	Displays detailed spanning tree information on active or blocked ports.

The following is an example of the CLI commands:

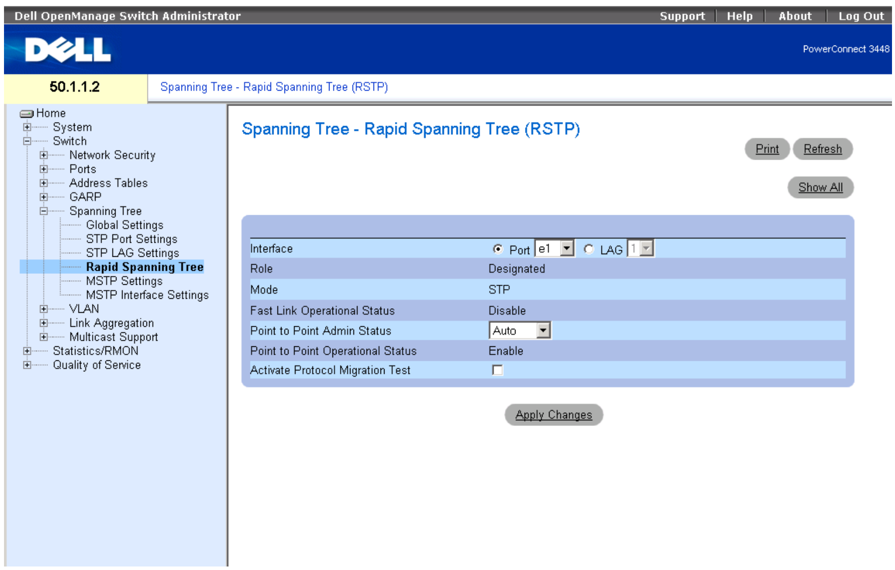
```
console(config)# interface port-channel 1
console(config-if)# spanning-tree disable
console(config-if)# spanning-tree cost 35000
console(config-if)# spanning-tree port-priority 96
console(config-if)# spanning-tree portfast
```

Defining Rapid Spanning Tree

While the classic spanning tree prevents Layer 2 forwarding loops on a general network topology, convergence can take 30-60 seconds. The delay allows time to detect possible loops, and propagate status changes.

Rapid Spanning Tree Protocol (RSTP) detects and uses network topologies that allow a faster convergence of the spanning tree, without creating forwarding loops. To open the Rapid Spanning Tree (RSTP) settings page, click **Switch→Spanning Tree→Rapid Spanning Tree** in the tree view.

Figure 7-25. Rapid Spanning Tree (RSTP) settings



The Spanning Tree RSTP page contains the following fields:

Interface — Port or LAG for which you can view and edit RSTP settings.

State — Disables RSTP state of the selected interface.

Role—Indicates the port role assigned by the STP algorithm in order to provide STP paths. The possible field values are:

> **Root**—Provides the lowest cost path to forward packets to root switch.
>
> **Designated**—Indicates that the port or LAG via which the designated switch is attached to the LAN.
>
> **Alternate**—Provides an alternate path to the root switch 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 by a point-to-point link. Backup ports also occur when a LAN has two or more connections connected to a shared segment.
>
> **Disabled**—Indicates the port is not participating in the Spanning Tree.

Mode—Indicates the current Spanning Tree mode. The Spanning Tree mode is selected in the **Spanning Tree Global Settings** page. The possible field values are:

Classic STP—Indicates that Classic STP is enabled on the device.

Rapid STP—Indicates that Rapid STP is enabled on the device.

Multiple STP—Indicates that Multiple STP is enabled on the device.

Fast Link Operational Status — Indicates if Fast Link is enabled or disabled for the port or LAG. If Fast Link is enabled for an interface, the interface 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 switch port link type. It may differ from the administrative state.

Point-to-Point Operational Status — The Point-to-Point operating state.

Activate Protocol Migrational — When checked, enables PPP sending Link Control Protocol (LCP) packets to configure and test the data link.

Defining RSTP parameters

1. Open the Spanning Tree RSTP Settings page.
2. Select an interface.
3. Define the fields.
4. Click **Apply Changes**.

   RSTP parameters are defined, and the device is updated.

Displaying the Rapid Spanning Tree (RSTP) Table

1. Open the Rapid Spanning Tree (RSTP) page.
2. Click **Show All**.

   The **Rapid Spanning Tree (RSTP) Table** opens.

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)**.

Table 7-77. 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** | **mstp**}	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:

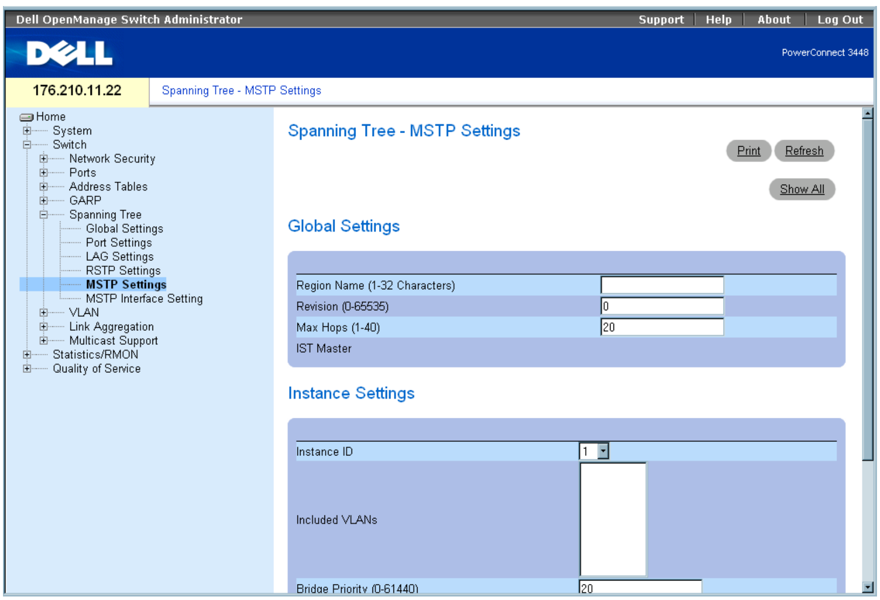
```
console(config)# interface ethernet 1/e5
console(config-if)# spanning-tree link-type shared
console(config-if)# spanning tree mode rstp
```

Configuring Multiple Spanning Tree

MSTP operation maps VLANs into STP instances. Multiple Spanning Tree provides differing load balancing scenario. For example, while port A is blocked in one STP instance, the same port is placed in the *Forwarding State* in another STP instance.

In addition, packets assigned to various VLANs are transmitted along different paths within Multiple Spanning Trees Regions (MST Regions). Regions are one or more Multiple Spanning Tree bridges by which frames can be transmitted. To open the **MSTP Settings** page, click **Switch** → **Spanning Tree** →**MSTP Settings** in the tree view.

Figure 7-26. MSTP Settings



The **MSTP Settings** page contains the following fields:

Region Name (1-32 Characters) — Indicates user-defined MSTP region name.

Revision (0-65535) — Defines unsigned 16-bit number that identifies the current MST configuration revision. The revision number is required as part of the MST configuration. The possible field range is 0-65535.

Max Hops (1-40) — Defines the total number of hops that occur in a specific region before the BPDU is discarded. Once the BPDU is discarded, the port information is aged out. The possible field range is 1-40. The field default is 20 hops.

IST Master — Indicates the Internal Spanning Tree Master ID. The IST Master is the instance 0 root.

Instance ID — Defines the MSTP instance. the field range is 1-15.

Included VLANs — Displays VLANs mapped to the selected instance. Each VLAN belongs to one instance.

Bridge Priority (0-61440) — Specifies the selected spanning tree instance device priority. The field range is 0-61440 in steps of 4096.

Designated Root Bridge ID — Indicates the ID of the bridge which is the root of the selected instance.

Root Port — Indicates the selected instance's root port.

Root Path Cost — Indicates the selected instance's path cost.

Bridge ID — Indicates the bridge ID of the selected instance.

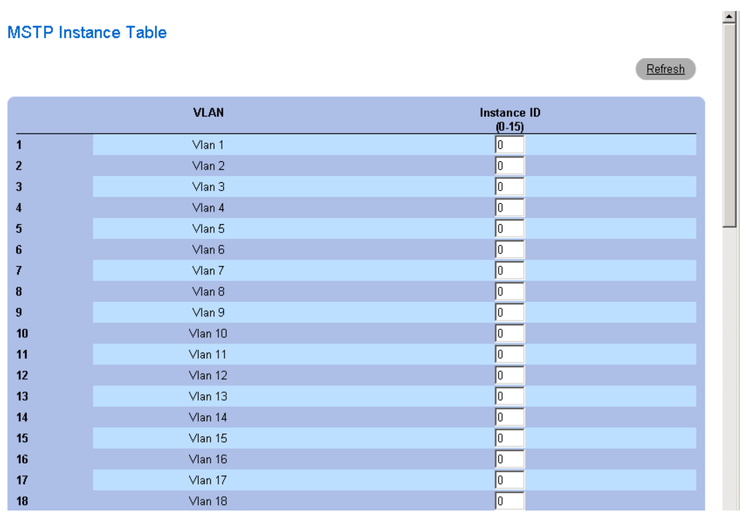
Remaining Hops — Indicates the number of hops remaining to the next destination.

Displaying the MSTP Instance Table

1 Open the **Spanning Tree MSTP Settings** page.

2 Click **Show All** to open the **MSTP Instance Table**.

Figure 7-27. MSTP Instance Table



Defining MST Instances Using CLI Commands

The following table summarizes the equivalent CLI commands for defining MST instance groups as displayed in the **Spanning Tree MSTP Settings** page.

Table 7-78. MSTP Instances CLI Commands

CLI Command	Description
spanning-tree mst configuration	Enters MST Configuration mode.
instance *instance-id* {**add** | **remove**} **vlan** *vlan-range*	Maps VLANs to the MST instance.
name *string*	Sets the configuration name.
revision *value*	Sets the configuration revision number
spanning-tree mst *instance-id* **port-priority** *priority*	Sets the priority of a port.
spanning-tree mst *instance-id* **priority** *priority*	Sets the device priority for the specified spanning tree instance.
spanning-tree mst max-hops *hop-count*	Sets the number of hops in an MST region before the BPDU is discarded and the information held for a port is aged.
spanning-tree mst *instance-id* **cost** *cost*	Sets the path cost of the port for MST calculations
exit	Exits the MST region configuration mode and applies configuration changes.
abort	Exits the MST region configuration mode without applying configuration changes.
show {**current** | **pending**}	Displays the current or pending MST region configuration.

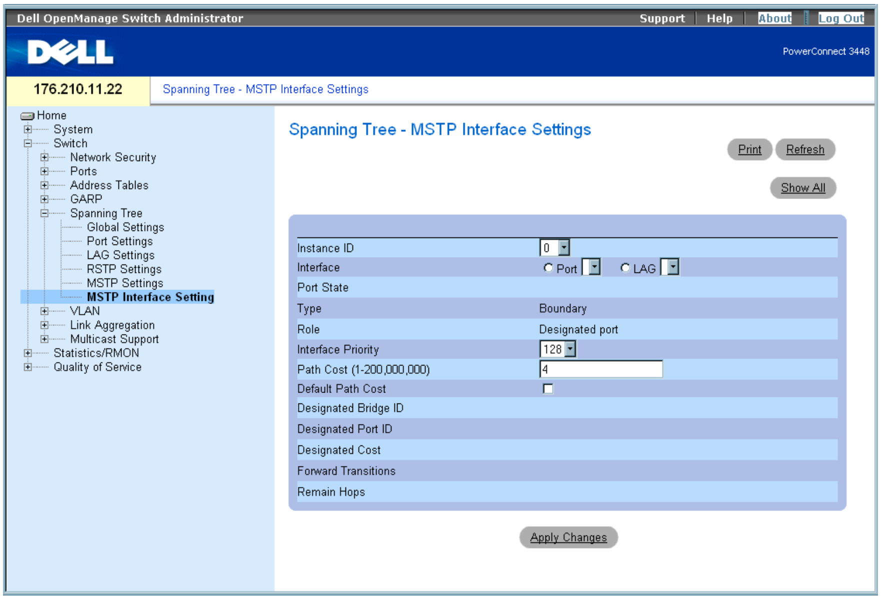
The following is an example of the CLI commands:

```
console(config)# spanning-tree mst configuration
console(config-mst)# instance 1 add vlan 10-20
console(config-mst)# name region1
console(config-mst)# revision 1
console(config)# spanning-tree mst configuration
console(config-mst)# instance 2 add vlan 21-30
console(config-mst)# name region1
console(config-mst)# revision 1
console(config-mst)# show pending
Pending MST configuration
Name: Region1
Revision: 1
Instance   Vlans Mapped
--------   ------------
0          1-9,31-4094
1          10-20
2          21-30
```

Defining MSTP Interface Settings

The **MSTP Interface Settings** page contains parameters assigning MSTP settings to specific interfaces. To open the **MSTP Interface Settings** page, click **Switch →Spanning Tree →MSTP Interface Settings** in the tree view.

Figure 7-28. MSTP Interface Settings



The **MSTP Interface Settings** page contains the following fields:

Instance ID — Lists the MSTP instances configured on the device. Possible field range is 1-15.

Interface — Assigns either ports or LAGs to the selected MSTP instance.

Port State— Indicates whether the port is enabled or disabled in the specific instance.

Type — Indicates whether MSTP treats the port as a point-to-point port, or a port connected to a hub, and whether the port is internal to the MST region or a boundary port. A Master port provides connectivity from a MSTP region to the outlying CIST root. A Boundary port attaches MST bridges to LAN in an outlying region. If the port is a boundary port, it also indicates whether the device on the other side of the link is working in RSTP or STP mode.

Role — Indicates 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 — Indicates 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 by a point-to-point link. Backup ports also occur when a LAN has two or more connections connected to a shared segment.

Disabled — Indicates the port is not participating in the Spanning Tree.

Interface Priority (0-240,in steps of 16)— Defines the interface priority for specified instance. The default value is 128.

Path Cost — Indicates the port contribution to the Spanning Tree instance. The range should always be 1-200,000,000.

Default Path Cost — Indicates that the default path cost is assigned according to the method selected on the **Spanning Tree Global Settings** page.

Designated Bridge ID — The bridge ID number that connects the link or shared LAN to the root.

Designated Port ID — The Port ID number on the designated bridge that connects the link or the shared LAN to the root.

Designated Cost — Cost of the path from the link or the shared LAN to the root.

Forward Transitions — Number of times the port changed to the forwarding state.

Remain Hops — Indicates the number of hops remaining to the next destination.

Defining MSTP Interface Settings

1. Open the **MSTP Interface Settings** page.
2. Select an interface.
3. Define the fields.
4. Click **Apply Changes**.

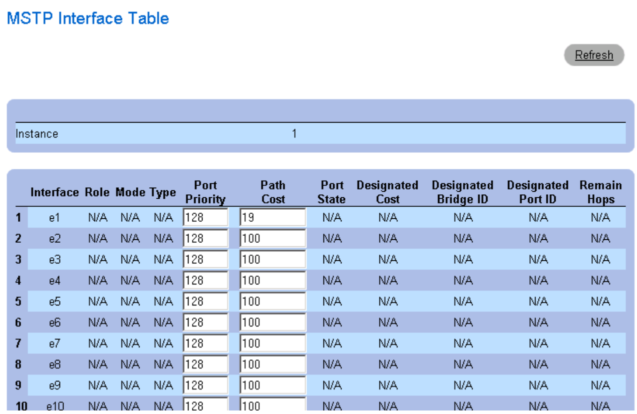
   MSTP parameters are defined, and the device is updated.

