

Dell™ PowerConnect™
28xx Systems
User Guide

Notes, Notices, and Cautions



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



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



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

Information in this document is subject to change without notice.

© 2008 Dell Inc. All rights reserved.

Reproduction in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: *Dell*, *Dell OpenManage*, the *DELL* logo, *Inspiron*, *Dell Precision*, *Dimension*, *OptiPlex*, *PowerConnect*, *PowerApp*, *PowerVault*, *Axim*, *DellNet*, and *Latitude* are trademarks of Dell Inc. *Microsoft* and *Windows* are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

December 2008

Rev. A00

Contents

1	Introduction	9
	System Description	9
	PowerConnect 2808	9
	PowerConnect 2816	9
	PowerConnect 2824	10
	PowerConnect 2848	10
	Summary of PowerConnect Models	11
	Features	11
	General Features	11
	MAC Address Supported Features	13
	Layer 2 Features	13
	VLAN Supported Features	14
	Spanning Tree Protocol Features	15
	Class of Service (CoS) Features	16
	Ethernet Switch Management Features	16
2	Hardware Description	17
	Switch Port Configurations	17
	PowerConnect 28xx Front and Back Panel Port Description	17
	Physical Dimensions	21
	LED Definitions	21
	Power LED	22
	Managed Mode LED	22
	Fan LED (2824/2848 only)	22
	Port LEDs	22
	Managed Mode Button	23
	Switch Ventilation Fan	23
	Cables, Port Connections, and Pinout Information	24
	1000BASE-T Cable Requirements	24
	RJ-45 Connections for 10/100/1000BASE-T Ports	24
	SFP Ports	25

	Power Connectors	26
	Internal Power Supply Connector	26
3	Installing the PowerConnect Device	27
	Installation Precautions	27
	Site Requirements	28
	Unpacking	28
	Package Contents.	28
	Unpacking the Device	28
	Mounting the Device.	29
	Overview	29
	Device Rack Installation	29
	Installing on a Flat Surface	30
	Installing on a Wall	31
	Connecting the Device.	32
	Connecting the Device to the Network	32
	Connecting the Terminal to the Device	33
	Connecting a Device to a Power Supply	34
	Port Connections, Cables, and Pinout Information	35
	RJ-45 Connections for 10/100/1000BaseT Ports	35
	Port Default Settings	36
	Auto-Negotiation	36
	MDI/MDIX.	36
	Flow Control.	36
	Back Pressure	36
	Switching Port Default Settings	37
4	Starting and Configuring the Device	39
	Booting the Device - Managed Mode	40
	Initial Configuration - Managed Mode	41
	Advanced Configuration	44
	Retrieving an IP Address From a DHCP Server	45

Startup Procedures	45
Startup Menu Procedures	45
Software Download	46
Erase FLASH File	46
Erasing the Device Configuration	47
Password Recovery	47
Software Download Through TFTP Server	47
Management Modes	49
Default Values	49
Transitioning Between Modes	50
Returning to Managed Mode	51
5 Using Dell OpenManage Switch Administrator	53
Understanding the Interface	53
Device Representation	54
Using the Switch Administrator Buttons	55
Information Buttons	55
Device Management Buttons	56
Starting the Application	56
Access Levels	56
6 Configuring System Information	59
Defining General Device Information	59
Viewing Device Information	59
Viewing the Versions Page	61
Resetting the Device	62
Entering Secure Mode	63
Defining Device IP Addresses	64
Defining IP Interface Parameters	64
Running Cable Diagnostics	65
Viewing Copper Cable Diagnostics	65
Viewing Optical Transceiver Diagnostics	67
Managing Device Security	69
Defining the Local User Databases	69

Configuring RADIUS Global Parameters	71
Defining SNMP Parameters	74
Defining SNMP Global Parameters.	75
Defining Communities.	76
Defining SNMP Notification Recipients	78
Managing Files.	80
Downloading Files	80
Uploading Files	82
Restoring Default Settings	83
Defining DHCP Server Settings	83
Configuring DHCP Properties.	84
Defining Network Pool	85
Excluding Addresses	87
Manually Allocating IP Addresses (Static Hosts)	89
Configuring Address Binding	92
Defining Advanced Settings.	93
Configuring General Device Parameters.	93
7 Configuring Device Switching.	95
 Configuring Network Security.	95
Configuring Port Based Authentication	96
Configuring Advanced Port Based Authentication.	100
Authenticating Users	102
 Configuring Ports.	103
Defining Port Parameters	103
Aggregating Ports.	105
Configuring Green Ethernet.	108
Enabling Storm Control	110
Defining Port Mirroring Sessions.	112
 Configuring Address Tables	114
Viewing Dynamic Addresses	114
 Configuring the Spanning Tree Protocol	116
Defining STP Global Settings	116
Defining STP Port Settings	119
Defining STP LAG Settings	122

	Configuring Rapid Spanning Tree.	124
	Configuring VLANs.	126
	Defining VLAN Members	126
	VLAN Port Membership Table	128
	Defining VLAN Ports Settings.	130
	Defining VLAN LAG Settings	131
	Aggregating Ports	133
	Defining LAG Membership	134
	Multicast Forwarding Support.	134
	Defining Multicast Global Parameters	135
	Adding Bridge Multicast Address Members	136
	Assigning Multicast Forward All Parameters	138
	IGMP Snooping	141
8	Viewing Statistics	143
	Viewing RMON Statistics	144
	Viewing RMON Statistics Group	144
	Viewing Charts.	145
	Viewing the CPU Utilization.	146
9	Configuring Quality of Service.	147
	Defining CoS Global Parameters	149
	Defining QoS Interface Settings.	150
	Defining Queue Settings.	151
	Mapping CoS Values to Queues	153
	Mapping DSCP Values to Queues	154
A	Managing the Device Using the CLI.	157
	Accessing the Device Through the CLI	157
	Console Connection.	157
	Telnet Connection.	157

Using the CLI	158
Command Mode Overview	158
User EXEC Mode	158
Privileged EXEC Mode	159
Global Configuration Mode	159
Interface Configuration Mode	160
CLI Commands	161
Command: asset-tag	161
Command: copy	161
Command: debug-mode	162
Command: do	163
Command: end	163
Command: exit (configuration)	163
Command: exit (EXEC)	164
Command: help	164
Command: interface ethernet	165
Command: interface port-channel	165
Command: interface vlan	166
Command: ip address	166
Command: ip default-gateway	167
Command: login	167
Command: ping	167
Command: reload	169
Command: show tech-support command	169
Command: snmp-server community	171
Command: username	172
Glossary	173
Index	183

Introduction

This User's Guide contains the information needed for installing, configuring and maintaining the PowerConnect 2808, PowerConnect 2816, PowerConnect 2824, and PowerConnect 2848 Web-managed Gigabit Ethernet switches.

The PowerConnect 28xx switches can be used to connect workstations and other network devices, such as:

- Servers
- Hubs
- Routers

The PowerConnect devices are primarily designated for the Small Office/Home Office (SOHO) that require high performance edge connectivity. These PowerConnect devices are ideal for the small to medium business that requires high performance network connectivity along with advanced web management features. The PowerConnect management features are designed to minimize administrative management effort, while enhancing and improving network traffic control.

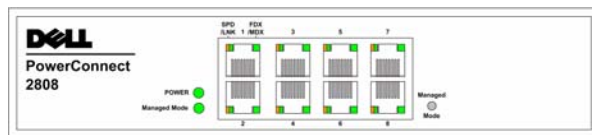
System Description

This section describes the hardware configurations of the PowerConnect 28xx. The switches are managed by Dell's OpenManage Switch Administrator.

PowerConnect 2808

The following figure illustrates the PowerConnect 2808 front panel.

Figure 1-1. PowerConnect 2808 Front Panel



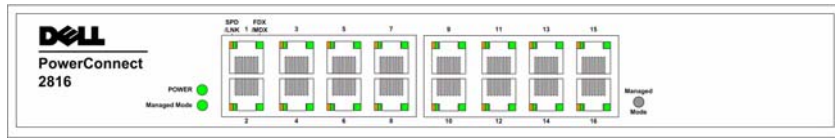
The PowerConnect 2808 supports the following ports:

- 8 Gigabit Ethernet copper ports

PowerConnect 2816

The following figure illustrates the PowerConnect 2816 front panel.

Figure 1-2. PowerConnect 2816 Front Panel



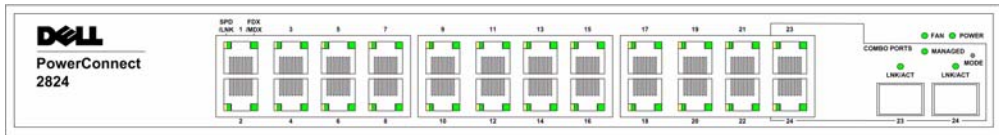
The PowerConnect 2816 supports the following ports:

- 16 Gigabit Ethernet copper ports

PowerConnect 2824

The following figure illustrates the PowerConnect 2824 front panel.

Figure 1-3. PowerConnect 2824 Front Panel



The PowerConnect 2824 supports the following ports:

- 24 Gigabit Ethernet copper ports
- 2 SFP combo ports (1000BASE-SX or 1000BASE-LX)

PowerConnect 2848

The following figure illustrates the PowerConnect 2848 front panel.

Figure 1-4. PowerConnect 2848 Front Panel



The PowerConnect 2848 supports the following ports:

- 48 Gigabit Ethernet copper ports
- 4 SFP combo ports (1000BASE-SX or 1000BASE-LX)

Summary of PowerConnect Models

The following table summarizes the PowerConnect models.

Table 1-1. PowerConnect Models

Model	Copper Ports/ RJ-45 Connectors	Optical Ports/ GbE	RS232 serial port - baud rate is 9600 bps	Fans
PowerConnect 2808	8 built-in 10/100/1000 Base-T ports	none	Internal console port	none
PowerConnect 2816	16 built-in 10/100/1000 Base-T ports	none	External console port	none
PowerConnect 2824	24 built-in 10/100/1000 Base-T ports	2 SFP (combo)	External console port	1
PowerConnect 2848	48 built-in 10/100/1000 Base-T ports	4 SFP (combo)	External console port	2

Features

General Features

Management Modes

The device supports the following modes:

- **Managed Mode** — Provides switch management through the web interface.
- **Unmanaged Mode** — In this mode, the device operates as a hub with default configuration, and configuration cannot be changed.
- **Secure Mode** — This mode keeps the existing configuration active, but it prevents users from making configuration changes by removing the IP address of the device so that it becomes inaccessible for configuration.

For more information about the management modes, see "Management Modes" on page 49.

Head of Line Blocking Prevention

Head of Line (HOL) blocking results in traffic delays and frame loss caused by traffic competing for the same egress port resources. HOL blocking queues packets, and the packets at the head of the queue are forwarded before packets at the end of the queue. By default, the device is configured so that the HOL blocking prevention mechanism is active at all times, except when QoS (Quality of Service), Flow Control or Back Pressure is active on a port where the HOL blocking prevention mechanism is disabled on the whole system.

Back Pressure Support

On half-duplex links, the receiving port prevents buffer overflows by occupying the link so that it is unavailable for additional incoming traffic. The user may enable or disable this feature on a per-port basis. The default status on all ports is set to **OFF**.

Auto Negotiation

Auto negotiation allows an Ethernet switch to advertise modes of operation. The auto negotiation function provides the means to exchange information between two Ethernet switches that share a point-to-point link segment, and to automatically configure both Ethernet switches to take maximum advantage of their transmission capabilities. Port advertisement allows the system administrator to configure the port speeds advertised.

Jumbo Frames Support

Jumbo frames are frames with an MTU (Maximum Transmission Unit) size of up to 10K bytes. The Jumbo Frames Support feature, utilizes the network optimally by transporting the same data using less frames.

The main benefits of this facility are reduced transmission overhead and reduced host processing overhead. Jumbo frames are used for server-to-server transfers.

AutoMDI/MDIX Support

The switch automatically detects whether the cable connected to an RJ-45 port is crossed or straight through.

Standard wiring for end stations is Media-Dependent Interface (MDI) and the standard wiring for hubs and switches is known as Media-Dependent Interface with Crossover (MDIX).

Auto MDI/MDIX works on 10/100/1000BASE-T Ethernet ports. This feature is automatically enabled for the entire system and cannot be turned off by the user.

Flow Control Support (IEEE802.3X)

On Full Duplex links (FDX), the flow control mechanism allows the receiving side to signal to the sending side that transmission must be halted temporarily, in order to prevent buffer overflows. Flow control is enabled by default.

Virtual Cable Testing (VCT)

VCT technology provides the mechanism to detect and report potential cabling issues, such as cable opens and cable shorts on copper links.

Cable analysis is available on Copper Cables (10BASE-T/100BASE-T/1000BASE-T), and is only done when the link is down. When the system initiates a cable-testing operation, upon explicit user action, the following parameters are detected:

- Cable Type and Status
- Cable Length
- Fault-Distance

MAC Address Supported Features

MAC Address Capacity Support

The PowerConnect 2808, 2816, 2824 switches support a total of 8K MAC addresses, and the PowerConnect 2848 supports a total of 16K MAC addresses.

Auto-Learning MAC Addresses

The switch enables MAC address auto-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 of time are aged out. This prevents the Bridging Table from overflowing.

VLAN-aware MAC-based Switching in Managed and Secure Modes

In Managed or Secure mode, the switch system 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 may be configured for untagged frames. Addresses are associated with ports by learning them from the incoming frames source address.

802.1D Bridging in Unmanaged Mode

In Unmanaged Mode, the switch performs classic bridging. Frames are forwarded based on their destination MAC address only, regardless of the VLAN tag.

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. IGMP Snooping is supported, including IGMP Querier which simulates the behavior of a multicast router, allowing snooping of the layer 2 multicast domain even though there is no multicast router. When Multicast groups are statically enabled, you can set the destination port of registered groups, as well as define the behavior of unregistered multicast frames.

Layer 2 Features

Green Ethernet

Green Ethernet, also known as Energy Efficient Ethernet, is an effort to make networking equipment environmentally friendly, specifically by reducing power usage of Ethernet connections. The following methods are supported by the device:

- **Energy-Detect** — Auto-detection of inactivity on a port, and subsequent reducing of transmit power.

- **Short-Reach** — Reduction of power over Ethernet cables shorter than 40m.

IGMP Snooping

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

Port Mirroring

The port mirroring mechanism monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from a monitored port to a monitoring port. Users can specify which target port receives copies of all traffic passing through one or more source ports.

Storm Control

Storm Control enables limiting the amount of Multicast, Broadcast and Unknown Unicast frames accepted and forwarded by the switch. When Layer 2 frames are forwarded, Broadcast and Multicast frames are flooded to all ports on the relevant VLAN. All nodes connected to these ports accept and attempt to process these frames, thus placing load on both the network links and the host operating system.

Dynamic VLAN Assignment (DVA)

Dynamic VLAN Assignment allows automatic assignment of users to VLANs during the RADIUS server authentication. When a user is authenticated by the RADIUS server, the user is automatically joined to the VLAN configured on the RADIUS server.

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 package contents. Packets sharing common attributes can be grouped in the same VLAN.

Port Based Virtual LANs (VLANs)

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

Link Aggregation

The PowerConnect 28xx switches support up to six aggregated links. Each of the six aggregated links may be defined with up to four member ports to form a single Link Aggregated Group (LAG).

The benefits of this facility are:

- Fault tolerance protection from physical link disruption

- Higher bandwidth connections
- Improved bandwidth granularity
- High bandwidth server connectivity

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

DHCP Server

Dynamic Host Configuration Protocol is a method of managing network parameter assignment from a single DHCP server. The Dynamic Host Configuration Protocol (DHCP) automates the assignment of IP addresses, subnet masks, default gateway, and other IP parameters.

BootP and DHCP Clients

DHCP (Dynamic Host Configuration Protocol) 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.

The BootP client is operational if there is a corrupted or invalid software image. The BootP client then continuously attempts to find a BootP server, by sending BootP requests to all ports on the default VLAN, until a BootP server replies. The information replied is then used to provide the switch system with a TFTP server IP address and a download file name. The switch can then configure these values to the TFTP client and try to download a valid runtime image.

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.

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.

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.

STP Root Guard

Root guard restricts the interface from functioning as the root port for the switch

Class of Service (CoS) Features

The PowerConnect 28xx system enables users to define various services for traffic classes of service. The underlying mechanism for supporting bandwidth management and control is based on the use of multiple priority queues for classifying traffic. The switches support four queues per port.

A CoS is defined by the user, whereby packets are related to the same Class of Service. After a packet has been classified, it is assigned to one of the queues. The PowerConnect 28xx system can classify according to IPv4 information (DSCP).

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.

Ethernet Switch Management Features

Web-Based Management

With a Web-based management interface, the Ethernet Switches' 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.

TFTP Trivial File Transfer Protocol

The PowerConnect 28xx switches support software boot image and software download through TFTP.

Remote Monitoring

Remote Monitoring (RMON) is an extension to the Simple Network Management Protocol (SNMP), which provides network traffic statistics. RMON defines current and historical MAC-layer statistics and control objects, allowing real-time information to be captured across the entire network. The switches support one RMON group for Ethernet statistics. The system provides a means to collect the statistics defined in RMON and to view the results, using the Web management interface in the system.

Hardware Description

Switch Port Configurations

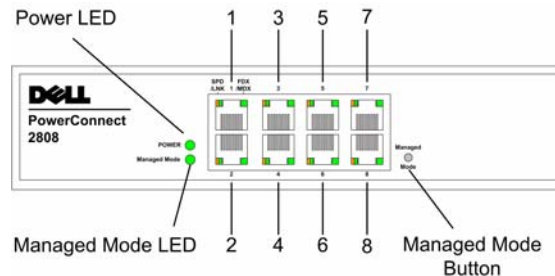
PowerConnect 28xx Front and Back Panel Port Description

The Dell™ PowerConnect™ 28xx switches use 10/100/1000BASE-T ports on the front panel for connecting to a network.

The Gigabit Ethernet ports can operate at 10, 100 or 1000 Mbps. These ports support auto-negotiation, duplex mode (Half or Full duplex), and flow control. The combo 1000 Mbps optical ports can only operate at 1000 Mbps, full-duplex mode.

The following figures illustrate the front panels and back panels of the PowerConnect 28xx switches.

Figure 2-1. PowerConnect 2808 Front Panel



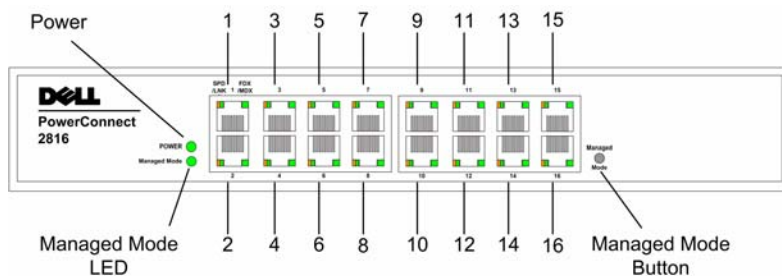
On the front panel there are eight ports which are numbered 1 to 8, top down and left to right. On each port there are LEDs (Light Emitting Diode) to indicate the port status.

On the left side of the front panel is the Managed Mode LED which indicates the Ethernet switch operational status and the management mode. The Power LED on the front panel indicates whether the device is powered on or not. A Mode push-button, located on the right side on the front panel is used to transition between management modes and to reset the device. For more information about management modes and transitioning between them, see "Management Modes" on page 49.

Figure 2-2. PowerConnect 2808 Back Panel



Figure 2-3. PowerConnect 2816 Front Panel



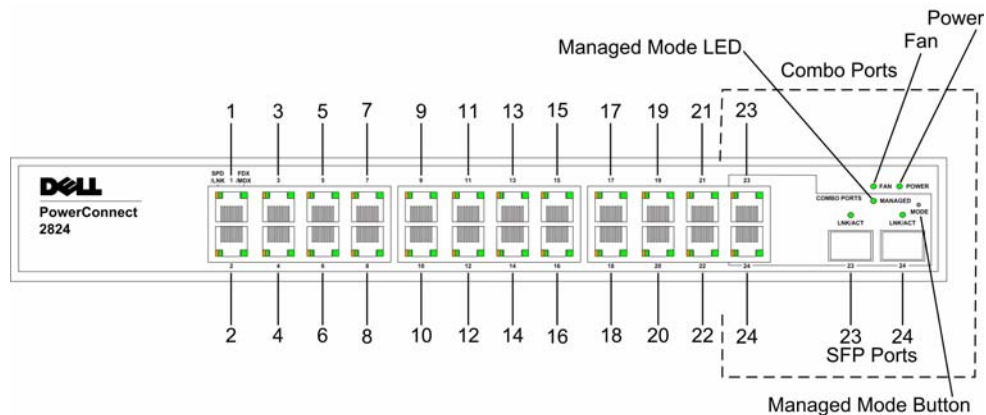
On the front panel there are 16 ports which are numbered 1 to 16, top down and left to right. On each port there are LEDs to indicate the port status.

On the left side of the front panel is the Managed Mode LED which indicates the Ethernet switch operational status and the management mode. The Power LED on the front panel indicates whether the device is powered on or not. A Mode push-button, located on the right side on the front panel, is used to transition between management modes and to reset the device. For more information about management modes and transitioning between them, see "Management Modes" on page 49.

Figure 2-4. PowerConnect 2816 Back Panel



Figure 2-5. PowerConnect 2824 Front Panel



On the front panel there are 24 ports which are numbered 1 to 24, top down and left to right. On each port there are LEDs to indicate the port status. There are two SFP (Small Form-Factor Pluggable) ports, designated as ports 23 and 24, for fiber connection. The two combo ports are logical ports with two physical connections:

- An RJ-45 connection for Twisted Pair (TP) copper cabling
- An SFP port for swappable optical transceiver, which offers high-speed 1000BASE-SX or 1000BASE-LX connection.

NOTE: Only one of the two physical connections of a combo port can be used at any one time. Port features and port controls are determined by the physical connection used. The system automatically detects the media used on a combo port, and utilizes the information in all the control interfaces.

NOTE: The system can switch from the RJ-45 to the SFP (or vice versa) without resetting the device. If both RJ-45 and SFP ports are present, the SFP port will be the active port, whereas the RJ-45 port will be disabled.

On the front panel is the Managed Mode LED which indicates the Ethernet switch operational status and the management mode. The Fan LED indicates the device fan operations status, and the Power LED on the front panel indicates whether the device is powered on or not. A Mode push-button, located on the right side on the front panel is used to transition between management modes and to reset the device. For more information about management modes and transitioning between them, see "Management Modes" on page 49.