Viewing the MSTP Interface Table

1. Open the **MSTP Interface Settings** page.
2. Click **Show All**.

   The **MSTP Interface Table** page opens:

Figure 7-29. MSTP Interface Table


MSTP Interface Table

Refresh

Instance	1

	Interface	Role	Mode	Type	Port Priority	Path Cost	Port State	Designated Cost	Designated Bridge ID	Designated Port ID	Remain Hops
1	e1	N/A	N/A	N/A	128	19	N/A	N/A	N/A	N/A	N/A
2	e2	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
3	e3	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
4	e4	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
5	e5	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
6	e6	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
7	e7	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
8	e8	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
9	e9	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
10	e10	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A

Defining MSTP Interfaces Using CLI Commands

The following table summarizes the equivalent CLI commands for defining MSTP interfaces as displayed in the **Spanning Tree MSTP Interface Settings** page.

Table 7-79. MSTP Interface CLI Commands

CLI Command	Description
spanning-tree mst *instance-id* **cost** *cost*	Sets the path cost of the port for MST calculations
spanning-tree mst *instance-id* **priority** *priority*	Sets the device priority for the specified ST instance.
show spanning-tree mst-configuration	Displays the MST configuration.

The following is an example of the CLI commands:

```
console# show spanning-tree mst-configuration
Gathering information ..........
Current MST configuration
Name: Gili
Revision: 65000
Instance            Vlans Mapped            State
---------           -------------------------   -----------
0                   16-4094                 enabled
1                   1                       enabled
2                   2                       enabled
3                   3                       enabled
4                   4                       enabled
5                   5                       enabled
6                   6                       enabled
7                   7                       enabled
8                   8                       enabled
9                   9                       enabled
10                  10                      enabled
11                  11                      enabled
12                  12                      enabled
13                  13                      enabled
14                  14                      enabled
15                  15                      enabled
```

Configuring VLANs

VLANs are logical subgroups with a LAN created via software, rather than defining a hardware solution. VLANs combine user stations and network devices into a single unit, 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 reduce the amount of time network changes, additions, and moves are implemented.

VLANs have no minimum number of ports, and can be created per unit, per device, per stack, or any other logical connection combination, as VLANs are software-based and not defined by physical attributes.

VLANs function at Layer 2 level. Since VLANs isolate traffic within the VLAN, a router working at the Layer 3 protocol level is needed to allow traffic flow between VLANs. Layer 3 routers identify segments and coordinate with VLANs. VLANs are Broadcast and Multicast domain. 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 4-byte tag to packet headers. The VLAN tag indicates to which VLAN the packet belongs. VLAN tags are attached to the VLAN by either the end station or by the network device. VLAN tags also contains VLAN network priority information.

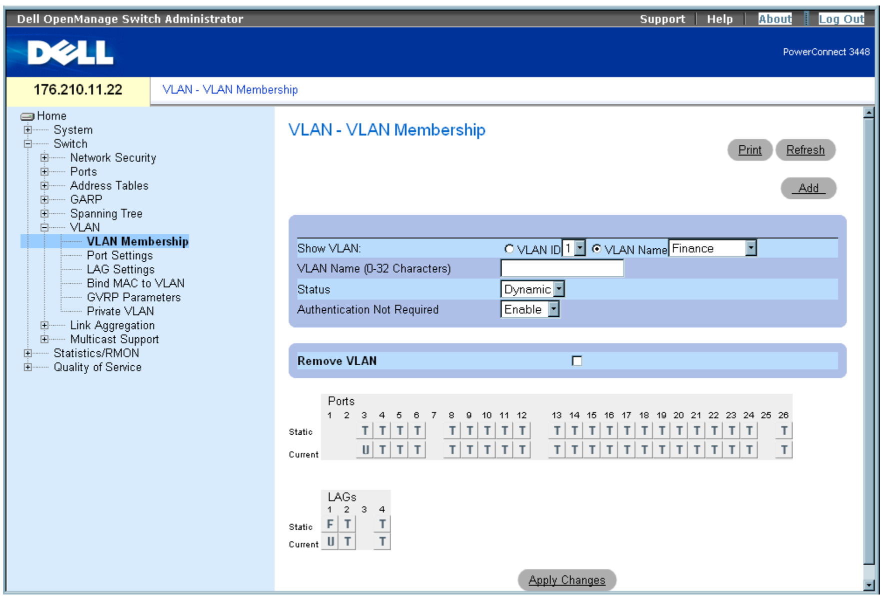
Combining VLANs and GVRP allows network managers to define network nodes into Broadcast domains. Broadcast and Multicast traffic is confined to the originating group.

To open the **VLAN** page, click **Switch →VLAN** in the tree view.

Defining VLAN Membership

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 ID #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 7-30. VLAN Membership



The **VLAN Membership** page contains the following fields:

Show VLAN — Lists and displays specific VLAN information according to VLAN ID or VLAN name.

VLAN Name (0-32 Characters) — 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.

Authentication Not Required— 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 VLANs

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 7-80. VLAN Membership Group CLI Commands

CLI Command	Description
`vlan database`	Enters the VLAN configuration 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)# end
console(config)# interface vlan 1972
console(config-if)# name Marketing
console(config-if)# end
```

VLAN Port Membership Table

The **VLAN Port Membership Table** contains a **Port Table** for assigning ports to VLANs. Ports are assigned to a VLAN by toggling through the **Port Control** settings. Ports can have the following values:

Table 7-81. 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.

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 7-82. 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).
switchport general allowed vlan add *vlan-list* [**tagged** | **untagged**]	Adds or removes VLANs for a port in general mode.
switchport general pvid vlan-id	Configures the PVID when the interface is in general mode.

The following is an example of the CLI commands:

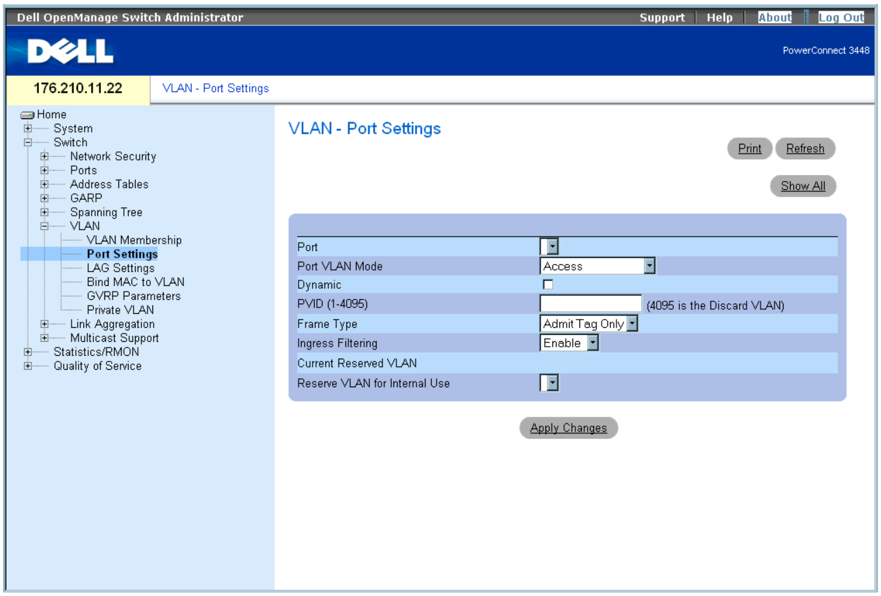
```
console(config)# vlan database
console(config-vlan)# vlan 23-25
console(config-vlan)# end
console(config)# interface vlan 23
console(config-if)# name Marketing
console(config-if)# end
console(config)# interface ethernet 1/e8
console(config-if)# switchport mode access
console(config-if)# switchport access vlan 23
console(config-if)# end
console(config)# interface ethernet 1/e9
console(config-if)# switchport mode trunk
console(config-if)# switchport mode trunk allowed vlan
add 23-25
console(config-if)# end
console(config)# interface ethernet 1/e11
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 7-31. VLAN Port Settings



The **VLAN Port Settings** page contains the following fields:

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).
>
> **PVE Promiscuous** — The port is part of a PVE Promiscuous VLAN.
>
> **PVE Community** — The port is part of a PVE Community VLAN.
>
> **PVE Isolated** — The port is part of a PVE Isolated VLAN.

Dynamic — Assigns a port to a VLAN based on the host source MAC address connected to the port.

PVID — Assigns a VLAN ID to untagged packets. The possible values are 1-4095. 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 port is not a member.

Current Reserved 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

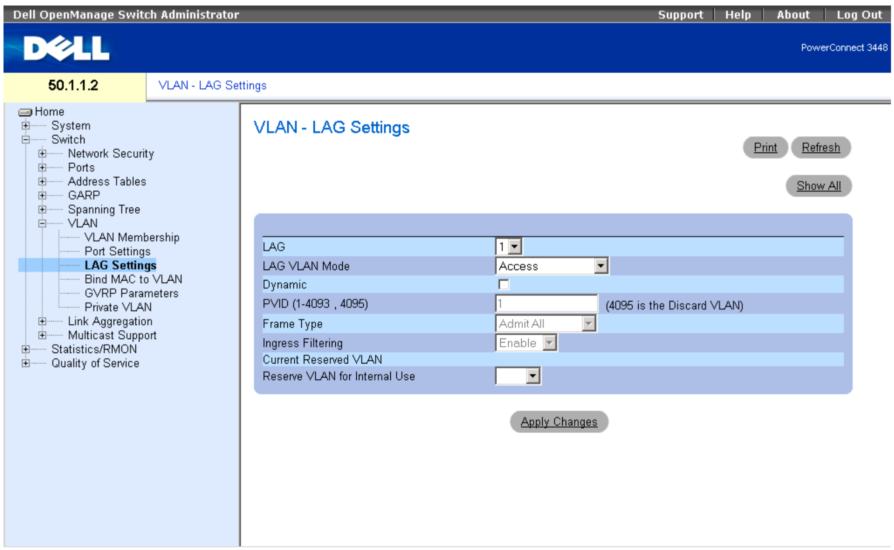
1. Open the **VLAN Port Settings** page.
2. Click **Show All.**

   The **VLAN Port Table** opens.

Defining VLAN LAGs Settings

The **VLAN LAG Settings** 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 Settings** page, click **Switch→VLAN→LAG Settings** in the tree view.

Figure 7-32. VLAN LAG Settings



The **VLAN LAG Settings** page contains the following fields:

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 one port that can be untagged).
>
> **PVE Promiscuous** — The LAG belongs to a PVE Promiscuous VLAN.
>
> **PVE Community** — The LAG belongs to a PVE Community VLAN.
>
> **PVE Isolated** — The LAG belongs to a PVE Isolated VLAN.

Dynamic — Assigns a LAG to a VLAN based on the host source MAC address connected to the LAG.

PVID (1-4093 , 4095) — 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 LAG 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 Settings** 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 Settings** 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 Settings** page.

Table 7-83. LAG VLAN Assignments CLI Commands

CLI Command	Description
switchport mode {access | trunk | general}	Configures a LAG 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 LAG default VLAN ID (PVID).
switchport general pvid *vlan-id*	Configure the LAG VLAN ID (PVID) when the interface is in general mode.

Table 7-83. LAG VLAN Assignments CLI Commands *(continued)*

CLI Command	Description
switchport general allowed vlan add *vlan-list* [**tagged** | **untagged**]	Adds or removes VLANs from a general LAG.
switchport general acceptable-frame-type tagged-only	Discards untagged packets at ingress.
switchport access vlan dynamic	Binds the MAC address to the VLAN.
switchport general ingress-filtering disable	Disables LAG 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
```

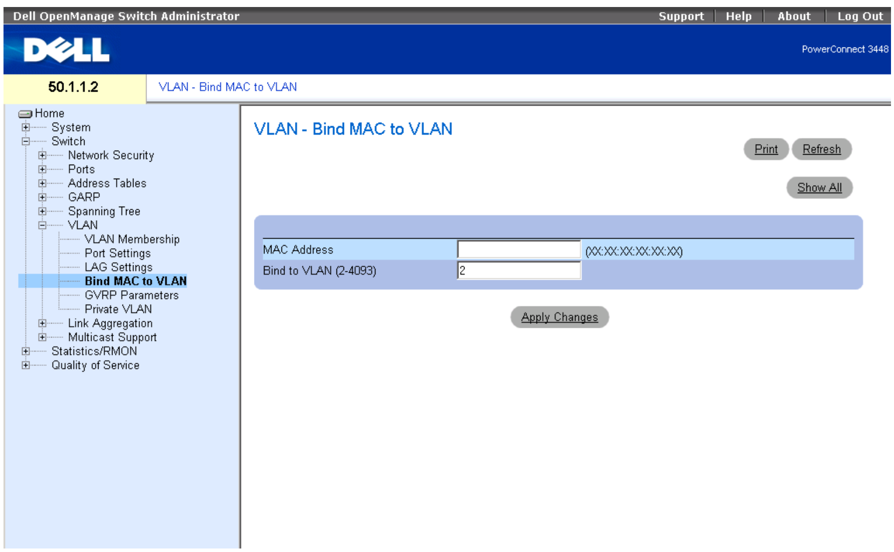
Binding MAC Address to VLANs

Binding MAC addresses to VLANs provides port to VLAN assignment based on MAC addresses. Once a VLAN is assigned a MAC address, and the MAC address is learned on a port, the port joins the bound VLAN. When the MAC address is aged out, the port leaves the VLAN. Only dynamic VLANs can be bound to MAC addresses.

To bind MAC addresses to a VLAN, ensure the VLAN ports were dynamically added, and are not static VLAN ports.

To open the **Bind MAC to VLAN** page, click **Switch→VLAN→Bind MAC to VLAN**.

Figure 7-33. Bind MAC to VLAN



The **Bind MAC to VLAN** page contains the following fields:

MAC Address — Indicates the MAC Address which is bound to the VLAN.

Bind to VLAN (2-4093) — Indicates the VLAN to which the MAC address is bound.

Displaying the MAC to VLAN table:

1 Open the **Bind MAC to VLAN** page.

2 Click **Show All**.

The **MAC to VLAN table** opens.

Binding MAC address to VLAN using CLI commands:

The following table summarizes the equivalent CLI commands for binding MAC addresses to VLAN.

Table 7-84. Binding MAC address to VLANs CLI Commands

CLI Command	Description
mac-to-vlan *mac-address vlan-id*	Binds the MAC address to the VLAN.
switchport access vlan dynamic	Configures private VLANs.
show mac-to-vlan	Displays the MAC to VLAN database
no mac-to-vlan *mac-address*	Unbinds the MAC address from the VLAN.

The following is an example of the CLI commands:

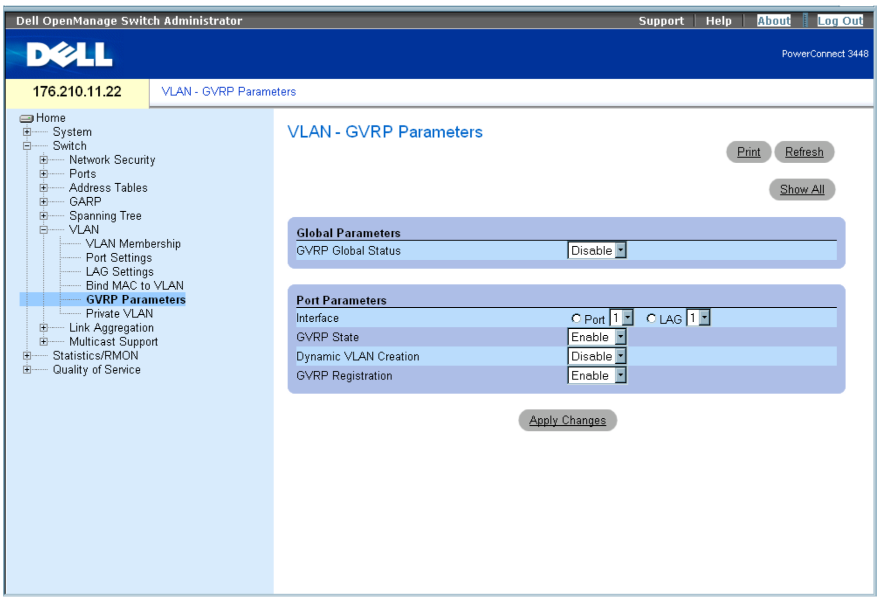
```
console(config-vlan)# mac-to-vlan 0060.704c.73ff 123

console(config-vlan)# exit

console(config)# exit

console# show vlan mac-to-vlan

MAC Address  VLAN

------------ ------

0060.704c.73ff 123
```

Configuring GVRP Parameters

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.

The **GVRP 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 7-34. GVRP Parameters



The GVRP Parameters page contains the following fields:

GVRP Global Status — Enables or disables GVRP on the device. GVRP is disabled by default.

Interface — Specifies port or LAG for editing GVRP settings.

GVRP State — Enables or disables GVRP on an interface.

Dynamic VLAN Creation — Enables or disables VLAN creation through GVRP on an interface.

GVRP Registration — Enables or disables VLAN registration through GVRP on an interface.

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**.
3. Select **Enable** in the GVRP State field for the desired interface.
4. Select **Enable** in the **GVRP Registration** field.
5. 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 7-85. 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 1/e1
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
-------  ------   ------------  --------  -------------- -----   -----
1/e11    Enabled  Forbidden     Disabled  200            900     10000
1/e12    Disabled Normal        Enabled   200            600     10000
```

Configuring Private VLANs

Private VLANs (PVLAN) increase network security by limiting inter-port communication within a VLAN. Private VLANs limit network traffic at the Layer 2 level. Network administrators define a Primary VLAN. Within the Primary VLAN there are Isolated and Community VLANs. Private VLAN ports can have the following states:

- **Promiscuous** — Promiscuous ports can communicate with all ports within a PVLAN. All promiscuous packets are automatically assigned to both the Isolated and the Community VLANs.
- **Isolated** — Isolated ports are completely isolated from other ports in the same PVLAN. However isolated ports can communicate with promiscuous ports. In addition, all traffic to and from isolated ports with a VLANs is blocked, except for traffic from promiscuous ports. All isolated ports are automatically assigned to the Isolated VLAN.
- **Community** — Community ports communicate with other community ports and with promiscuous ports. Community ports are separated from all other interfaces in other communities or isolated ports in the same PVLAN. All community ports are automatically assigned to the Community VLAN and to the Private VLAN.

NOTE: Ports cannot be defined as either promiscuous or isolated port if the ports are existing VLAN members.

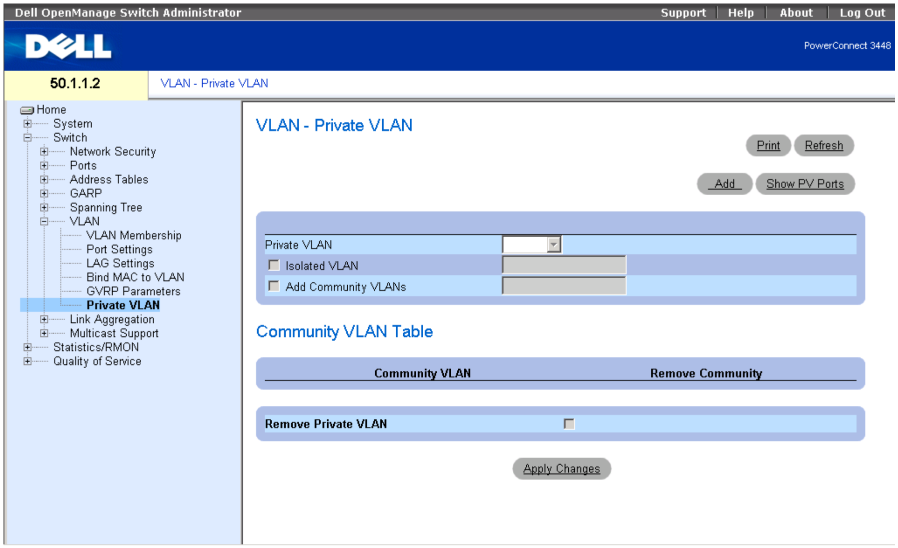
NOTE: Previously created VLANs cannot be configured as isolated or community VLANs.

NOTE: Isolated and Community VLANs included in the total VLAN count.

If the Primary VLAN is deleted, both the Isolated and the Community VLANs are also deleted. In addition, the Isolated and Community VLANs only forward untagged traffic.

To open the **Private VLAN** page, click **Switch→VLAN→Private VLAN** in the tree view.

Figure 7-35. Private VLAN



The **Private VLAN** page contains the following fields:

Private VLAN — Contains a list of user-defined Private VLANs. The Private VLANs are defined in the **Add Private VLAN** page.

Isolated VLAN — Indicates which VLAN to which isolated ports are assigned.

Add Community VLANs — Adds a Community VLAN to which community ports are assigned.

Community VLAN — Displays a list of the Community VLANs.

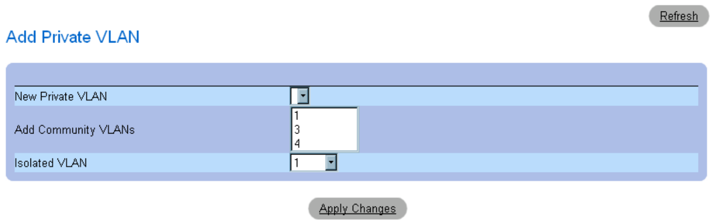
Remove Community — Removes a Community VLAN, when checked.

Remove Private VLAN — Removes a Private VLAN when checked.

Adding Private VLANs

1. Open the **Private VLAN** page.
2. Click **Add**. The **Add Private VLAN** page opens:

Figure 7-36. Add Private VLAN



The **Add Private VLAN** page contains the following additional fields:

New Private VLAN — Contains a Private VLAN list. Community VLANs are added to the Private VLAN.

Add Community VLANs — Adds a Community VLAN to the private VLAN.

Isolated VLAN — Adds an Isolated VLAN to the Private VLAN.

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

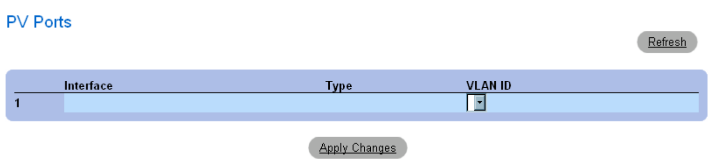
   The Private VLAN is defined, and the device is updated.

Displaying the PV Ports Table

1. Open the **Private VLAN** page.
2. Click **Show PV Ports**.

   The **PV Ports Table** opens:

Figure 7-37. PV Ports Table



Configuring PVLANs using CLI commands

The following table summarizes the equivalent CLI commands for configuring PVLANs as displayed in the **Private VLAN** page.

Table 7-86. Private VLAN CLI Commands

CLI Command	Description
switchport mode private vlan promiscuous	Adds a promiscuous port to a promiscuous VLAN.
switchport mode private vlan community	Adds a community port to a community VLAN.
switchport mode private vlan isolated	Adds a isolated port to a isolated VLAN.
private-vlan primary	Defines a primary VLAN.
private-vlan community {**add** *community-vlan-list* | **remove** *community-vlan-list* }	Defines or removes a community VLAN of the primary VLAN.
private-vlan isolated	Defines an isolated VLAN of the primary VLAN
switchport private-vlan *pvlan* [**community** *cvlan*]	Defines private VLAN ports.
show vlan private-vlan [primary vlan-id]	Displays the private primary VLAN.

The following is an example of the CLI commands:

```
console(config)# vlan database
console(config-vlan)#vlan 2
console(config-vlan)#exit
console(config)#interface vlan 2
console(config-if)# private-vlan primary
console(config)#interface vlan 2
console(config-if)# private-vlan isolated 10
console(config-if)# private-vlan community add 20
console# show vlan private-vlan
console(config-if)# end
```

Aggregating Ports

Link Aggregation optimizes port usage by linking a group of ports together to form a single LAG (aggregated group). Aggregating ports multiplies the bandwidth between the devices, increases port flexibility, and provides link redundancy.

The device supports both static LAGs and Link Aggregation Control Protocol (LACP) LAGs. LACP LAGs negotiate aggregating port's 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.

Consider the following when aggregating ports:

- All ports within a LAG must be the same media type.
- A VLAN is not configured on the port.
- The port is not assigned to a different LAG.
- Auto-negotiation mode is not configured on the port.
- The port is in full-duplex mode.
- All ports in the LAG have the same ingress filtering and tagged modes.
- All ports in the LAG have the same back pressure and flow control modes.
- All ports in the LAG have the same priority.
- All ports in the LAG have the same transceiver type.
- The device supports up to eight LAGs, and eight ports in each LAG.
- Ports can be configured as LACP ports only if the ports are not part of a previously configured LAG.

Ports added to a LAG lose their individual port configuration. When ports are removed from the LAG, the original port configuration is applied to the ports.

The device uses a hash function to determine which packets are carried on which aggregated-link member. The hash function statistically load-balances the aggregated link members. The device considers an Aggregated Link a single logical port.

Defining LACP Parameters.

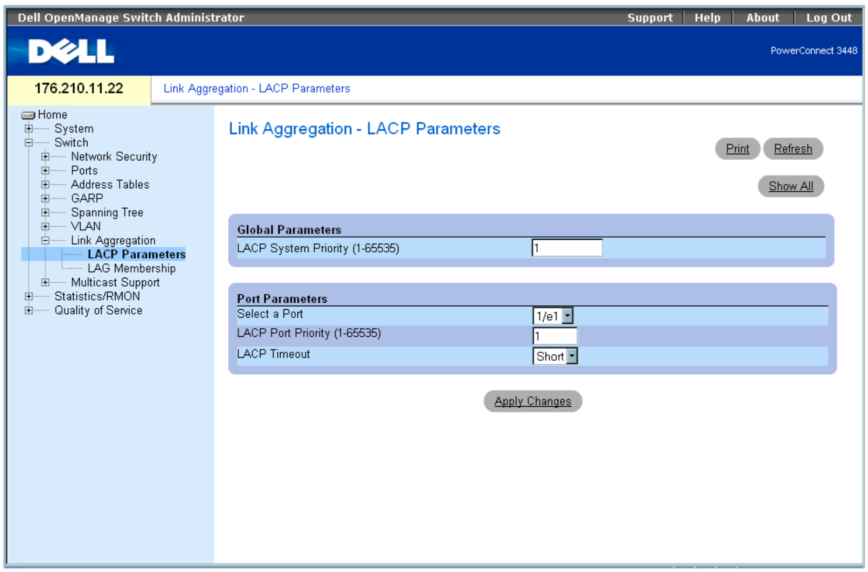
Aggregate ports can be linked into link-aggregation port-groups. Each group comprises ports with the same speed, set to full-duplex operations.

Ports in a Link Aggregated group (LAG) can contain different media types if the ports are operating at the same speed. Aggregated links can be manually or automatically configured by enabling Link Aggregation Control Protocol (LACP) on the relevant links.

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 7-38. LACP Parameters



The **LACP Parameters** page contains the following fields:

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 7-87. 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 1/e11
Console (config-if)# lacp port-priority 247
Console (config-if)# lacp timeout long
Console (config-if)# end
Console# show lacp ethernet 1/e11 statistics
Port 1/e11 LACP Statistics:
LACP PDUs sent:2
LACP PDUs received:2
```

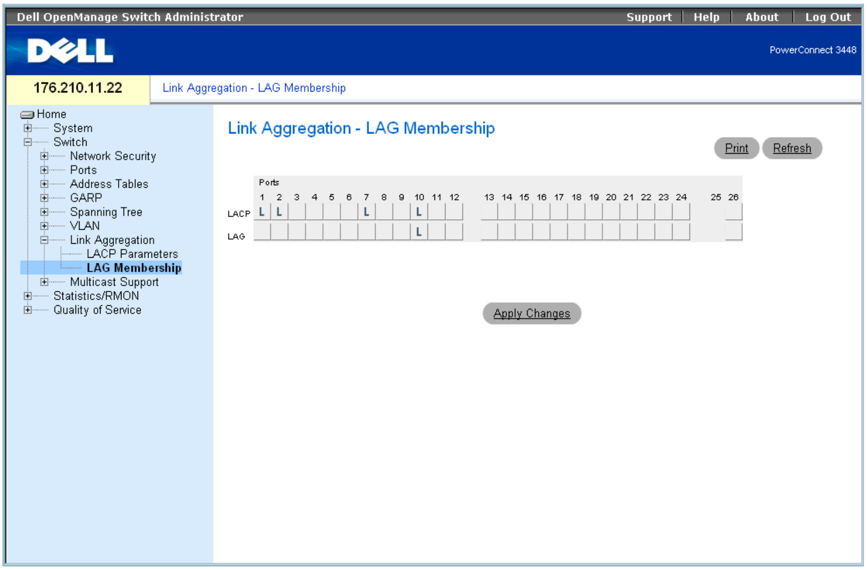
Defining LAG Membership

The device supports eight LAGs per system, and eight ports per LAG, whether the device is a stand-alone device or in a stack.

When a port is added to a LAG, the port acquires the LAG's properties. If the port cannot be configured with the LAG's properties, it is not added to the LAG. An error message is generated. However, if the first port joining the LAG cannot be configured with the LAG settings, the port is added to the LAG, using the port default settings. An error message is generated. However, as this is the only port in the LAG, the entire LAG operates with the port's settings, instead of the LAG's defined settings.

Use the **LAG Membership** page to assign ports to LAGs. To open the **LAG Membership** page, click **Switch →Link Aggregation→LAG Membership** in the tree view.

Figure 7-39. LAG Membership



The **LAG Membership** page contains the following fields:

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.

Adding Ports 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.

Adding 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 7-88. LAG Membership CLI Commands

CLI Command	Description
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)# interface ethernet 1/e11
console(config-if)# channel-group 1 mode on
```

Multicast Forwarding Support

Multicast forwarding allows a single packet to be forwarded to multiple destinations. Layer 2 Multicast service is based on Layer 2 device 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.

Registered Multicast traffic — If traffic addressed to a registered multicast group is seen it is handled by an entry in the Multicast Filtering Database and forwarded only to the registered ports.