Figure 2-6. PowerConnect 2824 Back Panel

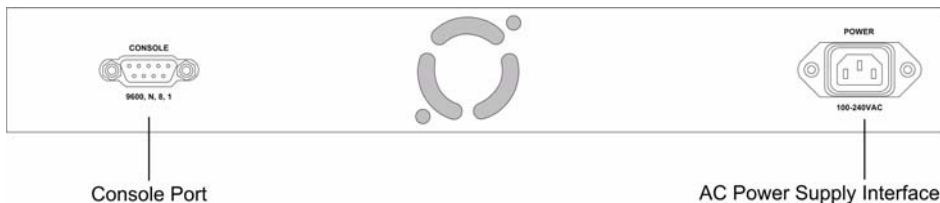
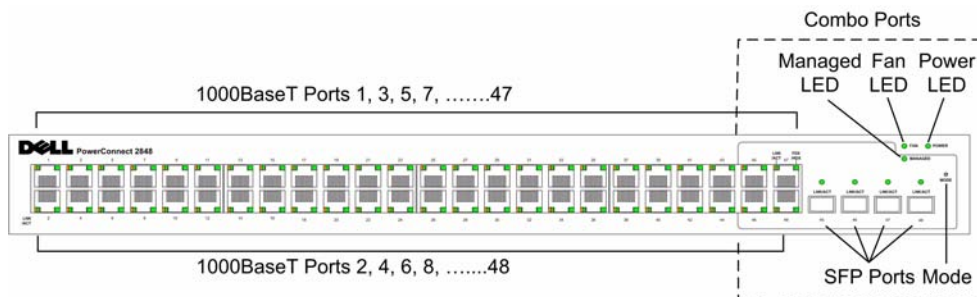


Figure 2-7. PowerConnect 2848 Front Panel



On the front panel there are 48 ports, which are numbered 1 to 48, top down and left to right. On each port, there are LEDs to indicate the port status. There are four SFP (Small Form-Factor Pluggable) ports, designated as ports 45, 46, 47 and 48, for fiber connection. The four combo ports are logical ports with two physical connections:

- An RJ-45 connection for Twisted Pair (TP) copper cabling.
- An SFP port for swappable optical transceiver, which offers high-speed 1000BASE-SX or 1000BASE-LX connection.

NOTE: Only one of the two physical connections of a combo port can be used at any one time. Port features and port controls are determined by the physical connection used. The system automatically detects the media used on a combo port, and utilizes the information in all the control interfaces.

NOTE: The system can switch from the RJ-45 to the SFP (or vice versa) without resetting the device. If both RJ-45 and SFP ports are present, the SFP port will be the active port, whereas the RJ-45 port will be disabled.

On the top right side of the front panel is the Managed Mode LED which indicates the Ethernet switch operational status and the management mode. The Fan LED indicates the device fan operations status, and the Power LED on the front panel indicates whether the device is powered on or not. A Mode push-

button, located on the right side on the front panel is used to transition between management modes and to reset the device. For more information about management modes and transitioning between them, see "Management Modes" on page 49.

Fans are provided on the side panel. The back panel contains an AC Power Supply Interface.

The following figure illustrates the back panel of the PowerConnect 2848 device.

Figure 2-8. PowerConnect 2848 Back Panel



Physical Dimensions

The PowerConnect 2808 switch has the following physical dimensions:

- Height — 43.2 mm (1.7008 in.)
- Width — 256 mm (10.079 in.)
- Depth — 161.7 mm (6.366 in.)

The PowerConnect 2816 and PowerConnect 2824 switches have the following physical dimensions:

- Height — 43.2 mm (1.7008 in.)
- Width — 330 mm (12.992 in.)
- Depth — 230.50 mm (9.075 in.)

The PowerConnect 2848 switch has the following physical dimensions:

- Height — 43.2 mm (1.70 in.)
- Width — 440 mm (17.32 in.)
- Depth — 255 mm (10.04 in.)

LED Definitions

The front panel contains LEDs that indicate the status of links, power supply, fan status, and Managed Mode status.

Power LED

On the PowerConnect 28xx front panel there is a Power LED. The following table describes the Power Supply status LED indications.

Table 2-1. Power LED Indications

LED Color	Description
Green Solid	The switch is turned on.
Off	The switch is not turned on.

Managed Mode LED

On the PowerConnect 28xx front panel there is a Managed Mode LED monitoring the switch node as well as indicating diagnostic test results. The following table describes the Managed Mode LED indications. For more information about management modes and transitioning between them, see "Management Modes" on page 49.

Table 2-2. Managed Mode LED Indications

LED Color	Description
Green Flashing	Indicates diagnostics in progress, firmware loading, or Management Mode transition.
Green Solid	Indicates the switch is in Managed Mode.
Amber Solid	Diagnostics has failed.
Amber Flashing	No valid image.
Off	Indicates Unmanaged mode or Secure mode.

Fan LED (2824/2848 only)

On the PowerConnect 2824 and PowerConnect 2848 front panel there is a fan LED. The following table describes the fan status LED indications.

Table 2-3. Fan LED Indications

LED Color	Description
Green Solid	All fans are operating correctly.
Red Solid	One or more fans have failed.

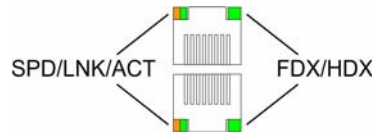
Port LEDs

10/100/1000BASE-T Port LEDs

Each 10/100/1000BASE-T port has two LEDs. Speed/Link/Activity is indicated on the left LED and the duplex mode is indicated on the right LED.

The following figure illustrates the RJ-45 10/100/1000BASE-T LEDs.

Figure 2-9. RJ-45 Copper-based 10/100/1000BASE-T LEDs



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

Table 2-4. RJ-45 Copper based 10/100/ 1000BASE-T LED Indications

LED	Color	Description
Left LED	Green Solid	The port is linked at 1000 Mbps.
	Green Flashing	The port is transmitting or receiving data at 1000 Mbps.
	Amber Solid	The port is linked at either 10 or 100 Mbps.
	Amber Flashing	The port is transmitting or receiving data at 10 or 100 Mbps.
	Off	No link is established.
Right LED	Green Solid	The port is currently transmitting in Full Duplex mode.
	Off	The port is operating in Half Duplex mode.

SFP Port LED

The following table describes the SFP LED indications.

Table 2-5. SFP LED Indications

LED Color	Description
Green Solid	Link is established.
Green Flashing	Activity is occurring.
Off	No link is established.

Managed Mode Button

The PowerConnect 28xx has a Mode push button on the front panel. The Mode button is for changing between Managed Mode and Unmanaged (or Secure) Mode and for resetting the device. To transition between modes, press the button normally. To reset the device, press and hold the button for at least 7 seconds. For more information about management modes and transitioning between them, see "Management Modes" on page 49.

Switch Ventilation Fan

The PowerConnect 2848 switch has three fans and the PowerConnect 2824 switch has one fan for system ventilation. The PowerConnect 2808 and PowerConnect 2816 devices have no internal fans.

Cables, Port Connections, and Pinout Information

This section explains the switch physical interfaces, and provides information about cables and port connections. Copper cable diagnostics are supported. High-speed workstations, hubs, routers, or other switches are connected through standard RJ-45 connectors to the switch physical interface ports, located on the front panel. For each device, the supported mode is set to Half Duplex, Full Duplex, and Auto.

1000BASE-T Cable Requirements

All Category 5 UTP cables that are used for 100BASE-TX connections also operate with 1000BASE-T, provided if all four wire pairs are connected. However, it is recommended that enhanced Category 5 (Category 5e) cable is used for all critical connections or any new cable installations. The Category 5e specification includes test parameters that are only recommendations for Category 5, and comply with the IEEE 802.3ab standards.

RJ-45 Connections for 10/100/1000BASE-T Ports

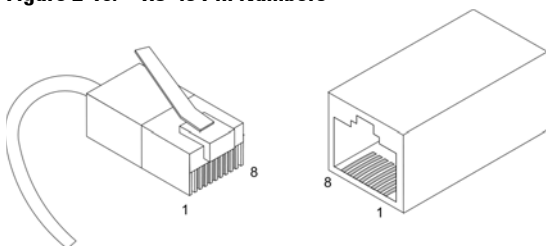
The 10/100/1000BASE-T ports are copper Twisted-Pair ports.

Table 2-6. Port Default Settings

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

The following figure illustrates the RJ-45 pin connector pin numbers.

Figure 2-10. RJ-45 Pin Numbers



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

Table 2-7. RJ-45 Pin Number Allocation for 10/100/ 1000BASE-T Ethernet Port

Pin No	Function
1	TxRx 1+
2	TxRx 1-
3	TxRx 2+
4	TxRx 2-
5	TxRx 3+

Table 2-7. RJ-45 Pin Number Allocation for 10/100/ 1000BASE-T Ethernet Port

Pin No	Function
6	TxRx 3-
7	TxRx 4+
8	TxRx 4-

SFP Ports

The PowerConnect 2824 switch supports two SFP transceivers combo ports, and the PowerConnect 2848 switch supports four SFP transceivers combo ports for various fiber-based modules (1000BASE-SX or 1000BASE-LX). Only one of the two physical connections of a combo port can be used at any time. The system can switch from the RJ-45 to the SFP (or vice versa) without a system reset. The system automatically detects the media used on a combo port, and utilizes this information in the control interfaces.

PowerConnect 2824 switch supports SFP diagnostics. The optical transceiver provides access to a set of parameters that can be monitored and displayed to the system administrator.



NOTE: If both RJ-45 and SFP ports are present, the SFP port will be the active port, whereas the RJ-45 port will be disabled and ignored.

The pin number allocation for the SFP ports is listed in the following table.

Table 2-8. SFP Pin Connections

Pin No	Use
1	Transmitter ground (common with receiver ground)
2	Transmitter fault
3	Transmitter disable; laser output disabled on high or open.
4	Module definition 2; data line for serial ID.
5	Module definition 1; clock line for serial ID.
6	Module definition 0; grounded within the module.
7	Rate select; no connection required.
8	Loss of signal indication; logic 0 indicates normal operation.
9	Receiver ground (common with transmitter ground)
10	Receiver ground (common with transmitter ground)
11	Receiver ground (common with transmitter ground)
12	Receiver inverted data out; AC coupled.
13	Receiver non-inverted data out; AC coupled.
14	Receiver ground (common with transmitter ground)

Table 2-8. SFP Pin Connections

Pin No	Use
15	Receiver power supply
16	Transmitter power supply
17	Transmitter ground (common with receiver ground)
18	Transmitter non-inverted data in
19	Transmitter inverted data in
20	Transmitter ground (common with receiver ground)

Power Connectors

The PowerConnect 28xx is powered by using the AC internal power supply.

Internal Power Supply Connector

The PowerConnect 28xx supports a single internal power supply to provide power for switching operations. The internal power supply supports input voltages between 100 and 240 VAC. The AC power connector is located on the back panel of the switch.

Installing the PowerConnect Device

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

Installation Precautions

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

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

- Ensure that the rack or cabinet housing the device is adequately secured to prevent it from becoming unstable and/or falling over.
- Ensure that the power source circuits are properly grounded.
- Observe and follow the service markings. Do not service any device except as explained in the system documentation. Opening or removing covers marked with a triangular symbol with a lightning bolt may cause electrical shock. These components are to be serviced by trained service technicians only.
- Ensure that the power cable, extension cable, and/or plug is not damaged.
- Ensure that the device is not exposed to water.
- Ensure that the device is not exposed to radiators and/or heat sources.
- Ensure that the cooling vents are not blocked.
- Do not push foreign objects into the device, as it may cause a fire or electric shock.
- Use the device only with approved equipment.
- Allow the device to cool before removing covers or touching internal equipment.
- Ensure that the device does not overload the power circuits, wiring, and over-current protection. To determine the possibility of overloading the supply circuits, add together the ampere ratings of all switches installed on the same circuit as the device. Compare this total with the rating limit for the circuit.
- Do not install the device in an environment where the operating ambient temperature might exceed 45°C (113°F).
- Ensure that the airflow around the front, sides, and back of the device is not restricted.

Site Requirements

The PowerConnect 28xx can be mounted in a standard equipment rack, placed on a tabletop, or mounted on the wall.