Unregistered Multicast traffic — If traffic addressed to an unregistered Multicast group is seen, it is handled by a special entry in the Multicast Filtering Database. The default setting of this is to flood all such traffic (traffic in unregistered Multicast groups).

The device supports:

- **Forwarding L2 Multicast Packets** — Forwards Layer 2 Multicast packets. Layer 2 Multicast filtering is enabled by default, and not user-configurable.

  NOTE: The system supports Multicast filtering for 256 Multicast groups.

- **Filtering L2 Multicast Packets** — Forwards 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, managing the packet as a single Multicast transmission. While Multicast traffic forwarding is effective, it is not optimal, as irrelevant ports also receive the Multicast packets. The excess packets cause increased network traffic. Multicast forwarding filters enable forwarding of Layer 2 packets to port subsets.

When IGMP Snooping is enabled globally, all IGMP packets are forwarded to the CPU. The CPU analyzes the incoming packets and determines:

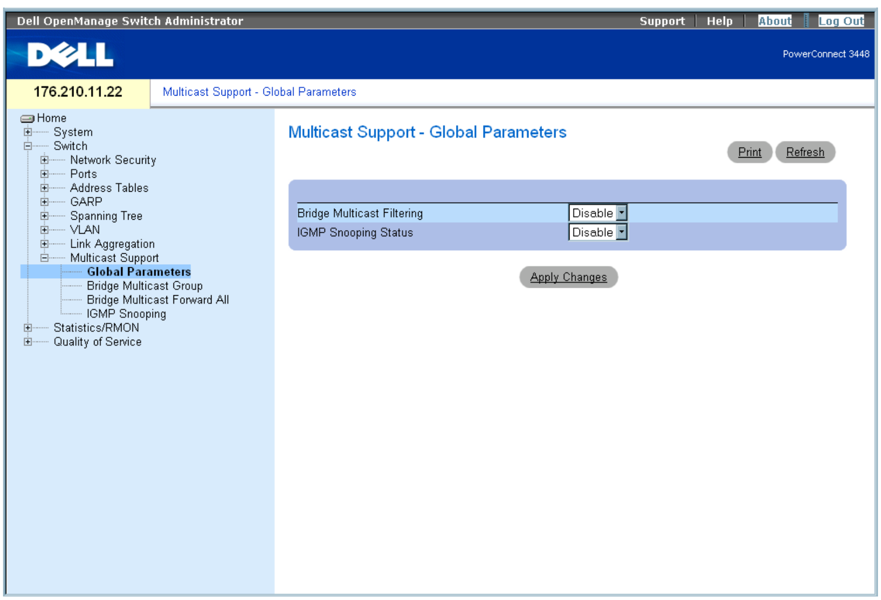
- Which ports want to join which Multicast groups.
- Which ports have Multicast routers generating IGMP queries.
- What routing protocols are forwarding packets and Multicast traffic.

Ports requesting to join a specific Multicast group issue an IGMP report, specifying that Multicast group is accepting members. This results in the creation of the Multicast filtering database.

To open the **Multicast Support** page, click **Switch →Multicast Support** in the tree view.

The **Global Parameters** page contains fields for enabling IGMP Snooping on the device. To open the **Global Parameters** page, click **Switch→Multicast Support→Global Parameters** in the tree view.

Figure 7-40. Global Parameters



The **Global Parameters** page contains the following fields:

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. IGMP Snooping can be enabled only if **Global Parameters** is enabled.

Enabling Bridge Multicast Filtering on the device

1 Open the **Global Parameters** page.

2 Select **Enable** in the **Bridge Multicast Filtering** field.

3 Click **Apply Changes**.

Bridge Multicast Filtering is enabled on the device.

Enabling IGMP Snooping on the device

1 Open the **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 Filtering and IGMP Snooping Using CLI Commands

The following table summarizes the equivalent CLI commands for enabling Multicast Filtering and IGMP Snooping as displayed on the **Global Parameters** page.

Table 7-89. Multicast Filtering 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
```

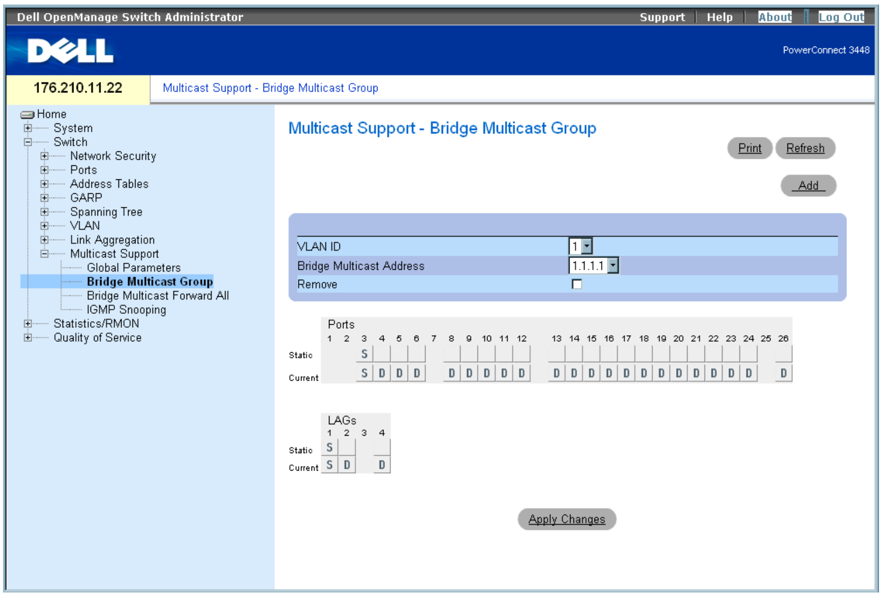
Adding Bridge Multicast Address Members

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 Group** in the tree view.

Figure 7-41. Bridge Multicast Group



The **Bridge Multicast Group** page contains the following fields:

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 7-90. IGMP Port/LAG Members Table Control Settings

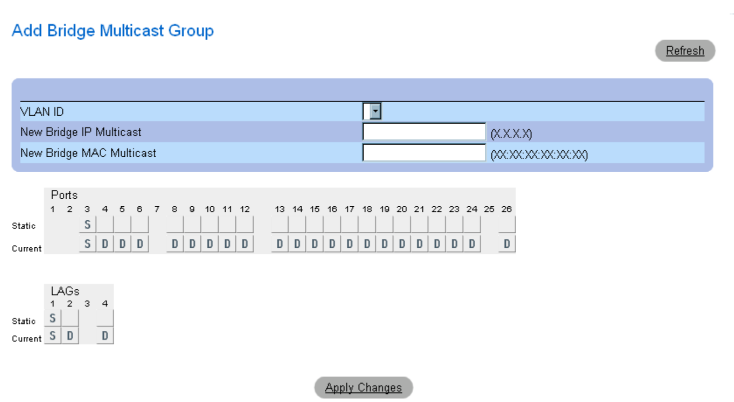
Port Control	Definition
D	The port/LAG has joined the Multicast group dynamically in the Current Row.
S	Attaches the port to the Multicast group as static member in the Static Row. The port/LAG has joined the Multicast group statically in the Current Row.
F	Forbidden.
Blank	The port is not attached to 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 7-42. Add Bridge Multicast Group



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 7-91. 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(config-if)# bridge multicast address 0100.5e02.0203
add ethernet 1/e11,1/e12
console(config-if)# end
console # show bridge multicast address-table

Vlan     MAC Address            Type              Ports
----     -----------            -----             ----------
1        0100.5e02.0203         static            1/e11, 1/e12
19       0100.5e02.0208         static            1/e11-16
19       0100.5e02.0208         dynamic           1/e11-12

Forbidden ports for multicast addresses:

Vlan     MAC Address            Ports
----     -----------            ----------
1        0100.5e02.0203         1/e8
19       0100.5e02.0208         1/e8

console # show bridge multicast address-table format ip

Vlan     IP Address             Type              Ports
----     -----------            -----             ----------
1        224-239.130|2.2.3      static            1/e11, 1/e12
19       224-239.130|2.2.8      static            1/e11-16
19       224-239.130|2.2.8      dynamic           1/e11-12
```

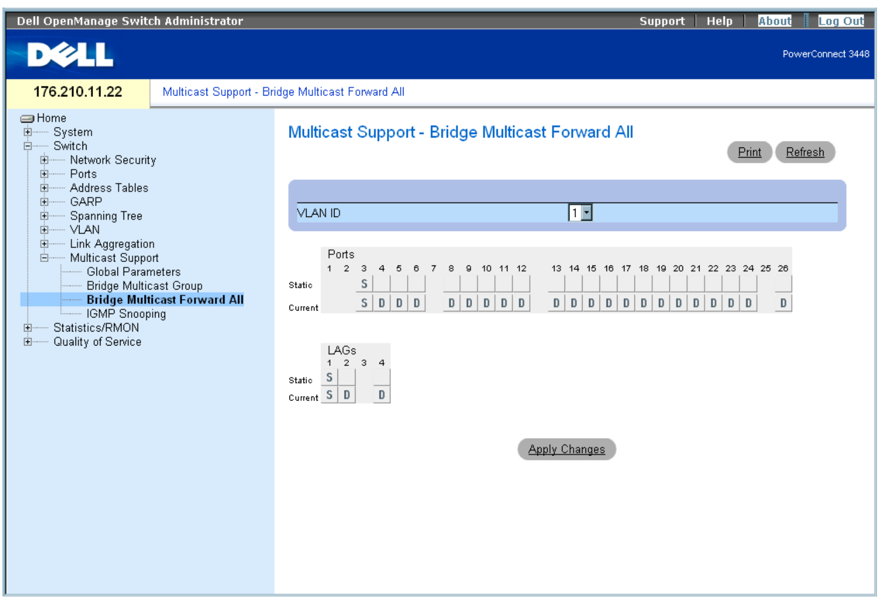
```
Forbidden ports for multicast addresses:

Vlan      IP Address               Ports
----      -----------              ----------
1         224-239.130|2.2.3        1/e8
19        224-239.130|2.2.8        1/e8
```

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 Forward All** page in the tree view.

Figure 7-43. Bridge Multicast Forward All



The Bridge Multicast Forward All page contains the following fields:

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 Switch/Port Control Settings Table** contains the settings for managing router and port settings.

Managing Bridge Multicast Forward All Switch/Port Control Settings Table

The following table describes the controls used to set the port controls.

Table 7-92. Bridge Multicast Forward All Switch/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 7-93. 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.
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.

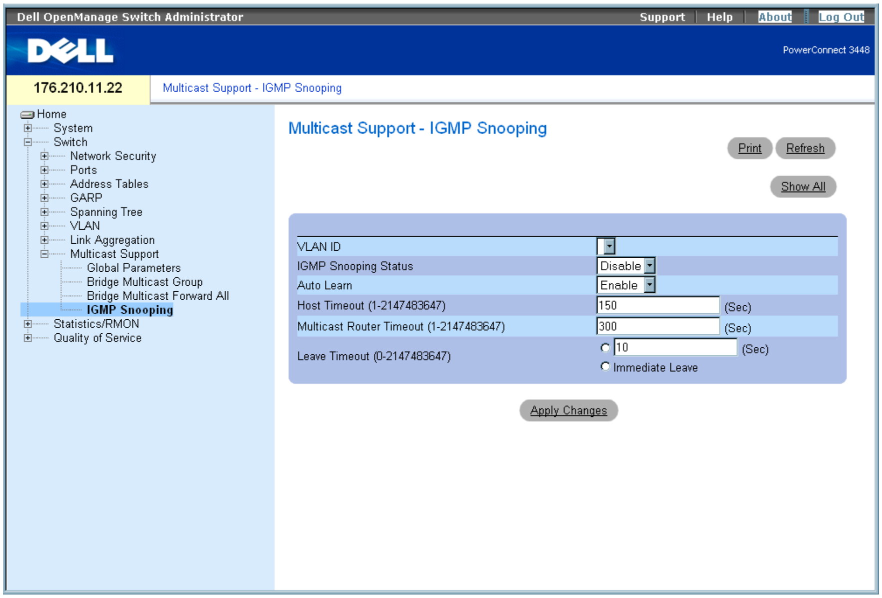
The following is an example of the CLI commands:

```
Console(config)# interface vlan 1
Console(config-if)# bridge multicast forward-all add ethernet
1/e3
Console(config-if)# end
Console# show bridge multicast filtering 1
Filtering: Enabled
VLAN:           Forward-All
Port            Static                   Status
-------         -----------------        -----------
1/e11           Forbidden                Filter
1/e12           Forward                  Forward(s)
1/e13           -                        Forward(d)
```

IGMP Snooping

The **IGMP Snooping** page contains fields for enabling IGMP snooping per VLAN, and defining the aging time for packets. To open the **IGMP Snooping** page, click **Switch→Multicast Support→ IGMP Snooping** in the tree view.

Figure 7-44. IGMP Snooping



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 Ethernet 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. 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 7-94. 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)# ip igmp snooping leave-time-out 60
console(config-if)# end
console# show ip igmp snooping groups

Vlan      IP Address              Querier    Ports
--------  ----------------------  ---------  ----------------
1         224-239.130|2.2.3       Yes        1/e11, 1/e12
19        224-239.130|2.2.8       Yes        1/e11-13