Before installing the device, verify that the site selected for the device meets the following site requirements:

- **Power** — The device is installed within 1.5 m (5 feet) of a grounded, easily accessible outlet 220/110 VAC, 50/60 Hz. If the device has two power supplies, the site should have two power outlets with different power feeders.
- **General** — Ensure that the power supply is correctly installed.
- **Clearance** — There is adequate frontal clearance for operator access. Allow clearance for cabling, power connections, and ventilation.
- **Cabling** — Cabling is routed to avoid sources of electrical noise such as radio transmitters, broadcast amplifiers, power lines, and fluorescent lighting fixtures.
- **Ambient Requirements** — The ambient device operating temperature range is 0 to 45 °C (32 to 113 °F) at a relative humidity of up to 95%, non-condensing. Verify that water or moisture cannot enter the device case.

Unpacking

Package Contents

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

- The device
- AC power cable
- Self-adhesive rubber pads (for on-shelf installation)
- Rack-mount kit for installation
- Documentation CD
- *Product Information Guide*

Unpacking the Device

To unpack the PowerConnect device:

NOTE: Before unpacking the device, inspect the packaging and 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 package and place it on a secure, stable and clean surface.
- 4 Remove all packing material.

- 5 Inspect the product for damage. Report any damage immediately.

Mounting the Device

Overview

There are three device mounting options:

- Installing in a Rack
- Installing on a Flat Surface
- Installing on a Wall

Device Rack Installation

 **CAUTION** Read the safety information in the Product Information Guide as well as the safety information for other devices that connect to or support the switch.

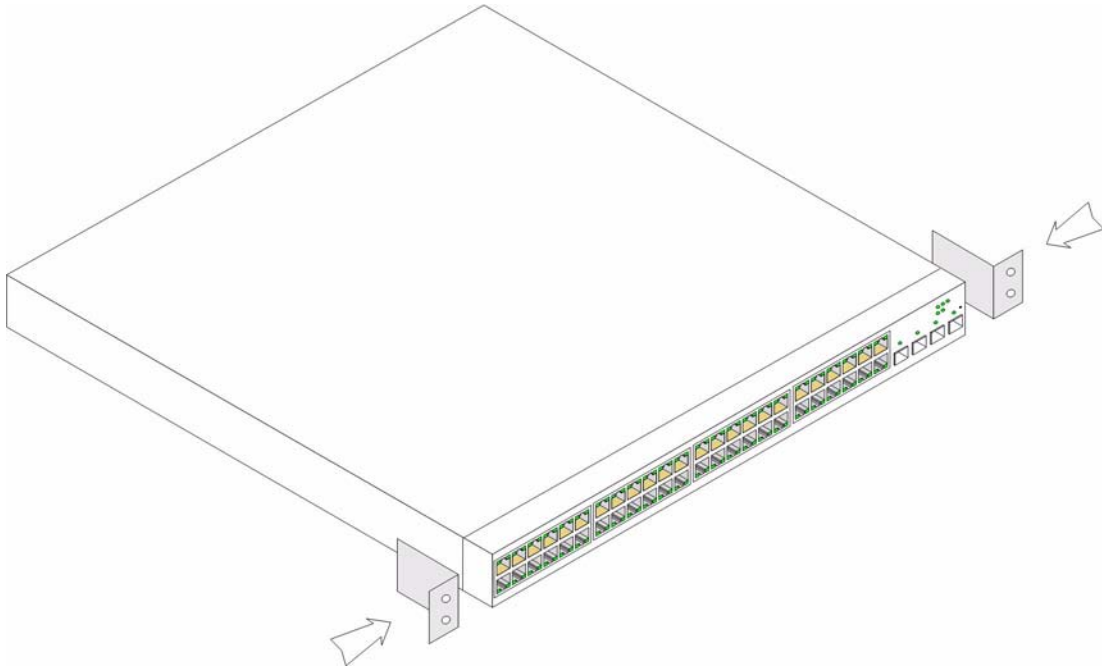
 **CAUTION** Disconnect all cables from the device before mounting the device in a rack or cabinet.

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

Install the device in a rack as follows:

- 1 Place the supplied rack-mounting bracket on one side of the device ensuring the mounting holes on the device line up to the mounting holes on the rack mounting bracket. 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 device into the rack, ensuring the rack-mounting holes on the device line up to the mounting hole on the rack.
- 5** Secure the device 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.

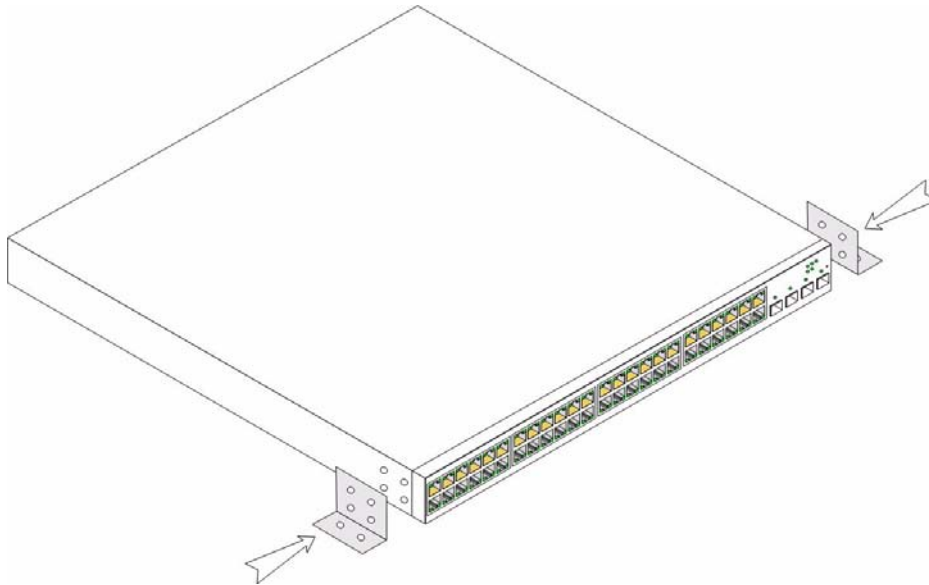
- 1** Attach the self-adhesive rubber pads (provided with the device) on each marked location on the bottom of the chassis.
- 2** Set the device on a flat surface, while leaving 2 inches (5.08 cm) on each side and 5 inches (12.7 cm) at the back.
- 3** Ensure that the device has proper ventilation.

Installing on a Wall

To mount the device on a wall:

- 1 Ensure that the mounting location meets the following requirements:
 - The surface of the wall must be capable of supporting the device.
 - Allow at least 2 inches (5.1 cm) space on the sides for proper ventilation and 5 inches (12.7 cm) at the back for power cable clearance.
 - The location must not be exposed to direct sunlight.
 - The location must be at least 2 feet (61 cm) away from any heating vents, and no area-heating vent should point towards the device.
 - The location must be ventilated to prevent heat buildup.
 - Do not locate the device near any data or electrical cabling.
 - The power cable must be able to reach an outlet.
- 2 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.

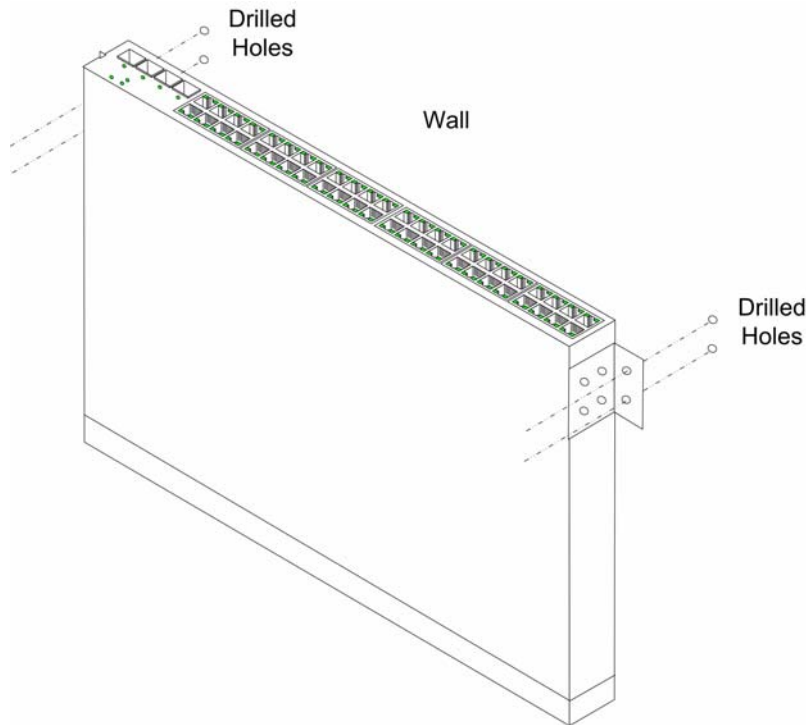
Figure 3-2. Bracket Installation for Wall Mounting



- 3 Insert the supplied screws into the rack-mounting holes and tighten with a screwdriver.
- 4 Repeat the process for the wall-mounting bracket on the other side of the device.
- 5 Place the device on the wall in the location where the device is being installed.

- 6 On the wall mark the locations where the screws to hold the device must be prepared.
- 7 On the marked locations, drill the holes and place all plugs (not provided) in the holes.
- 8 Secure the device to the wall with screws (not provided). Ensure that the ventilation holes are not obstructed.

Figure 3-3. Mounting Device on a Wall





Connecting the Device

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

Connecting the Device to the Network

To connect to an uplink port, use Category 5 Unshielded Twisted-Pair (UTP) cables with RJ-45 connectors at both ends. The RJ-45 ports on the Ethernet device support automatic Media-Dependent Interface/Media-Dependent Interface with internal crossover wiring (MDI/MDIX) operation under Auto-Negotiation mode. Standard straight-through twisted-pair cables can be used to connect to any other Ethernet network (systems, servers, switches or routers) that supports auto-negotiation.

 **NOTE:** Do not plug a phone jack connector into an RJ-45 port. This will damage the Ethernet device. Use only twisted-pair cables with RJ-45 connectors that conform to FCC standards.

 **NOTE:** If auto negotiation is turned off on the ports, a straight through cable must be used.

To connect the device to the network:

- 1 Attach one end of a Twisted-Pair cable to the device's RJ-45 connector and the other end to a switch or server.
- 2 Make sure each twisted pair cable does not exceed 328 feet (100 meters) in length.

As each connection is made, the link LED corresponding to each port on the device is illuminated (green or amber) indicating that the connection is valid.

Connecting the Terminal to the Device

The device provides an external console port in models 28016/24/48. The console port 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, perform the following:

- 1 Connect the supplied RS-232 crossover cable to the terminal running VT100 terminal emulation software.
- 2 Ensure that the terminal emulation software is set as follows:
 - a Select the appropriate serial port (serial port 1 or serial port 2) to connect to the console.
 - b Set the data rate to 9600 baud.
 - c Set the data format to 8 data bits, 1 stop bit, and no parity.
 - d Set flow control to none.
 - e Under Properties, select VT100 for Emulation mode.
 - f Select Terminal keys for Function, Arrow, and Ctrl keys. Ensure that the setting is for Terminal keys (not Windows keys).

 **NOTE:** When using HyperTerminal with Microsoft® Windows 2000, Windows XP, or Windows Vista, ensure that you have the latest service packs 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, Windows XP, and Windows Vista service packs.

- 3 Connect the female connector of the RS-232 crossover cable directly to the device Console port on the device, and tighten the captive retaining screws. The Console port is located on the back panel.

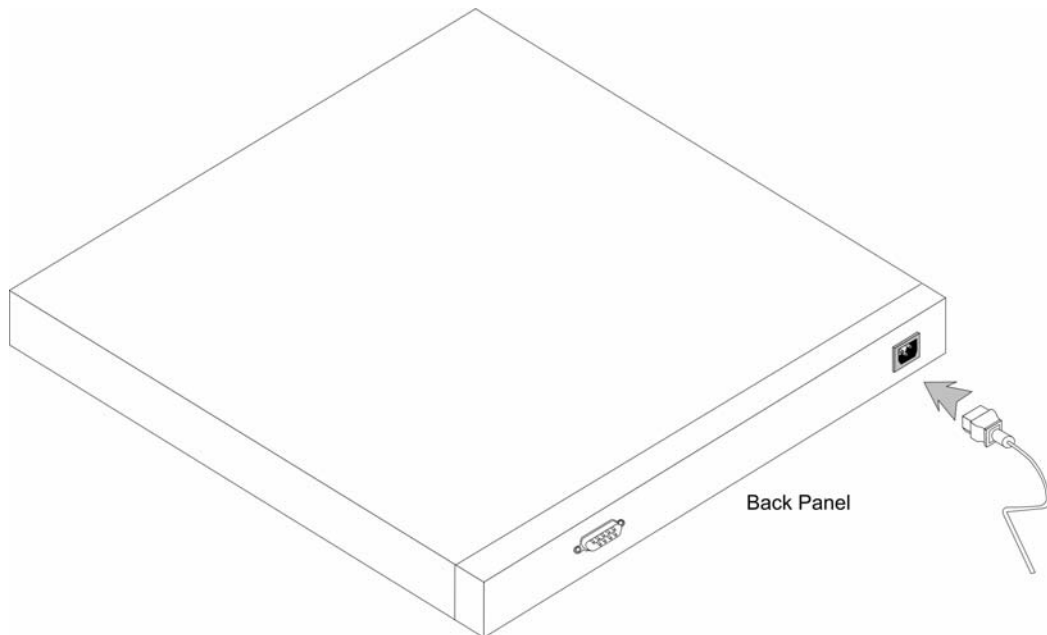
Connecting to Console Port



Connecting a Device to a Power Supply

- 1 Connect the supplied standard AC power cable to the AC connector on the back panel.
- 2 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. Connecting to Power Supply



- 3 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.

Port Connections, Cables, and Pinout Information

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

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

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

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

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

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

Table 3-1. Ports, Connectors and Cables

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

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

Table 3-2. RJ-45 Pin Number Allocation for 10/100/1000BaseT Ethernet Port

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

Port Default Settings

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

Auto-Negotiation

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

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

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

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

MDI/MDIX

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

When the MDI/MDIX (Media Dependent Interface with Crossover) is enabled, the automatic correction of errors in cable selection is possible, making the distinction between a straight through cable and a crossover cable irrelevant. (The standard wiring for end stations is known as MDI (Media Dependent Interface), and the standard wiring for hubs and switches is known as MDIX.)

Flow Control

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

Back Pressure

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

Switching Port Default Settings

The following table gives the port default settings.


Table 3-3. Port Default Settings


Function	Default Setting
Port speed and mode	10/100/1000BaseT copper: auto-negotiation full duplex
Port forwarding state	Enabled
Port tagging	No tagging
Flow Control	On
Back Pressure	Off (disabled on ingress)
MDIX (not user-configurable)	On (relevant to coppers ports only)


Starting and Configuring the Device

After completing all external connections, proceed as follows:

- If the device is to be used as an unmanaged switch, there is no need for a terminal connection.
- A terminal connection is required if the device is to be used in a managed mode.

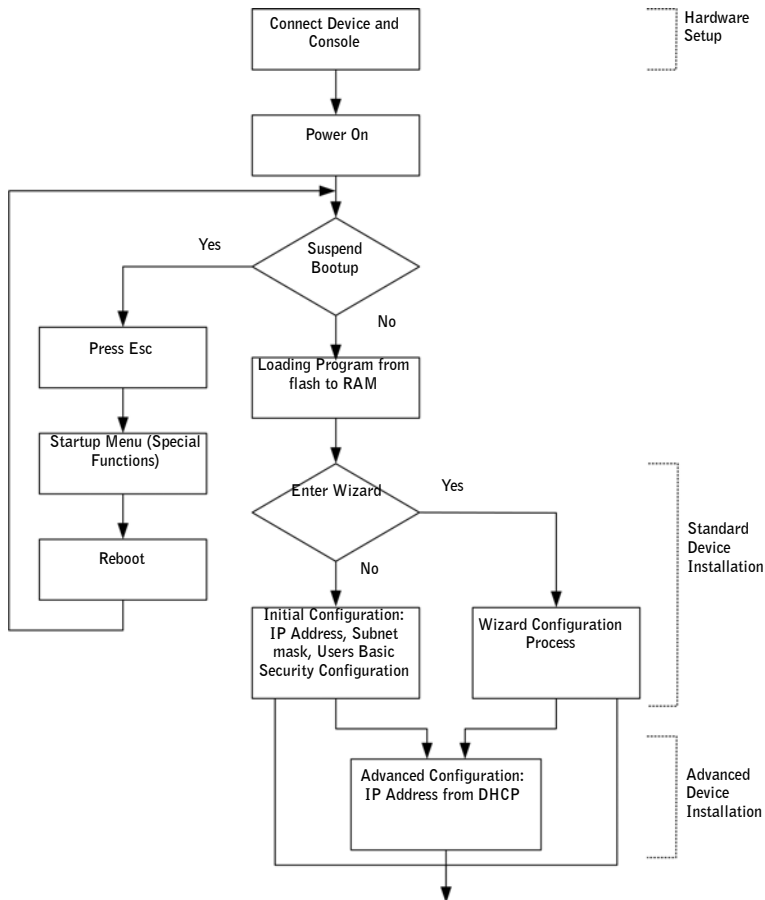
 **NOTE:** The PowerConnect 2808 has an internal serial port.

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

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

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

Figure 4-1. Installation and Configuration Flow



Booting the Device - Managed Mode

The procedure described in this section refers to the device when set to operate as a managed switch. The PowerConnect 2808/16/24/48 models include a built-in dual purpose Mode Button. To change between managed and unmanaged modes, press the Mode Button for less than seven seconds.

Once the device is set to operate as a managed switch the boot procedure can be monitored on the connected terminal as follows:

- 1 Ensure that the 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 the power is turned on with the local terminal already connected, the device goes through Power On Self Test (POST). POST runs every time the device is initialized and checks hardware components to determine if the device is fully operational before completely booting. If a critical problem is detected, the program flow stops. If POST 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 less than 45 seconds when in unmanaged mode (and approximately 90 seconds when in other modes).

Initial Configuration - Managed Mode

The information and procedures described in this section apply to the device when set as a Managed Mode switch.


 **NOTE:** The switch is factory-set in Unmanaged Mode.

 **NOTE:** The initial simple configuration uses the following assumptions:

- 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. (Press the <Enter> key several times to verify that the prompt displays correctly.)

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

The system prompts you to use the Set-up wizard when the device boots up for the first time or if the configuration file is empty because the device is not configured. 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 your network administrator before configuring the device:

- SNMP Community String and SNMP Management System IP address (optional).
- Username and Password.
- The IP address to be assigned to the VLAN 1 interface through which the device is to be managed (by default, every external and internal 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.

The Setup Wizard guides you through the initial device configuration, and gets the system up and running as quickly as possible. You can skip using the setup wizard and configure the device manually through the device CLI mode (see "Managing the Device Using the CLI" on page 157).

The Setup Wizard configures the following fields.

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

The Setup Wizard displays the following information:

```
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
```

NOTE: If you select not to use the Setup Wizard, you can access the Web interface by using the default IP address/mask (192.168.2.1/255.255.255.0).

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

Wizard Step 1

The following information displays:

```
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/v2 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 Set-up wizard. The following information displays:

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]

Wizard Step 2

The following information displays:

Now we need to setup your initial privilege (Level 15) user account.

This account is used to login to the CLI, Telnet 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:*****

Wizard Step 3

The following information displays:

Next, an IP address is setup.

The IP address is defined on the default VLAN ,(VLAN #2) . This is the IP address you use to access the Telnet, 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):10.6.22.100

Please enter the IP subnet mask (A.B.C.D or nn):[255.255.255.224]

Wizard Step 4

The following information displays:

```
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):[10.6.22.97]
```

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 = 10.6.22.100 255.255.255.224
```

```
Default Gateway is 10.6.22.97
```

```
=====
```

Wizard Step 5

The following information displays:

```
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
```

```
Configuring SNMP management interface.
```

```
Configuring user account.....
```

```
Configuring IP and subnet.....
```

Thank you for using Dell Easy Setup Wizard.


Advanced Configuration

This section provides information about dynamic allocation of IP addresses.

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

Retrieving an IP Address From a DHCP Server

When using the DHCP protocol to retrieve an IP address, the device acts as a DHCP client. When the device is reset, the DHCP command is saved in the configuration file, but not the IP address. To configure the device so it will retrieve an IP address from a DHCP server, use the web interface (see "Defining DHCP Server Settings" on page 83).

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

Startup Procedures

Startup Menu Procedures

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

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

To enter the Startup menu:

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

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

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

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

```
BOOT Software Version 1.0.0.20 Built 22-Jan-xxxx 15:09:28
```

Processor: FireFox 88E6218 ARM946E-S , 64 MByte SDRAM.
I-Cache 8 KB. D-Cache 8 KB. Cache Enabled.


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

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

- [1] Download Software
- [2] Erase Flash File
- [3] Password Recovery Procedure
- [4] Enter Diagnostic Mode
- [5] Set Terminal Baud-Rate
- [6] Back

Enter your choice or press 'ESC' to exit

The following sections describe the available Startup menu options.

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

Software Download


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

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

Downloading code using XMODEM

- 2** When using the HyperTerminal, click **Transfer** on the HyperTerminal Menu Bar.
- 3** In the **Filename** field, enter the file path for the file to be downloaded.
- 4** Ensure that the **Xmodem** protocol is selected in the **Protocol** field.
- 5** Press **Send**. The software is downloaded.

 **NOTE:** After software download, the device reboots automatically.

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

Erase FLASH File

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

Erasing the Device Configuration

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

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

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

- 2 Press **y**. The following message is displayed.

```
Write Flash file name (Up to 8 characters, Enter for none.):config
File config (if present) will be erased after system initialization
===== Press Enter To Continue =====
```

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

Password Recovery

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

To recover a lost password for the local terminal only:

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



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

Software Download Through TFTP Server

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

System Image Download

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

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

To download a system image through the TFTP server:

- 1 Ensure that an IP address is configured on one of the device ports and pings can be sent to a TFTP server.
- 2 Make sure that the file to be downloaded is saved on the TFTP server (the `ros` file).

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

```
console# copy tftp://176.215.31.3/file1.ros image
Accessing file `file1' on 176.215.31.3
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.

- 4 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]?
```

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

```
console# copy tftp://176.215.31.3/332448-10018.rfb boot
Erasing file..done.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Copy: 2739187 bytes copied in 00:01:13 [hh:mm:ss]
```

- 4 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]?

5 Enter y.

The device reboots.

Management Modes

The device supports the following modes:

- **Managed Mode** — Provides switch management through the web interface. From Managed mode, you can move to Unmanaged mode by pressing the Mode button on the device, or you can move to Secure mode using the web interface (see "Entering Secure Mode" on page 63). Before leaving Managed mode it is highly recommended to save the configuration (see "Uploading Files" on page 82).
- **Unmanaged Mode** — In this mode, the device does not have an IP address; STP is disabled; there is no web management interface, the CLI works in debug mode only; and there is no configuration in the CDB—default configuration is used. From this mode, you can return to Managed mode by pressing the Mode button on the device.
- **Secure Mode** — This mode keeps the existing configuration active, but it prevents users from making configuration changes by removing the IP address of the device so that it becomes inaccessible for configuration. In this mode, no web management interface is available, and CLI works in debug mode only. From this mode, you can return to Managed mode by pressing the Mode button on the device.