console# show ip igmp snooping interface 1/e1
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         1/e11
```

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.

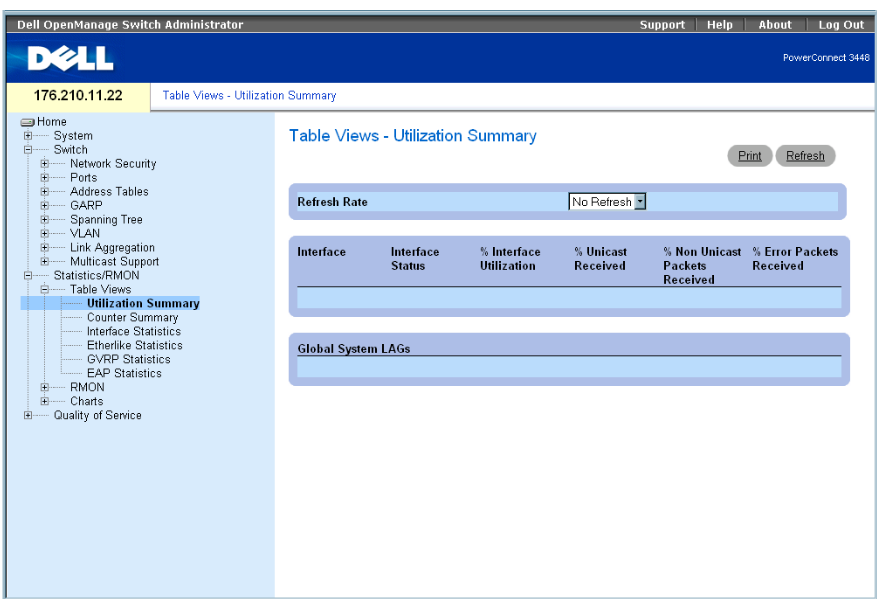
Viewing Tables

The **Table Views** page contains links for displaying statistics in a table 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 8-1. Utilization Summary



NOTE: This screen is refreshed periodically to minimize the impact on computers with lower memory. Display may be disrupted during this period.

The **Utilization Summary** page contains the following fields:

Refresh Rate—Indicates 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.

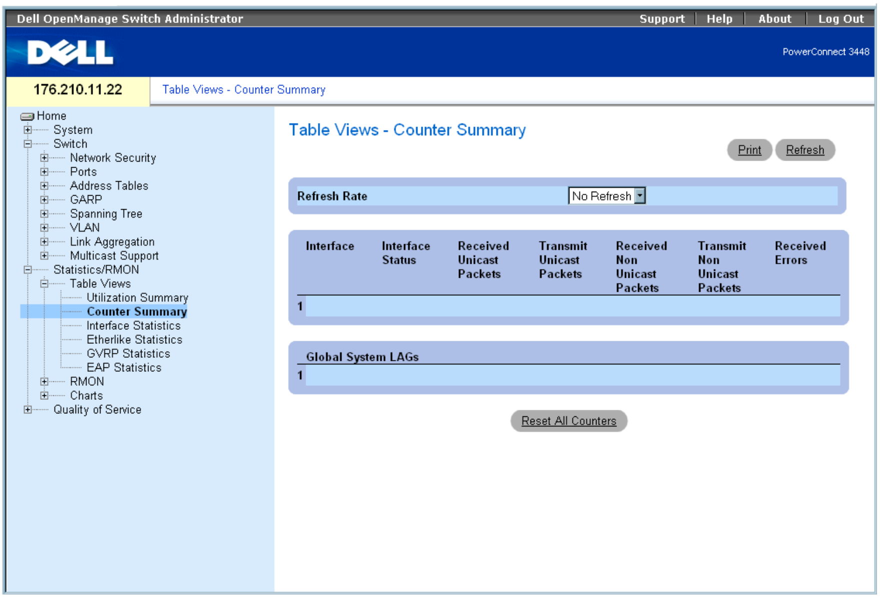
% Error Packets Received — Percentage of packets with errors received on the interface.

Global System LAGs — Indicates the current global LAG utilization.

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 8-2. Counter Summary



The **Counter Summary** page contains the following fields:

Refresh Rate — Indicates the amount of time that passes before the interface statistics are refreshed.

Interface — The interface number.

Interface Status — Status of the interface.

Received Unicast Packets — Number of received Unicast packets on the interface.

Transmit Unicast Packets — Number of transmitted Unicast packets from the interface.

Received Non Unicast Packets — Number of received non-Unicast packets on the interface.

Transmit Non Unicast Packets — Number of transmitted non-Unicast packets from the interface.

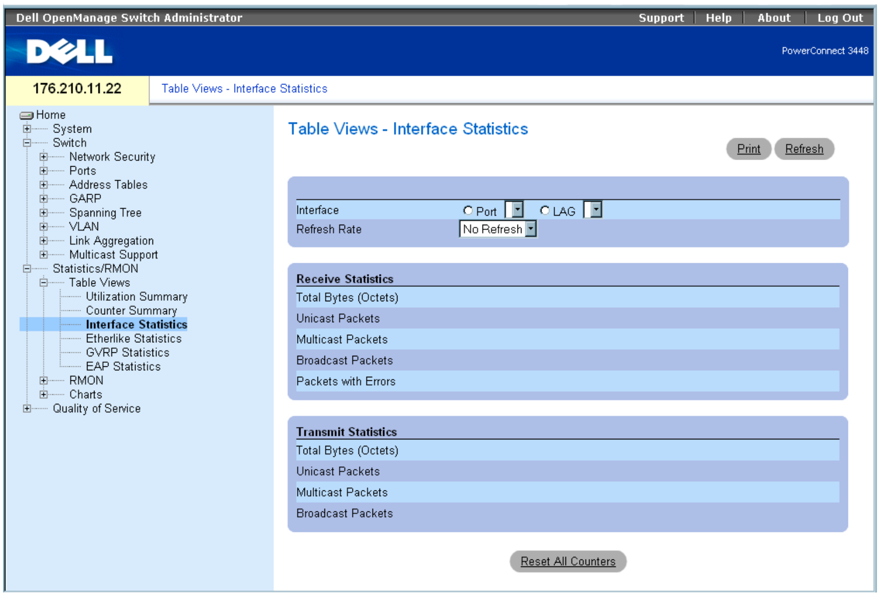
Received Errors — Number of received packets with errors on the interface.

Global System LAGs — Provides a counter summary for global system LAGs.

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 8-3. Interface Statistics



The **Interface Statistics** page contains the following fields:

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) — Amount of octets received on the selected interface.

Unicast Packets — Amount of Unicast packets received on the selected interface.

Multicast Packets — Amount of Multicast packets received on the selected interface.

Broadcast Packets — Amount of Broadcast packets received on the selected interface.

Transmit Statistics

Total Bytes (Octets) — Amount of octets transmitted from the selected interface.

Unicast Packets — Amount of Unicast packets transmitted from the selected interface.

Multicast Packets — Amount of Multicast packets transmitted from the selected interface.

Broadcast Packets — Amount of Broadcast packets 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 for the selected interface 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 contains the CLI commands for viewing interface statistics.

Table 8-95. Interface Statistics CLI Commands

CLI Command	Description
show interfaces counters [**ethernet** *interface* | **port-channel** *port-channel-number*]	Displays traffic seen by the physical interface.

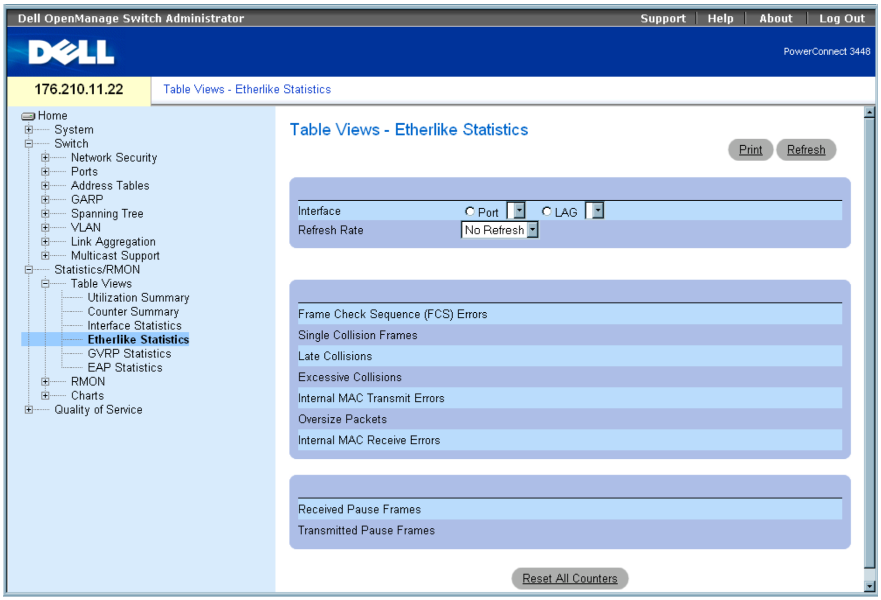
The following is an example of the CLI commands.

```
console> enable
console# show interfaces counters
Port InOctets InUcastPkts InMcastPkts InBcastPkts
------------------------------------------------
1/e1   0        0           0           0
1/e2   0        0           0           0
1/e3   0        0           0           0
1/e4   0        0           0           0
1/e5   0        0           0           0
1/e6   0        0           0           0
1/e7   0        0           0           0
1/e8   0        0           0           0
1/e9   0        0           0           0
1/e10  0        0           0           0
```

Viewing Etherlike Statistics

The **Etherlike Statistics** page contains interface errors statistics. To open the **Etherlike Statistics** page, click **Statistics/RMON→Table Views→Etherlike Statistics** in the tree view.

Figure 8-4. Etherlike Statistics



The **Etherlike Statistics** page contains the following fields:

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 frame errors received on the selected interface.

Late Collisions — Number of late collisions received on the selected interface.

Oversize Packets — Number of oversize packets on the selected interface.

Internal MAC Transmit Errors — Number of internal MAC transmit errors on the selected interface.

Received Pause Frames — Number of received paused errors on the selected interface.

Transmitted Pause Frames — Number of transmitted paused errors on the selected interface.

Displaying Etherlike Statistics for an Interface

1. Open the **Etherlike Statistics** page.
2. Select an interface in the **Interface** field.

Resetting Etherlike Statistics

1. Open the **Etherlike Statistics** page.
2. Click **Reset All Counters**.

   The Etherlike Statistics counters are reset.

Viewing Etherlike Statistics Using the CLI Commands

The following table contains the CLI commands for viewing etherlike statistics.

Table 8-96. 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.

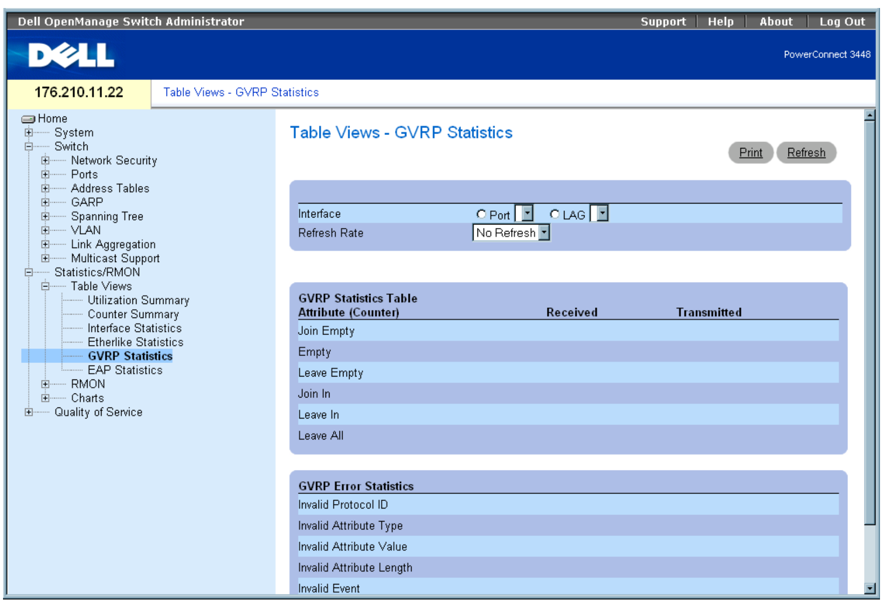
```
Console# show interfaces counters ethernet 1/1

Port      IN Octets    InUcastPkts   InMcastPkts   InBcastPkts
----      ---------    -----------   -----------   -----------
1/e1      183892       1289          987           8

Port      OUT Octets   OutUcastPkts  OutMcastPkts  OutBcastPkts
----      ----------   ------------  ------------  ------------
1/e1      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 8-5. GVRP Statistics



The **GVRP Statistics** page contains the following fields:

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.

Leave Empty — Device GVRP Leave Empty statistics.

Empty — Indicates the number of empty GVRP 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 Event — 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 GVRP statistics for the selected interface are displayed.

Resetting GVRP Statistics

1. Open the **GVRP Statistics** page.
2. Click **Reset All Counters**.

   The GVRP statistics counters are reset.

Viewing GVRP Statistics Using the CLI Commands

The following table contains the CLI commands for viewing GVRP statistics.

Table 8-97. 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:

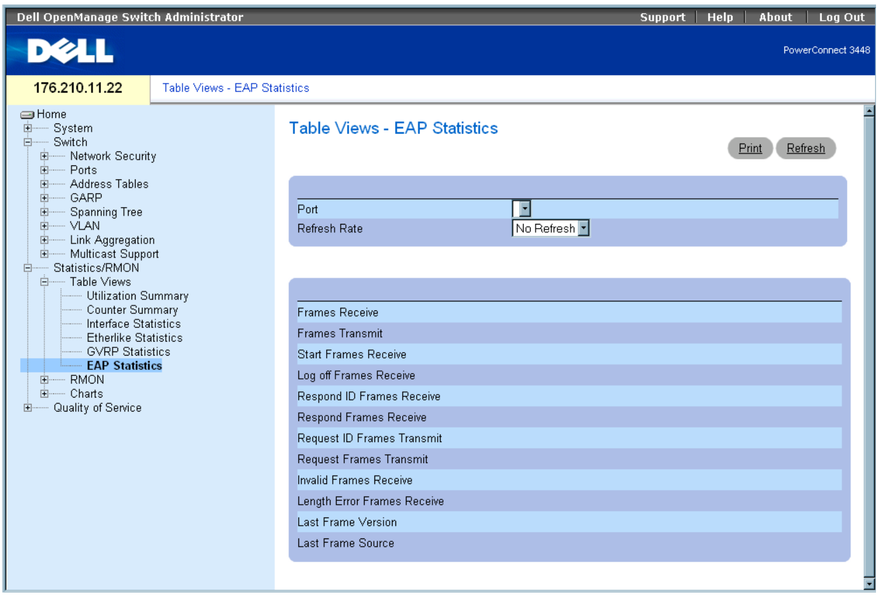
```
console# show gvrp statistics
GVRP statistics:
----------------
Legend:
rJE : Join Empty Received
rJIn : Join In Received
rEmp : Empty Received
rLIn : Leave In Received
rLE : Leave Empty Received
rLA : Leave All Received
sJE : Join Empty Sent
sJIn : Join In Sent
sEmp : Empty Sent
sLIn : Leave In Sent
sLE : Leave Empty Sent
sLA : Leave All Sent
Port rJE rJIn rEmp rLIn rLE rLA sJE sJIn sEmp sLIn sLE sLA
---- --- ---- ---- ---- --- --- --- --- --- ---- --- ---
1/e1   0   0    0    0    0   0   0   0   0   0    0   0
1/e2   0   0    0    0    0   0   0   0   0   0    0   0
1/e3   0   0    0    0    0   0   0   0   0   0   00   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 INVPLEN INVALEN INVEVENT
---- ------- ------- ------- ------- ------- -------
1/e1   0       0       0        0       0      0
1/e2   0       0       0        0       0      0
1/e3   0       0       0        0       0      0
1/e4   0       0       0        0       0      0

sLE : Leave Empty Sent
sLA : Leave All Sent
Port rJE rJIn rEmp rLIn rLE rLA sJE sJIn sEmp sLIn sLE sLA
---- --- ---- ---- ---- --- --- --- --- --- ---- --- ---
1/e1   0   0    0    0    0   0   0   0   0   0    0   0
1/e2   0   0    0    0    0   0   0   0   0   0    0   0
1/e3   0   0    0    0    0   0   0   0   0   0    0   0
1/e4   0   0    0    0    0   0   0   0   0   0    0   0
1/e5   0   0    0    0    0   0   0   0   0   0    0   0
1/e6   0   0    0    0    0   0   0   0   0   0    0   0
1/e7   0   0    0    0    0   0   0   0   0   0    0   0
1/e8   0   0    0    0    0   0   0   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 "**Configuring Port Based Authentication**". To open the **EAP Statistics** page, click **Statistics/RMON→Table Views→EAP Statistics** in the tree view.

Figure 8-6. EAP Statistics



The **EAP Statistics** page contains the following fields:

Port — Indicates the port which is polled for statistics.

Refresh Rate — Amount of time that passes before the interface statistics are refreshed.

Frames Receive — Indicates the number of valid EAPOL frames received on the port.

Frames Transmit — Indicates the number of EAPOL frames transmitted via the port.

Start Frames Receive — Indicates the number of EAPOL Start frames received on the port.

Log off Frames Receive — Indicates the number of EAPOL Logoff frames received on the port.

Respond ID Frames Receive — Indicates the number of EAP Resp/Id frames received on the port.

Respond Frames Receive — Indicates the number of valid EAP Response frames received on the port.

Request ID Frames Transmit — Indicates the number of EAP Req/Id frames transmitted via the port.

Request Frames Transmit — Indicates the number of EAP Request frames transmitted via the port.

Invalid Frames Receive — Indicates the number of unrecognized EAPOL frames that have been received on this port.

Length Error Frames Receive — Indicates the number of EAPOL frames with an invalid Packet Body Length received on this port.

Last Frame Version — Indicates the protocol version number attached to the most recently received EAPOL frame.

Last Frame Source — Indicates 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.

To reset the EAP Statistics

1. Open the **EAP Statistics** page.
2. Click **Reset All Counters**.

   The EAP statistics counters are reset.

Viewing EAP Statistics Using the CLI Commands

The following table summarizes the CLI commands for viewing EAP statistics.

Table 8-98. EAP Statistics CLI Commands

CLI Command	Description
`show dot1x statistics`	Displays 802.1X statistics for the specified interface.

The following is an example of the CLI commands:

```
console# show dot1x statistics ethernet 1/e1
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
```

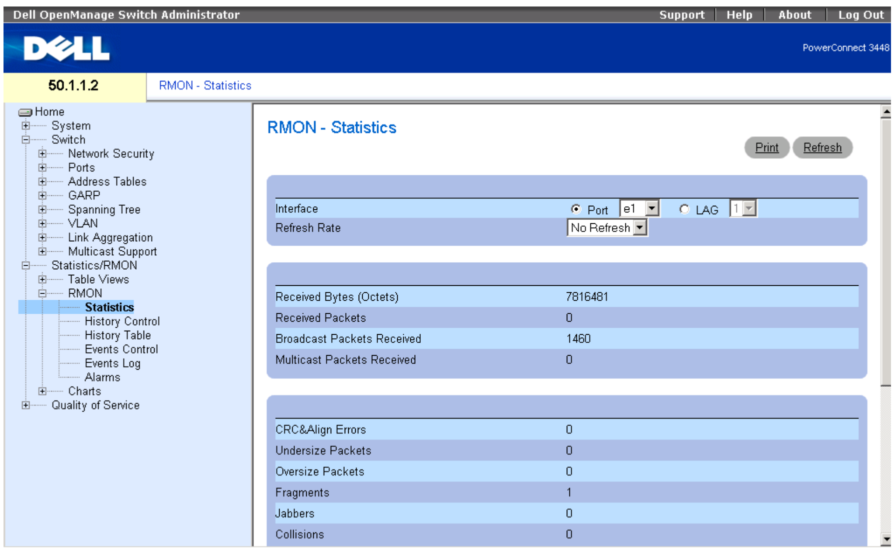
Viewing RMON Statistics

Remote Monitoring (RMON) allows network managers to view network information from a remote location. To open the **RMON** page, click **Statistics/RMON→RMON** in the tree view.

Viewing RMON Statistics Group

Use the **RMON Statistics** page view 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 8-7. RMON Statistics



The **RMON Statistics** page contains the following fields:

Interface — Specifies the port or LAG for which statistics are displayed.

Refresh Rate — Amount of time that passes before the statistics are refreshed.

Received Bytes (Octets) — Number of bytes received on the selected interface.

Received Packets — Number of packets received on the selected interface.

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 contains the CLI commands for viewing RMON statistics.

Table 8-99. RMON Statistics CLI Commands

CLI Command	Description
show rmon statistics {**ethernet** *interface* | **port-channel** *port-channel-number*}	Displays RMON Ethernet statistics.

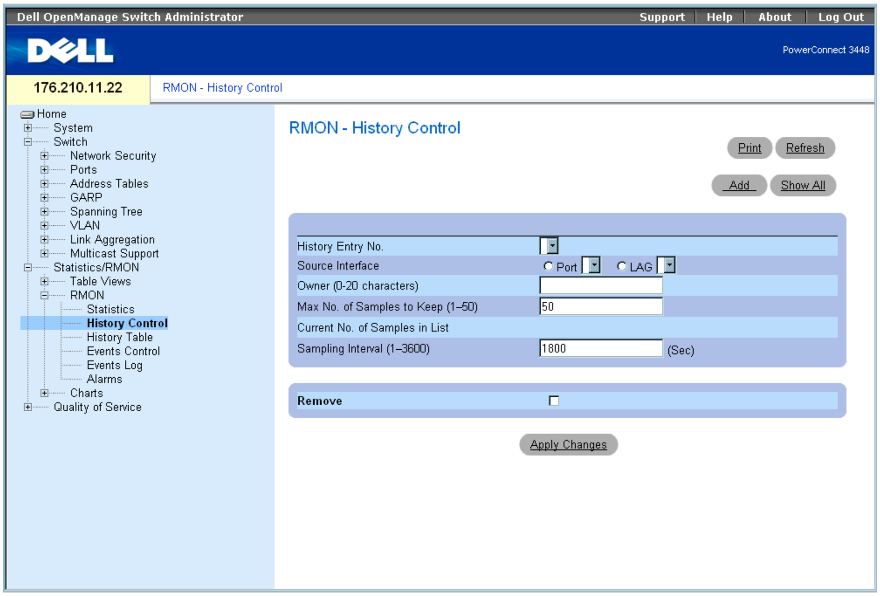
The following is an example of the CLI commands:

```
console# show rmon statistics ethernet 1/e1
Port 1/e1
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** 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→RMON→History Control** in the tree view.

Figure 8-8. RMON History Control



The **RMON History Control** page contains the following fields:

History Entry No. — Entry number for the **History Control** 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 (1-50) — Number of samples to be saved. The default value is 50.

Current No. of Samples in List — Indicates the current number of samples taken.

Sampling Interval (1-3600) —Indicates the time interval in seconds, between what the samplings are taken from the ports. The possible values are 1-3600 seconds. The default is 1800 seconds (30 minutes).

Remove — When checked, 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 desired
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 **Apply Changes**.

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

Viewing RMON History Control Using the CLI Commands

The following table contains the CLI commands for viewing RMON History Control.

Table 8-100. 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.

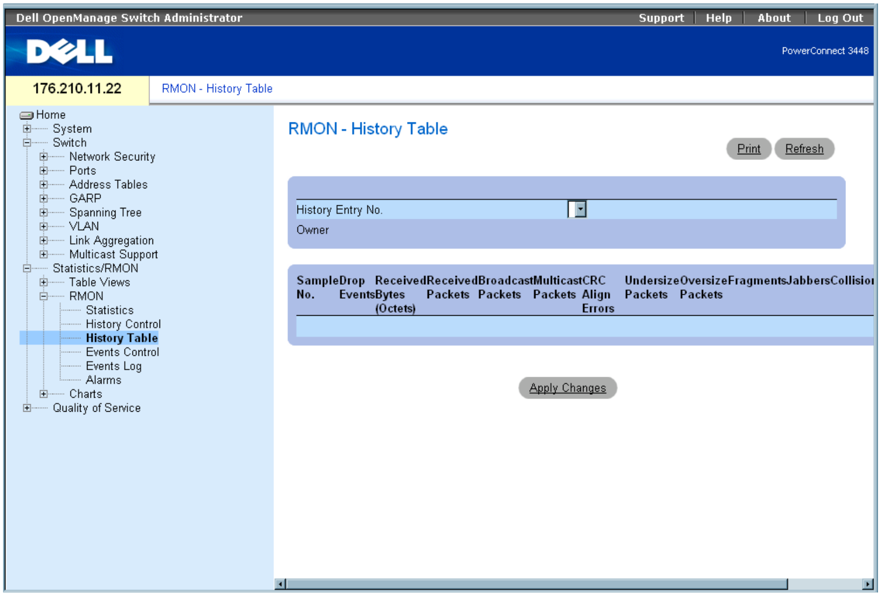
The following is an example of the CLI commands:

```
console(config)# interface ethernet 1/e8
console(config-if)# rmon collection history 1 interval 2400
```

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 8-9. RMON History Table



The **RMON History Table** page contains the following fields:

NOTE: Not all fields are shown in the RMON History Table.

History Entry No. — Specifies the entry number from the **History Control** page.

Owner — Indicates the RMON station or user that requested the RMON information.

Sample No. — Indicates the number of 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 64-1,518 octets. However, the packets has a bad packet Check Sequence (FCS) 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 1,518 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 1,518 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 port 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 hundredths of percent.

Viewing Statistics for a Specific History Entry

1. Open the **RMON History Table**.
2. Select an entry in the **History Entry No.** field.

   The entry statistics display in the RMON History Table.

Viewing RMON History Control Using the CLI Commands

The following table contains the CLI commands for viewing RMON history.

Table 8-101. RMON History Control CLI Commands

CLI Command	Description
show rmon history *index* {**throughput** | **errors** | **other**} [**period** *seconds*]	Displays RMON Ethernet statistics history.

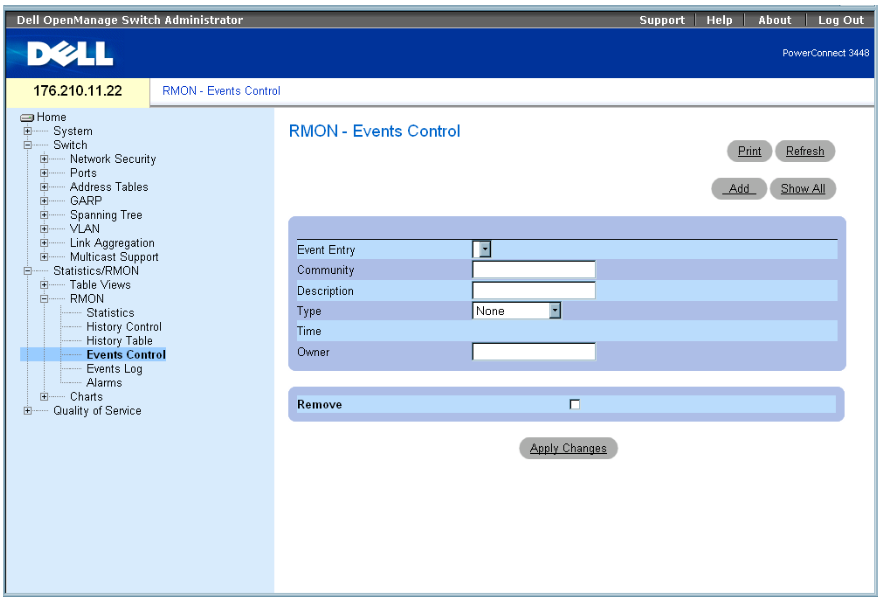
The following is an example of the CLI commands for displaying RMON ethernet statistics for throughput on index 1:

```
console> enable
console# show rmon history 1 throughput
Sample Set: 5Owner: cli
Interface: 24 interval: 10
Requested samples: 50 Granted samples: 50
Maximum table size: 270
Time                 Octets PacketsBroadcast Multicast%
------------------   ------ ---------------- --------------
09-Mar-2003 18:29:32 00     00               0
09-Mar-2003 18:29:42 00     00               0
09-Mar-2003 18:29:52 00     00               0
09-Mar-2003 18:30:02 00     00               0
09-Mar-2003 18:30:12 00     00               0
09-Mar-2003 18:30:22 00     00               0
```

Defining Device RMON Events

Use the **RMON Events Control** page to define RMON events. To open the **RMON Events Control** page, click **Statistics/RMON→RMON→Events Control** in the tree view.

Figure 8-10. RMON Events Control



The **RMON Events Control** page contains the following fields:

Event Entry — Indicates 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 — Time when the event occurred.

Owner — The device or user that defined the event.

Remove — When checked, removes the event from the **RMON Events Table**.

Adding a 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 a 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 **RMON Events Table** page opens.

3 Check the **Remove** checkbox for the event(s) that needs to be deleted and then click **Apply Changes**.

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

NOTE: A single event entry can be removed from the **RMON Events Control** page by checking the **Remove** check box on that page.

Defining Device Events Using the CLI Commands

The following table contains the CLI commands for defining device events.

Table 8-102. 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.

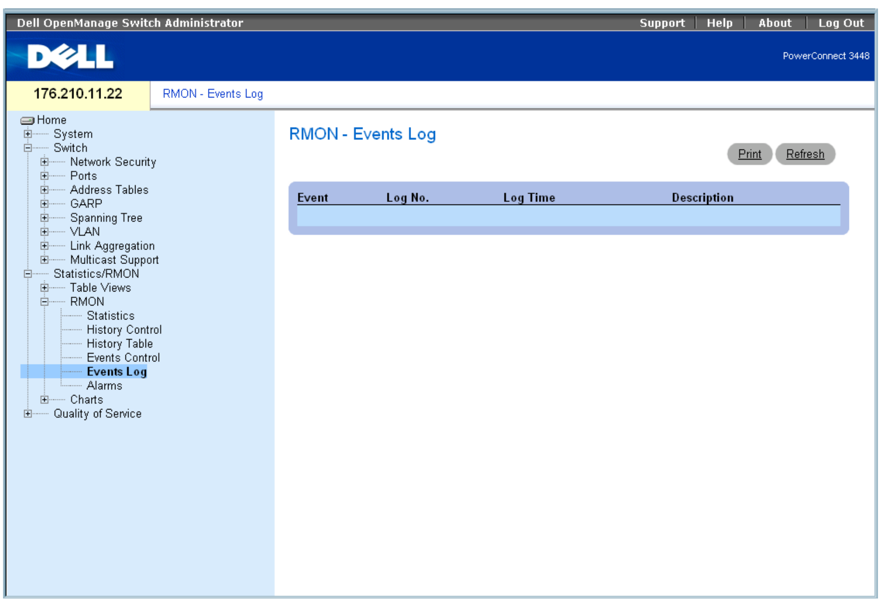
The following is an example of the CLI commands:

```
console(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
       Broadcast                                   23:59:48
```

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 Log** in the tree view.

Figure 8-11. RMON Events Log



The **RMON Events Log** page contains the following fields:

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 contains the CLI commands for defining device events.

Table 8-103. 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:

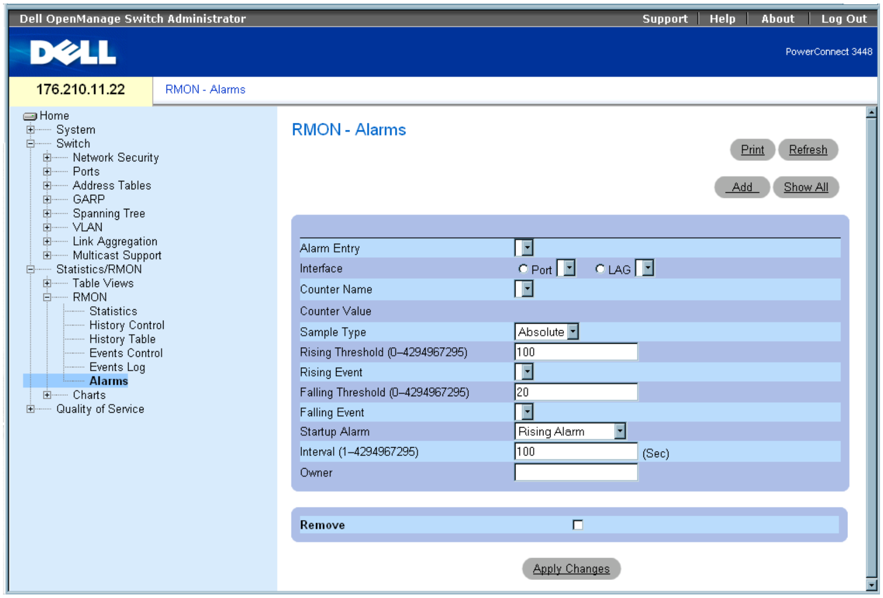
```
console(config)# rmon event 1 log

Console> show rmon log

Maximum table size: 500

Event Description     Time

----- --------------- --------------

1     Errors          Jan 18 2002 23:58:17

2     High Broadcast  Jan 18 2002 23:59:48
```

Defining RMON Device Alarms

Use the **RMON Alarms** page to set network alarms. Network alarms occur when a network problem, or event, is detected. Rising and falling thresholds generate events. For more information about events, see "Viewing the RMON Events Log."

To open the **RMON Alarms** page, click **Statistics/RMON→RMON→Alarms** in the tree view.

Figure 8-12. RMON Alarms



The **RMON Alarms** page contains the following fields:

Alarm Entry — Indicates a specific alarm.

Interface — Indicates the interface for which RMON statistics are displayed.

Counter Name — Indicates 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 (0–4294967295) — 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. The field default is 100 seconds.

Rising Event — The mechanism in which the alarms are reported including a log, a trap, or both. When a 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 a trap is selected, an SNMP trap is generated and reported via the Trap mechanism. The trap can be saved using the same mechanism.

Falling Threshold (0–4294967295) — The falling counter value that triggers the falling threshold alarm. The falling threshold is graphically presented on top of the graph bars. Each monitored variable is designated a color. The field default is 20.

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 (1–4294967295) (sec) — Alarm interval time. The field default is 100 seconds.

Owner — Device or user that defined the alarm.

Remove — When checked, removes an RMON Alarm.

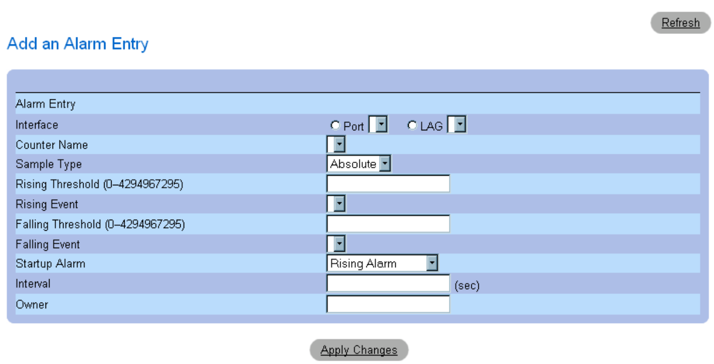
Adding an Alarm Table Entry

1 Open the **RMON Alarms** page.

2 Click **Add**.

The **Add an Alarm Entry** page opens:

Figure 8-13. Add an Alarm Entry Page



3 Select an interface.

4 Complete the fields.

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.

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** opens.

Deleting an Alarm Table Entry

1 Open the **RMON Alarms** page.
2 Select an entry in the **Alarm Entry** drop-down menu.
3 Check the **Remove** check box.
4 Click **Apply Changes**.
   The entry is deleted, and the device is updated.

Defining Device Alarms Using the CLI Commands

The following table contains the CLI commands for defining device alarms.

Table 8-104. Device Alarm CLI Commands

CLI Command	Description
rmon alarm *index MIB_Object_ID 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 the RMON alarm configuration.

The following is an example of the CLI commands:

```
console(config)# rmon alarm 1000 1.3.6.1.2.1.2.2.1.10.1 360000
1000000 1000000 10 20

Console# show rmon alarm-table

Index                       OID              Owner

------------------------------              -----

11.3.6.1.2.1.2.2.1.10.1                     CLI

21.3.6.1.2.1.2.2.1.10.1                     Manager

31.3.6.1.2.1.2.2.1.10.9                     CLI
```

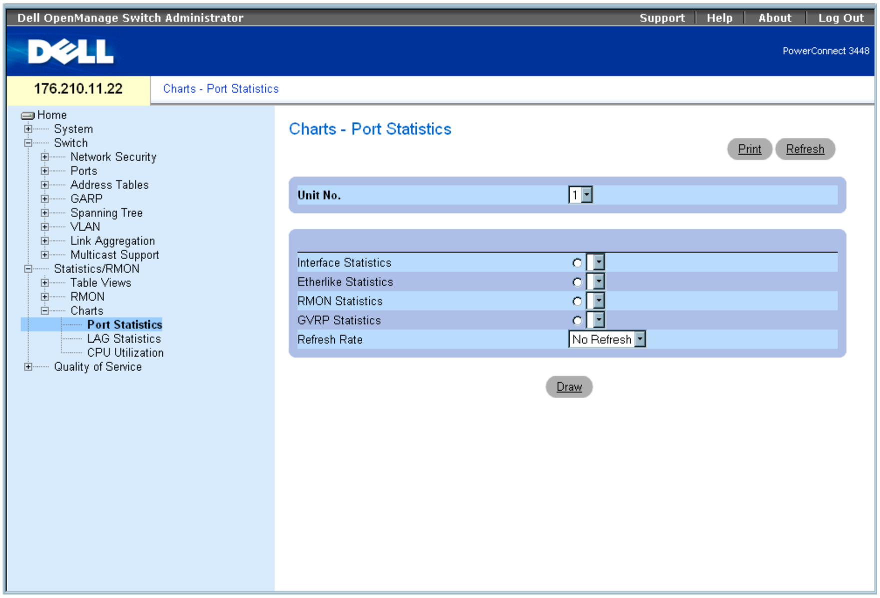
Viewing Charts

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

Use the **Port Statistics** page to open statistics in a chart form for port elements. To open the **Port Statistics** page, click **Statistics/RMON→Charts→Port Statistics** in the tree view.

Figure 8-14. Port Statistics



The **Port Statistics** page contains the following fields:

Unit No. — Indicates the stacking unit for which the statistics are displayed.

Interface Statistics — Selects the interface statistics to display.

Etherlike Statistics — Selects the Etherlike statistics to display.

RMON Statistics — Selects the RMON statistics to display.

GVRP Statistics — Selects the GVRP statistics type to display.

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 of 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 contains the CLI commands for viewing port statistics.

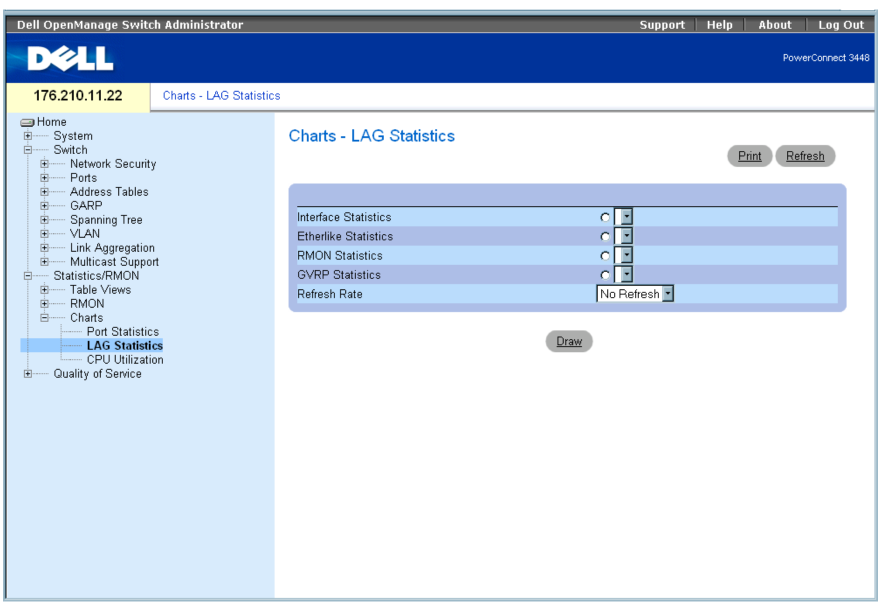
Table 8-105. Port Statistic CLI Commands

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.

Viewing LAG Statistics

Use the **LAG Statistics** page to open statistics in a chart form for LAGs. To open the **LAG Statistics** page, click **Statistics/RMON→Charts→LAG Statistics** in the tree view.

Figure 8-15. LAG Statistics



The **LAG Statistics** page contains the following fields:

Interface Statistics — Selects the interface statistics to display.

Etherlike Statistics — Selects the Etherlike statistics to display.

RMON Statistics — Selects the RMON statistics to display.

GVRP Statistics — Selects the GVRP statistics type to display.

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 contains the CLI commands for viewing LAG statistics.

Table 8-106. LAG Statistic CLI Commands

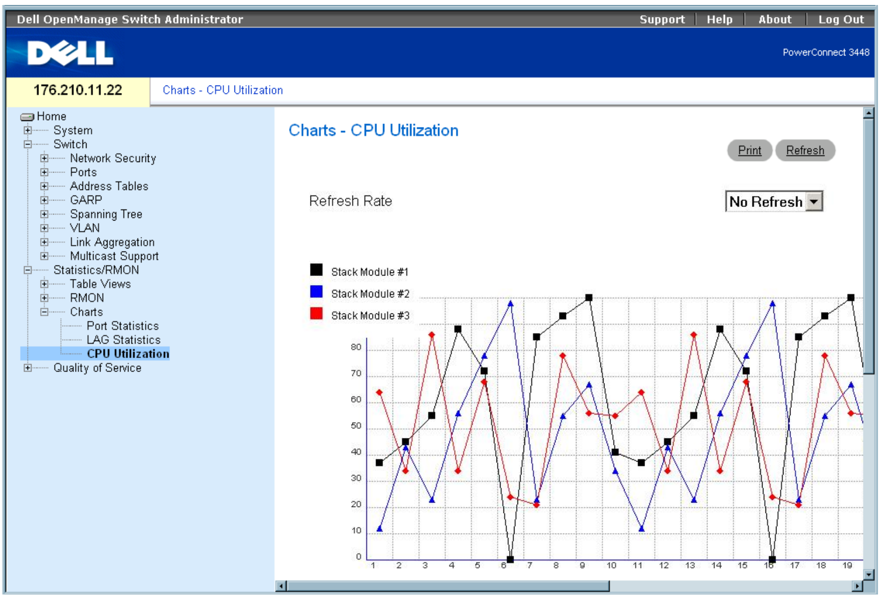
CLI Command	Description
show interfaces counters [**ethernet** *interface* | **port-channel** *port-channel-number*]	Displays traffic seen by the physical interface.
show rmon statistics {**ethernet** *interface* | **port-channel** *port-channel-number*}	Displays RMON Ethernet statistics.
show gvrp statistics {**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.

Viewing the CPU Utilization

The **CPU Utilization** page contains information about the system's CPU utilization and percentage of CPU resources consumed by each stacking member. Each stacking member is assigned a color on the graph.

To open the **CPU Utilization** page, click **Statistics/RMON→Charts→CPU Utilization** in the tree view.

Figure 8-16. CPU Utilization



The **CPU Utilization** page contains the following information:

Refresh Rate — Amount of time that passes before the statistics are refreshed.

9

Configuring Quality of Service

This section provides information for defining and configuring Quality of Service (QoS) parameters. To open the **Quality of Service** page, 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.

An implementation example that requires QoS includes 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 tag (VPT) and DSCP (DiffServ Code Point).

VPT Classification Information

VLAN Priority Tags are used to classify the packets by mapping packets to one of the egress queues. VLAN Priority Tag to queue assignments are user-definable. The table below details the VPT to queue default settings:

Table 9-107. CoS to Queue Mapping Table Default values

CoS Value	Forwarding Queue Values
0	q1 (Lowest Priority)
1	q1 (Lowest Priority)
2	q1(Lowest Priority)
3	q1 (Lowest Priority)
4	q2
5	q2
6	q3
7	q3

NOTE: In a stacking configuration, Queue 4 is used for forwarding stacking traffic. Therefore, assigning additional traffic to Queue 4 may interfere with traffic forwarding.

Packets arriving untagged are assigned a default VPT value, which is set on a per port basis. The assigned VPT is used to map the packet to the egress queue.

DSCP values can be mapped to priority queues. The following table contains the default DSCP mapping to egress queue values:

Table 9-108. DSCP to Queue Mapping Table Default Values

DSCP Value	Forwarding Queue Values
0-15	q1 (Lowest Priority)
16-39	q2
40-63	q3

DSCP mapping is enabled on a per-system basis.

CoS Services

After packets are assigned to a specific egress queue, CoS services can be assigned to the queue(s). Egress queues are configured with a scheduling scheme by one of the following methods:

- **Strict Priority** — Ensures that time-sensitive applications are always forwarded. Strict Priority (SP) allows the prioritization of mission-critical, time-sensitive traffic over less time-sensitive applications.
  For example, under Strict Priority, voice over IP traffic can be prioritized so the IP traffic is forwarded before FTP or e-mail (SMTP) traffic.
- **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. All queues can participate in WRR, with expect SP queues.
  SP queues are serviced before WRR queues. If the traffic flow is minimal, and SP queues do not occupy the whole bandwidth allocated to a port, the WRR queues can share the bandwidth with the SP queues. Ensuring the remaining bandwidth is distributed according to the weight ratio. If WRR is selected, the following weights are assigned to the queues: 1, 2, 4, 8.

Defining QoS Global Parameters

The **QoS Parameters** page contains links to pages that enable setting Quality of Service global parameters.

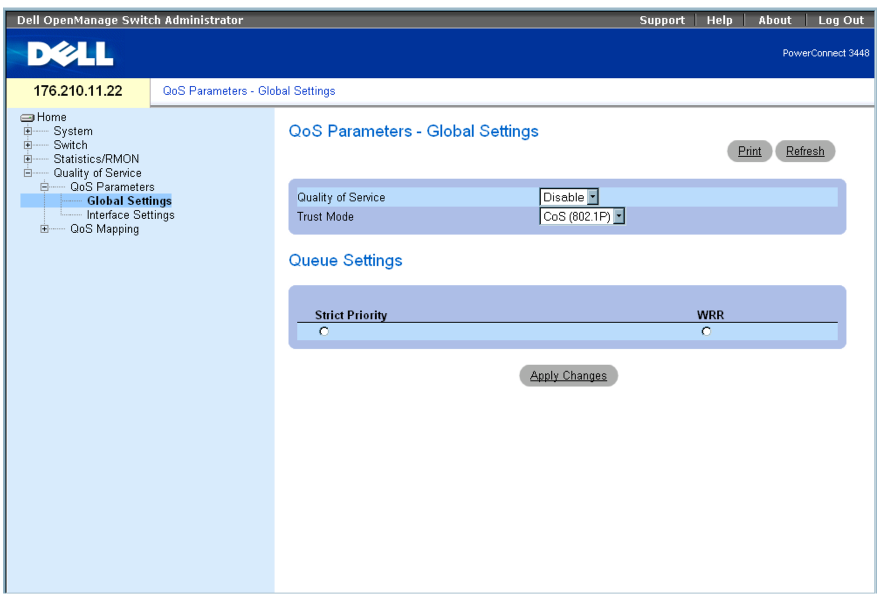
Configuring QoS Global Settings

The **Global Settings** page contains a field for enabling or disabling QoS. It also contains a field for selecting the Trust mode. The Trust mode relies on predefined fields within the packet to determine the egress queue.