All modes are maintained through power cycles. The Managed Mode LED provides an indication of the current mode (see "On the PowerConnect 28xx front panel there is a Managed Mode LED monitoring the switch node as well as indicating diagnostic test results. The following table describes the Managed Mode LED indications. For more information about management modes and transitioning between them, see "Management Modes" on page 50." on page 22).

Default Values

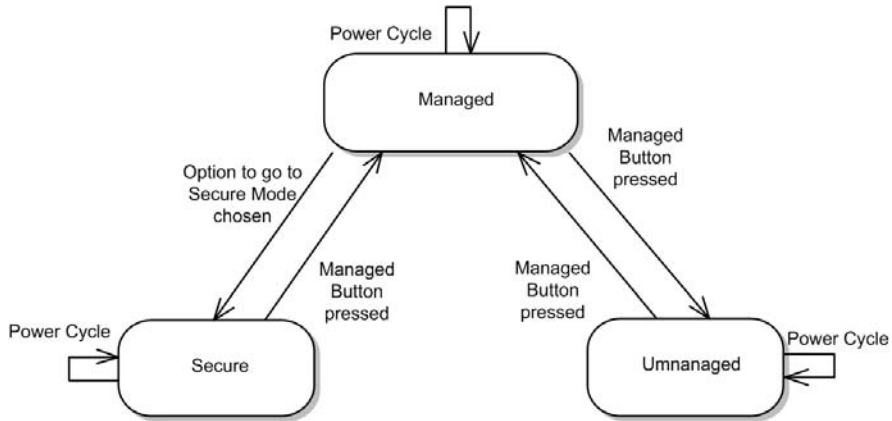
The factory default values, used when the device is in Unmanaged mode, include:

- IP Address — 192.168.2.1
- Netmask — 255.255.255.0
- Username — admin
- Permission — R/W privilege
- DHCP Client — Off
- Flow Control — On
- STP — Off

Transitioning Between Modes

The following diagram summarizes movement between modes:

Figure 4-2. Transitioning Between Management Modes



Returning to Managed Mode

When returning to Managed mode from either Unmanaged or Secure mode, the Restore Saved Configuration page appears. This page can be used to retrieve a saved configuration. You can also change the device IP address using this page.

Figure 4-3. Restore Saved Configuration

Dell OpenManage Switch Administrator Support Help About Log Out

DELL

176.210.11.22 Restore Saved Configuration

Home
Restore Configuration **Restore Saved Configuration** Print Refresh

Restore Saved Configuration
 Local Configuration Server IP Address (X.X.X.X)
File Name

Use Saved IP 192.168.2.1 Use Current IP 192.168.2.1
 Use Saved User Name/Password Use Current User Name/Password

Apply Changes

- **Local Configuration** — No saved configuration is loaded.
- **Server IP Address/File Name** — Loads a previously saved configuration.
- **Use Saved IP/User Name/Password** — When restoring local configuration, this option uses the IP address, user name and password that were automatically saved when you exited Managed mode. When restoring a saved configuration, this option uses the IP address, user name and password inside the saved configuration.
- **Use Current IP/User Name/Password** — When restoring local configuration, this option uses the system default IP address, user name and password.
- **Apply Changes** — The selected configuration is restored and the device reboots.

Using Dell OpenManage Switch Administrator

This section provides an introduction to the user interface.

Understanding the Interface

The home page contains the following views:

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

Figure 5-1. Switch Administrator Components

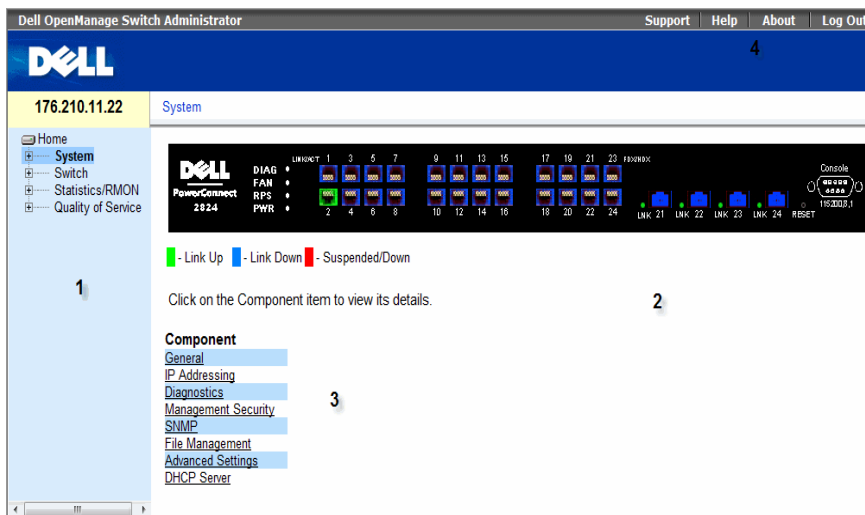


Table 5-1 lists the interface components with their corresponding numbers.

Table 5-1. Interface Components

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

Device Representation

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

Figure 5-2. Port LED Indicators



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

Table 5-2. Led Indicators

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



NOTE: The Port LEDs are not reflected in PowerConnect front panel in the PowerConnect OpenManage Switch Administrator. LED status can only be determined by viewing the actual device. For more information about LEDs, see "LED Definitions" on page 21.

Using the Switch Administrator Buttons

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

Information Buttons

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

Table 5-3. Information Buttons

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

Device Management Buttons

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

Table 5-4. Device Management Buttons

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

Starting the Application

- 1 Open a web browser.
- 2 Enter the device's IP address (as defined in the CLI) in the address bar and press <Enter>. For information about assigning an IP address to a device, see "Static IP Address and Subnet Mask."
- 3 When the **Enter Network Password** window opens, enter a user name and password.



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



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



NOTE: The device can be managed via web interface only in Managed mode. For more information about management modes, see "Management Modes" on page 49.

- 4 Click OK.

The Dell PowerConnect OpenManage™ Switch Administrator home page opens.

Access Levels

When you login to the device, you are automatically assigned one of the following modes, based upon the access level assigned to you:

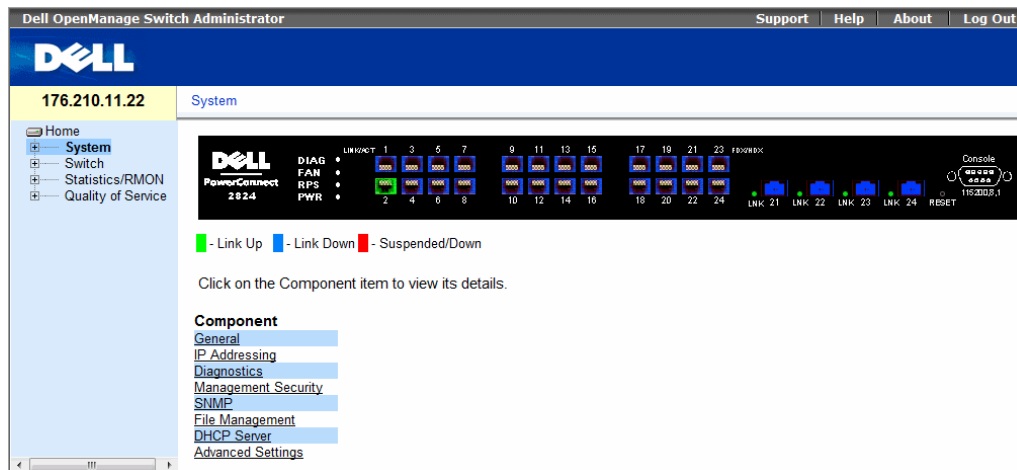
- **Management** — This is a read-write mode where you can see and edit all pages of the interface.
- **Monitor** — This is a read-only mode where you can see a subset of the interface pages, but you cannot edit them.

For more information about setting the access level, see ("Defining the Local User Databases" on page 69).

Configuring System Information

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

Figure 6-1. System



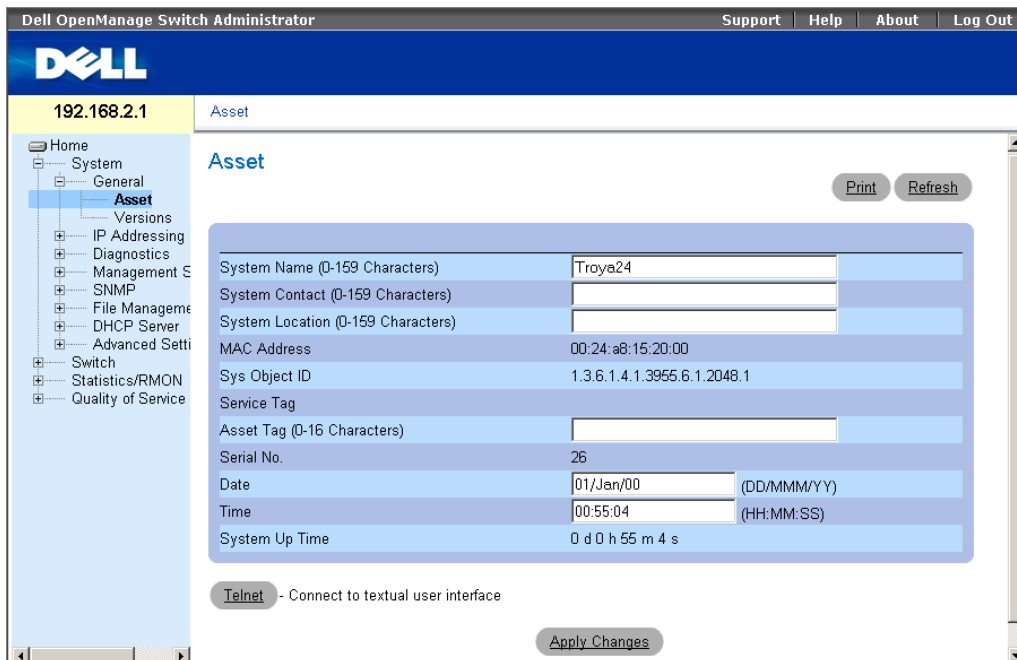
Defining General Device Information

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

Viewing Device Information

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

Figure 6-2. Asset



- **System Name (0-159 Characters)** — Defines the user-defined device name.
- **System Contact (0-159 Characters)** — Specifies the name of the contact person.
- **System Location (0-159 Characters)** — Specifies the location where the system is currently running.
- **MAC Address** — Specifies the device MAC address.
- **Sys Object ID** — Specifies the vendor's authoritative identification of the network management subsystem contained in the entity.
- **Service Tag** — Specifies the service reference number used when servicing the device.
- **Asset Tag (0-16 Characters)** — Specifies the user-defined device reference.
- **Serial No.** — Specifies the device serial number.
- **Date (DD/MMM/YY)** — Specifies the current date. The format is day, month, year, for example, 10/NOV/02 is November 10, 2002.
- **Time (HH:MM:SS)** — Specifies the time. The format is hour, minute, second, for example, 20:12:03 is eight twelve and three seconds in the evening.
- **System Up Time** — Specifies the amount of time since the last device reset. The system time is displayed in the following format: Days, Hours, Minutes and Seconds. For example, 41 days, 2 hours, 22 minutes and 15 seconds.

Defining System Information:

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

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

Initiating a Telnet Session:

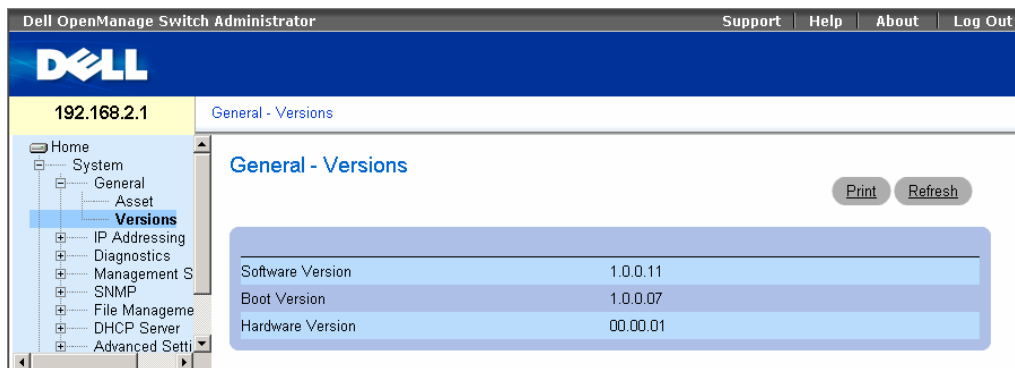
- 1 Open the Asset page.
- 2 Click Telnet.

A Telnet session is initiated.

Viewing the Versions Page

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

Figure 6-3. Versions

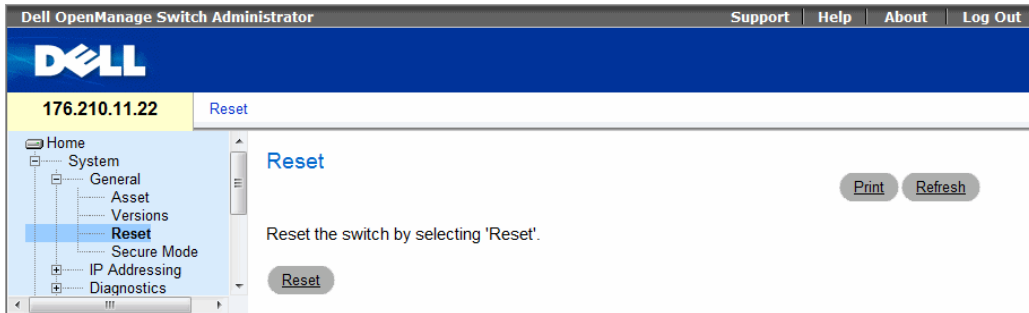


- **Software Version** — The current software version running on the device.
- **Boot Version** — The current Boot version running on the device.
- **Hardware Version** — The current hardware version.

Resetting the Device

The **Reset** page enables the device to be reset from a remote location. For more information about saved Configuration files, see "Managing Files" on page 80. To open the **Reset** page, click **System** → **General** → **Reset** in the tree view.

Figure 6-4. Reset



Resetting the Device

- 1 Open the **Reset** page
- 2 Click **reset**.
A confirmation message displays.
- 3 Click **OK**.
The device is reset. After the device is reset, a prompt for a user name and password displays.
- 4 Enter a user name and password to reconnect to the Web Interface.

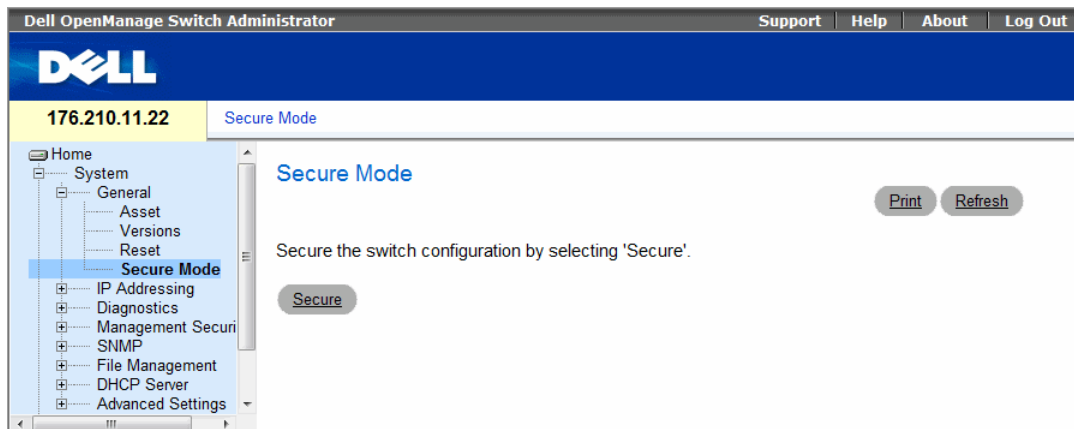
Entering Secure Mode

The **Secure Mode** page allows you to put the device in the *Secure* management mode. Once enabled, it prevents users from making any further configuration changes to the switch. This is done by removing the IP address of the switch so that it becomes inaccessible. In Secure Mode the switch retains configuration through power cycles just like in Managed Mode.

To use Secure Mode, configure the device in Managed Mode, and then switch to Secure Mode via the web interface. To exit Secure Mode, press the Managed Mode button on the device to enter the Managed Mode default configuration with the default IP address of 192.168.2.1. For information about management modes, see "Management Modes" on page 49. For information about saving Configuration files, see "Managing Files" on page 80.

To open the Secure Mode page, click **System** → **General** → **Secure Mode** in the tree view.

Figure 6-5. Secure Mode



Entering Secure Mode

- 1 Open the Secure Mode page.
- 2 Click Secure.
A confirmation message displays.
- 3 Click OK.
The device enters Secure mode.

Defining Device IP Addresses

The IP Addressing page contains links for assigning interface and default gateway IP addresses, and enabling or disabling DHCP.

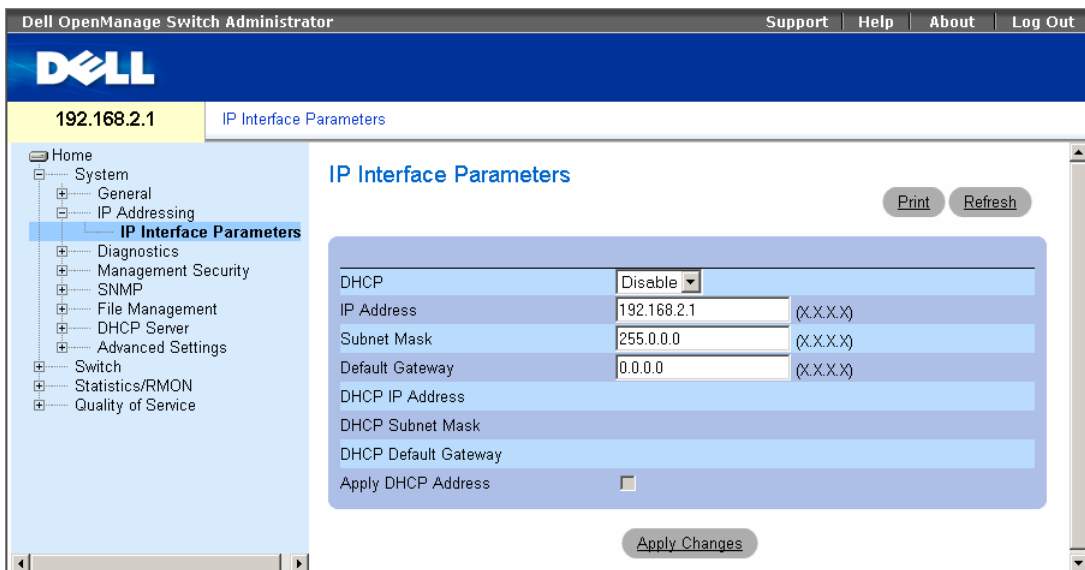
To open the IP Addressing page, click System → IP Addressing in the tree view.

Defining IP Interface Parameters

The IP Interface Parameters page is used to select whether the device IP address, mask and/or gateway is assigned statically, or dynamically using DHCP. The page is also used to make static assignments, and to approve dynamic assignments received from the DHCP server before they go into affect (until approval, the old address is used).

To open the IP Interface Parameters page, click System→ IP Addressing → IP Interface Parameters in the tree view.

Figure 6-6. IP Interface Parameters



- **DHCP** — The DHCP client can be enabled to acquire the network configuration dynamically. The DHCP default value is Disable. This field enables the DHCP client.
- **IP Address** — Specifies the static IP Address currently assigned to the device.
- **Subnet Mask**— Specifies the subnet mask of the static IP Address, currently assigned to the device.
- **Default Gateway** — Specifies the static Default Gateway Address, currently assigned to the device.
- **DHCP IP Address** — Specifies the IP Address received from the DHCP server.
- **DHCP Subnet Mask** — Specifies the Subnet Mask received from the DHCP server.

- **DHCP Default Gateway** — Defines the Default Gateway Address received from the DHCP server.
- **Apply DHCP Address** — Activates the IP Address, Subnet Mask Address, and Default Gateway Address, received from the DHCP server.

Enabling DHCP:

- 1 Open the **IP Interface Parameters** page.
- 2 Set **DHCP** to **Enable**.
- 3 Click the **Apply DHCP Address** checkbox.
- 4 Click **Apply Changes**.
DHCP is enabled and the device is updated.

Setting static IP Interface parameters:

- 1 Open the **IP Interface Parameters** page.
- 2 Set **DHCP** to **Disable**.
- 3 Set the **IP Address**, **Subnet Mask** and **Default Gateway**.
- 4 Click **Apply Changes**.
The static interface parameters are set and the device is updated.

Running Cable Diagnostics

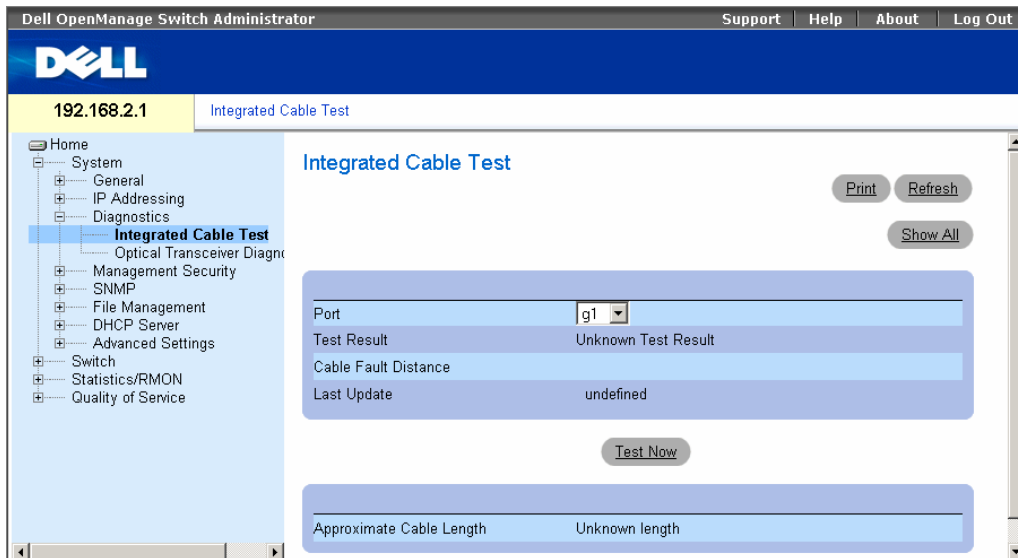
The **Diagnostics** page contains links to pages for performing virtual cable tests on copper and fiber optics cables. To open the **Diagnostics** page, click **System** → **Diagnostics** in the tree view.

Viewing Copper Cable Diagnostics

The **Integrated Cable Test for Copper Cables** page contains fields for performing tests on copper cables. Cable testing provides information about where errors occurred in the cable, the last time a cable test was performed, and the type of cable error which occurred. The tests use Time Domain Reflectometry (TDR) technology to test the quality and characteristics of a copper cable attached to a port. Cables up to 120 meters long can be tested. Cables are tested when the ports are in the down state, with the exception of the **Approximated Cable Length** test. The cable length returned is an approximation in the ranges of up to 50 meters, 50m-80m, 80m-110m, 110m-120m, or more than 120m. The deviation may be up to 20 meters.