In addition, the **Global Settings** page enables defining queues as either Strict Priority (SP) or Weighted Round Robin (WRR).

To open the **Global Settings** page, click **Quality of Service→QoS Parameters →Global Settings** in the tree view.

Figure 9-1. Global Settings



The **Global Settings** page contains the following sections:

- QoS Settings
- Queue Settings

QoS Settings

Quality of Service — Enables or disables managing network traffic using Quality of Service.

Trust Mode — Determines which packet fields are used to classify packets entering the device. When no rules are defined, the traffic containing the predefined CoS or DSCP packet field is mapped according to the selected trust mode. Traffic not containing a predefined packet field is mapped to the best effort queue (q2). The possible Trust Mode field values are:

> **CoS** (802.1p) — The egress queue assignment is determined by the IEEE802.1p VLAN priority tag (VPT) or by the default VPT assigned to a port. The device default is the IEEE802.1p.
>
> **DSCP** — The egress queue assignment is determined by the DSCP field.

NOTE: The interface Trust settings overrides the global Trust setting.

Queue Settings

Strict Priority — Indicates the system queues are SP queues, when selected.

WRR — Indicates the system queues are WRR queues, when selected.

Enabling Quality of Service:

1. Open the **Global Settings** page.
2. Select **Enable** in the **Quality of Service** field.
3. Click **Apply Changes**.

   Class of Service is enabled on the device.

Enabling the Trust Mode:

1. Open the **Global Settings** page.
2. Define the **Trust Mode** field.
3. Click **Apply Changes**.

   Trust mode is enabled on the device.

Enabling Trust Using the CLI Commands

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

Table 9-109. QoS Settings CLI Commands

CLI Command	Description
qos trust [cos | dscp]	Configures the system to trust mode.
no qos trust	Returns to the non-trusted state.

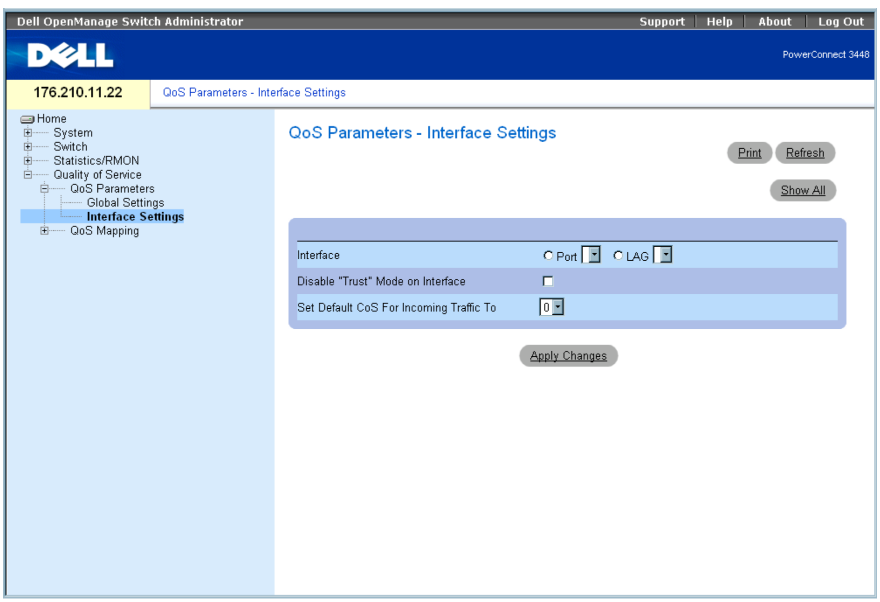
The following is an example of the CLI commands:

```
console(config)# qos trust dscp
```

Defining QoS Interface Settings

The **Interface Settings** page contains fields for deactivating the Trust mode, and setting the default CoS value on incoming untagged packets. To open the **Interface Settings** page, click **Quality of Service→QoS Parameters →Interface Settings** in the tree view.

Figure 9-2. Interface Settings



The **Interface Settings** page contains the following fields:

Interface — The specific port or LAG to configure.

Disable "Trust" Mode on Interface — Disables Trust mode on the specified interface. This setting overrides the Trust mode configured on the device globally.

Set Default CoS For Incoming Traffic To — Sets the default CoS tag value for untagged packets. The CoS tag values are 0-7. The default value is 0.

Assigning QoS settings for an interface:

1. Open the **Interface 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.

Displaying QoS/CoS settings:

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

   The Interface Table is displayed.

Assigning QoS Interfaces Using the CLI Commands

The following table summarizes the equivalent CLI commands for configuring fields in the **Interface Settings** page.

Table 9-110. QoS Interface CLI Commands

CLI Command	Description
qos trust	Enables the trust mode.
no qos trust	Disables Trust state on each port.

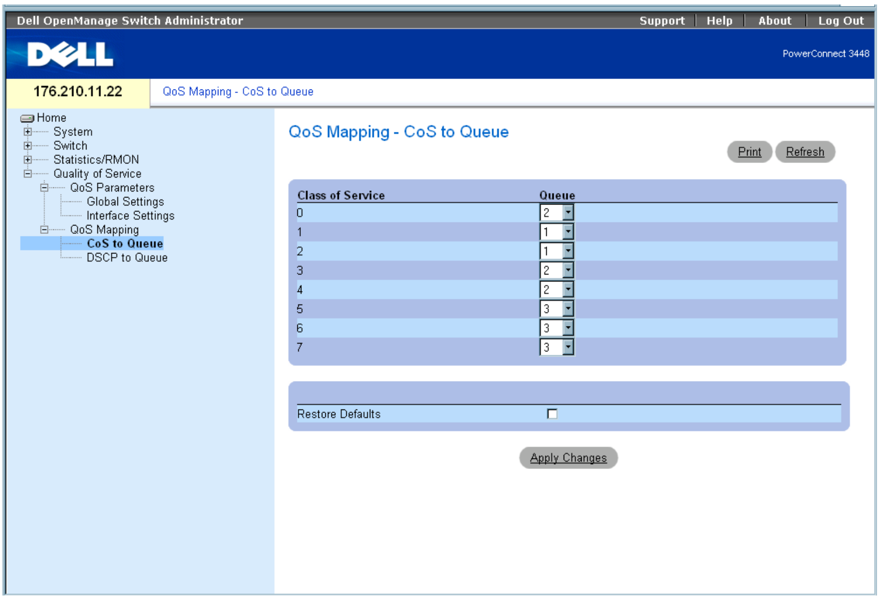
The following is an example of the CLI commands:

```
console(config)# interface ethernet 1/e15
console(config-if)# qos trust
```

Mapping CoS Values to Queues

The **CoS to Queue** page contains fields for classifying CoS settings to traffic queues. To open the **CoS to Queue** page, click **Quality of Service→QoS Mapping→CoS to Queue** in the tree view.

Figure 9-3. CoS to Queue



The **CoS to Queue** page contains the following fields:

Class of Service — Specifies the CoS priority tag values, where zero is the lowest and 7 is the highest.

Queue — The 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 an egress queue.

Mapping a CoS Value to a Queue

1. Open the **CoS to Queue** 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 an egress 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** page.

Table 9-111. CoS to Queue Settings CLI Commands

CLI Command	Description
wrr-queue cos-map *queue-id cos0.cos7*	Maps assigned CoS values to the egress queues.

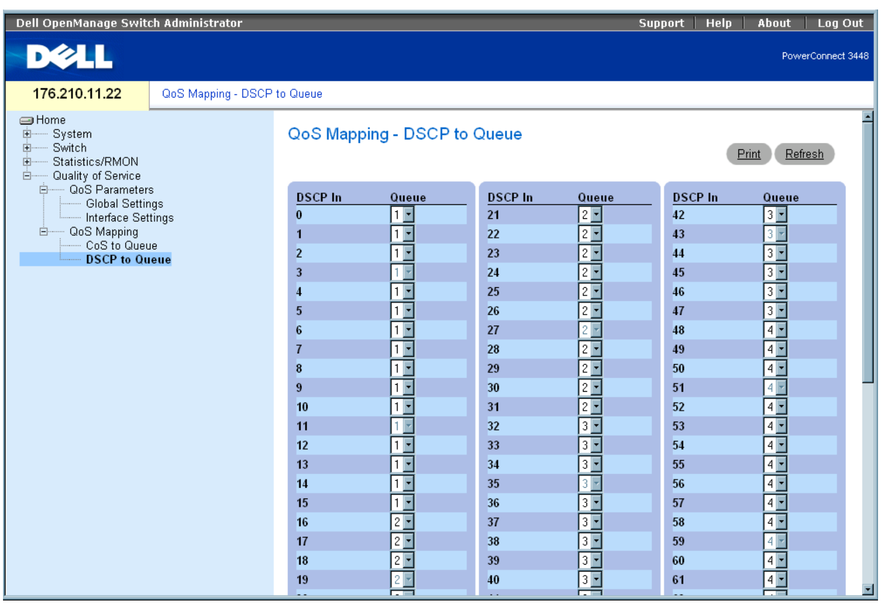
The following is an example of the CLI commands:

```
console(config)# wrr-queue cos-map 4 7
```

Mapping DSCP Values to Queues

The **DSCP to Queue** page provides fields for defining egress queue to specific DSCP fields. To open the **DSCP to Queue** page, click **Quality of Service→QoS Mapping→DSCP to Queue** in the tree view.

Figure 9-4. DSCP to Queue



The **DSCP to Queue** page contains the following fields:

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 1 is the lowest value and 4 is the highest.

Mapping a DSCP Value and Assigning a Priority Queue

1. Open the **DSCP to Queue** page.
2. Select a value in the **DSCP In** column.
3. Define the **Queue** field.
4. Click **Apply Changes**.

   The DSCP is overwritten, and the value is assigned an egress queue.

Assigning DSCP Values Using the CLI Commands

The following table summarizes the equivalent CLI commands for configuring fields in the **DSCP to Queue** page.

Table 9-112. 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 Feature Interaction Information

The following table contains information about feature interactions

Feature	Feature Notes
802.1x Unauthenticated VLAN	802.1x Unauthenticated VLANs have restricted functionality with: • 802.1X Guest VLAN • Private VLAN • Isolated VLAN • Community VLAN • Special VLAN
802.1x Unauthenticated VLAN Port	802.1X Unauthenticated VLAN Ports have restricted functionality with: • Isolated Ports • Community Ports • Promiscuous Ports • MAC based VLAN ports • Ingress Filtering
ACL	ACL functionality is restricted with: • MAC Based ACLs • Special VLANs
Auto-negotiation	No feature interaction restrictions or limitations.
Back Pressure Support	
Bridge Multicast Filtering	No feature interaction restrictions or limitations.
Cable Tests	No feature interaction restrictions or limitations.
Community ports	Community ports have restricted functionality with Locked Ports.
Community VLAN	Community VLANs have restricted functionality with: • Static MAC addresses • ACLs • GVRP • IGMP Snooping • Special VLANs
DNS	No Restrictions or limitations.

Feature	Feature Notes
Duplex Mode	
Flow Control	No feature interaction restrictions or limitations.
GARP	No feature interaction restrictions or limitations.
Guest VLANs	Guest VLANs cannot function with: • Private VLAN • Isolated VLAN • Community VLAN • MAC Based VLANs • Special VLANs
GVRP	No feature interaction restrictions or limitations.
IGMP Snooping	No feature interaction restrictions or limitations.
Ingress Filtering	No feature interaction restrictions or limitations.
Isolated Port	Isolated Ports cannot function with: • Community Ports • Promiscuous Ports • Port Lock • GVRP • MAC based ACLs • Ingress Filtering
Isolated VLAN	Isolated VLANs cannot function with: • Community VLANs • Static MAC Addresses • ACLs • GVRP • IGMP Snooping • Special VLANs
LAG Statistics	No feature interaction restrictions or limitations.
Link Aggregation	No feature interaction restrictions or limitations. However, this feature has several guidelines for configuring Link Aggregation. For all the feature guidelines, see "Defining LAG Parameters".
Locked Ports	‘Locked port functionality is restricted with: • MAC Based ACLs • Ingress Filtering
Logging	No feature interaction restrictions or limitations.
MAC Address Support	No feature interaction restrictions or limitations.

Feature	Feature Notes
MDI/MDIX Decection	No feature interaction restrictions or limitations.
Multicast Filtering	No feature interaction restrictions or limitations.
Multiple Hosts	802.1X Standard (multiple hosts) cannot function with: • Isolated Port • MAC Based VLAN Port
Multiple Spanning Tree	Multiple Spanning Tree cannot function with: • Isolated Port • Ingress Filtering
Port Based Authentication	Port based authentication has limited or restricted functionality with: • 802.1 Single • Isolated Port • Locked Ports • MAC Based VLANs • Ingress Ports
Port Mirroring	No feature interaction restrictions or limitations. However, this feature has several guidelines for configuring Storm Control. For all the feature guidelines, see "Defining Port Mirroring Sessions".
Port Statistics	No feature interaction restrictions or limitations
Private VLAN	Private VLANs cannot function with: • Isolated Ports • Community Ports • GVRP • IGMP Snooping • Special VLAN
Private VLAN	Private VLANs are limited or restricted functionality with: • Isolated VLANs • GVRP • IGMP Snooping • Special VLAN
Promiscuous Ports	Promiscuous Ports cannot function with: • Locked Ports • GVRP • MAC Based VLAN Ports
Quality of Service	No feature interaction restrictions or limitations.
RMON Statistics	No feature interaction restrictions or limitations.
SNMP Authentication Notifications	No feature interaction restrictions or limitations.

Feature	Feature Notes
SNMP Notifications	No feature interaction restrictions or limitations.
SNTP Authentication	No feature interaction restrictions or limitations.
Spanning Tree	No feature interaction restrictions or limitations.
Special VLAN	No feature interaction restrictions or limitations
Static MAC	No feature interaction restrictions or limitations
Storm Control	No feature interaction restrictions or limitations
System Logs	No feature interaction restrictions or limitations
System Time Synchronization	No feature interaction restrictions or limitations.
Unauthenticated VLAN Ports	Unauthenticated VLAN Ports have restricted functionality with: • Isolated Ports • Community Ports • Promiscuous Ports • GVRP • MAC Based VLAN ports • Ingress Filtering

11

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 switch module. Access to management functions can be limited to user groups, which are defined by the following criteria:

- Ingress interfaces
- Source IP address 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 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 switch module 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 switch module.

Backup Configuration Files

Contains a backup copy of the switch module configuration. The Backup file changes when the Running Configuration file or the Startup configuration 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 switch modules, bandwidth is defined in Bits per Second (bps) or Bytes per Second.

Bandwidth Assignments

The amount of bandwidth assigned to a specific application, user, 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 switch module.

BPDU

Bridge Protocol Data Unit. Provide bridging information in a message format. BPDUs are sent across switch module 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

device 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.

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

A device 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.

DRAC/MC

DRAC/MC. Provides a single point of control for Dell Modular Server System components.

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 device s, 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.

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 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 configuration file commands, as well as all commands entered during the current session. After the switch module 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. 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. Permits logging to another computer over a network, execute commands on a remote machine, and move files from one machine to another. Secure Shell provides strong authentication and secure communications methods over insecure channels.

Startup Configuration

Retains the exact switch module configuration when the switch module 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 switch module 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

T

U

V

W