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

Figure 6-7. Integrated Cable Test for Copper Cables



- **Port** — The port to which the cable is connected.
- **Test Result** — The cable test results. Possible values are:
 - **No Cable** — There is no cable connected to the port.
 - **Open Cable** — The cable is connected on only one side.
 - **Short Cable** — The cable is 2 meters long.
 - **OK** — The cable passed the test.
 - **Fiber Cable** — A fiber cable is connected to the port.
- **Cable Fault Distance** — The distance from the port where the cable error occurred.
- **Last Update** — The last time the port was tested.
- **Approximate Cable Length** — The approximate cable length. This test can only be performed when the port is up and operating at 1 Gbps.

Performing a Cable Test

- 1 Ensure that both ends of the copper cable are connected to a device.
- 2 Open the **Integrated Cable Test for Copper Cables** page.
- 3 Click **Test Now**.

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

Displaying Virtual Cable Test Results Table

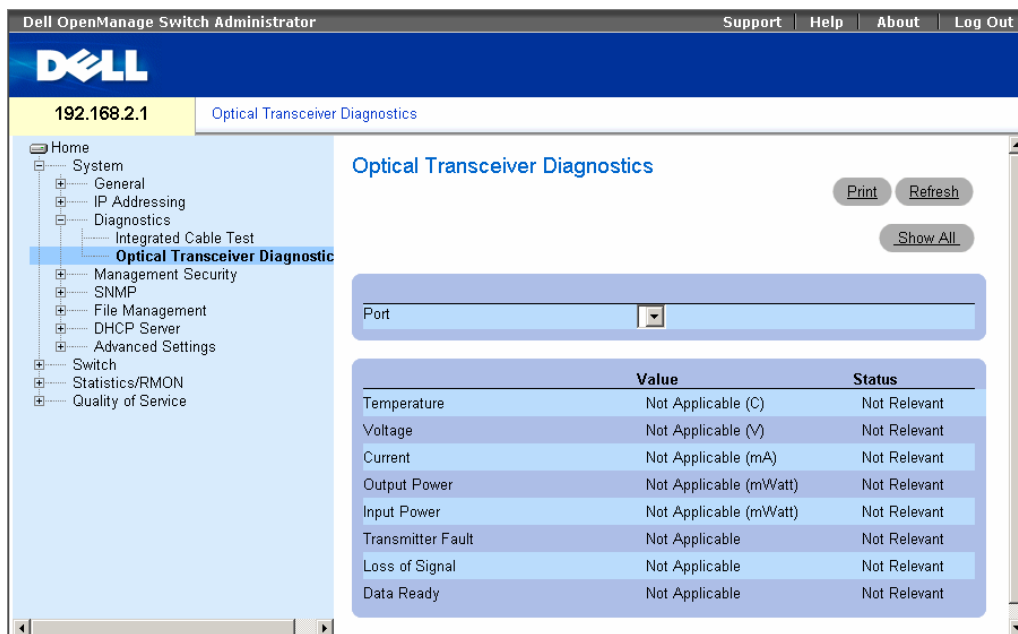
- 1 Open the Integrated Cable Test for Copper Cables page.
- 2 Click Show All.

The Virtual Cable Test Results Table opens.

Viewing Optical Transceiver Diagnostics

The Optical Transceiver Diagnostics page contains fields for performing tests on Fiber Optic cables. Optical transceiver diagnostics can be performed only when the link is present. To open the Optical Transceiver Diagnostics page, click System→Diagnostics→Optical Transceiver Diagnostics in the tree view.

Figure 6-8. Optical Transceiver Diagnostics



The screenshot shows the Dell OpenManage Switch Administrator interface. The main content area is titled "Optical Transceiver Diagnostics" and features a "Port" dropdown menu. Below the dropdown is a table with three columns: "Value" and "Status". The table lists various diagnostic metrics, all of which are currently "Not Applicable".

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

- **Port** — The port to which the fiber cable is connected.
- **Temperature** — The temperature (in Celsius) at which the cable is operating.
- **Voltage** — The voltage at which the cable is operating.
- **Current** — The current at which the cable is operating.
- **Output Power** — The rate at which the output power is transmitted.
- **Input Power** — The rate at which the input power is transmitted.
- **Transmitter Fault** — Indicates if a fault occurred during transmission.

- **Loss of Signal** — Indicates if a signal loss occurred in the cable.
- **Data Ready** — The transceiver has achieved power up and data is ready.

Displaying Optical Transceiver Diagnostics Test Results Table

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

The test is run and the **Virtual Cable Test Results Table** opens with the following columns:

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

Finisair transceivers do not support the transmitter fault diagnostic testing.

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

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

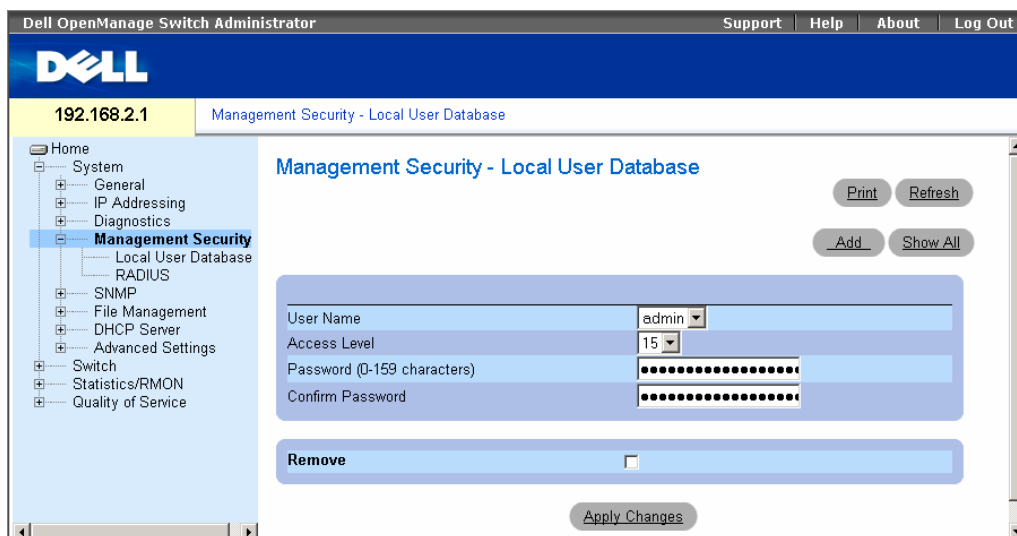
Managing Device Security

The Management Security page provides access to security pages that contain fields for setting security parameters for user database, password and RADIUS security. To open the Management Security page, click System→Management Security in the tree view.

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 6-9. Local User Database



- **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 edit all pages of the OpenManage Switch Administrator.
- **Password (0-64 Characters)** — User-defined password.
- **Confirm Password** — Confirms the user-defined password.
- **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 6-10. Add a User

Refresh

Add User

User Name (1-20 Characters)	<input type="text"/>
Access Level	1
Password (0-159 Characters)	<input type="password"/>
Confirm Password (0-159 Characters)	<input type="password"/>

Apply Changes

- 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 6-11. Local User Table

Refresh

Local User Table

	User Name	Access Level	Remove
1	admin	Read Write	<input type="checkbox"/>

Apply Changes

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.

Configuring RADIUS Global Parameters

Remote Authorization Dial-In User Service (RADIUS) servers provide additional security for networks. RADIUS servers provide a centralized authentication method for:

- Telnet Access
- Web Access
- Console to Device Access

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

Figure 6-12. RADIUS Settings

The screenshot shows the Dell OpenManage Switch Administrator interface. The top navigation bar includes 'Support', 'Help', 'About', and 'Log Out'. The main header displays the Dell logo and the IP address '192.168.2.1'. The left sidebar shows a tree view with 'RADIUS' selected under 'Management Security'. The main content area is titled 'RADIUS Settings' and contains the following configuration fields:

IP Address	192.254.254.3
Priority (0-65535)	0
Authentication Port (0-65535)	1812
Number of Retries (1-10)	<input type="checkbox"/> Use Default
Timeout for Reply (1-30)	(Sec) <input checked="" type="checkbox"/> Use Default
Dead Time (0-2000)	(Min) <input checked="" type="checkbox"/> Use Default
Key String (0-128 Characters)	qa (Alpha Numeric) <input type="checkbox"/> Use Default
Source IP Address	(X.X.X.X) <input checked="" type="checkbox"/>

Default Parameters

Default Retries (1-10)	3
Default Timeout for Reply (1-30)	3 (Sec)

- IP Address — The list of Authentication Server IP addresses.

- **Priority (0-65535)** — Specifies 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)** — Specifies the number of transmitted requests sent to RADIUS server before a failure occurs. The possible field values are 1 - 10. Three is the default value.
- **Timeout for Reply (1-30)** — Specifies the amount of the time in seconds the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server. The possible field values are 1 - 30. The default is 3.
- **Dead Time (0-2000)** — Specifies the amount of time (in seconds) that a RADIUS server is bypassed for service requests. The range is 0-2000.
- **Key String (0-128 Characters)** — Specifies the Key string used for authenticating and encrypting all RADIUS communications between the device and the RADIUS server. This key is encrypted.
- **Source IP Address** — Specifies the source IP address that is used for communication with RADIUS servers.

If host-specific Timeouts, Retries, or Dead time values are not specified, the Global values (Defaults) are applied to each host. The following fields set the RADIUS default values:

- **Default Retries (1-10)** — Specifies the default number of transmitted requests sent to RADIUS server before a failure occurs.
- **Default Timeout for Reply (1-30)** — Specifies the default amount of the time (in seconds) the device waits for an answer from the RADIUS server before timing out.
- **Default Dead time (0-2000)** — Specifies the default amount of time (in seconds) that a RADIUS server is bypassed for service requests. The range is 0-2000.
- **Default Key String (0-128 Characters)** — Specifies the Default Key string used for authenticating and encrypting all RADIUS communications between the device and the RADIUS server. This key is encrypted.
- **Source Address** — Specifies the source IP address that is used for communication with RADIUS servers.

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 6-13. Add RADIUS Server Page

Add RADIUS Server Refresh

IP Address	<input type="text"/>	(X.X.X.X)
Priority (0-65535)	<input type="text"/>	
Authentication Port (0-65535)	1812	
Number of Retries (1-10)	3	<input type="checkbox"/> Use Default
Timeout for Reply (1-30)	3	(Sec) <input type="checkbox"/> Use Default
Dead Time (0-2000)	0	(Min) <input type="checkbox"/> Use Default
Key String (0-128 Characters)	<input type="text"/>	<input type="checkbox"/> Use Default
Source IP Address	<input type="text"/>	(X.X.X.X) <input type="checkbox"/> Use Default
Usage Type	Login	<input type="checkbox"/>

Apply Changes

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

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

Displaying the RADIUS Server List:

- 1 Open the RADIUS Settings page.
- 2 Click Show All.

The Show all RADIUS Servers page opens:

Figure 6-14. Show all RADIUS Servers

RADIUS Servers List Refresh

IP Address	Priority	Authentication Port	Number of Retries	Timeout for Reply	Dead Time	Source IP Address	Usage Type	Remove
1							Login	<input type="checkbox"/>

Apply Changes

Modifying the RADIUS Server Settings:

- 1 Open the RADIUS Settings page.

- 2 Click **Show All**.

The **RADIUS Servers List** page opens.

- 3 Modify the relevant fields.

- 4 Click **Apply Changes**.

The RADIUS Server settings are modified, and the device is updated.

Deleting a RADIUS Server for the RADIUS Servers List:

- 1 Open the **RADIUS Settings** page.

- 2 Click **Show All**.

The **RADIUS Servers List** page opens.

- 3 Select a RADIUS Server in the **RADIUS Servers List**.

- 4 Select the **Remove** check box.

- 5 Click **Apply Changes**.

The RADIUS server is removed from the **RADIUS Servers List**.

Defining SNMP Parameters

Simple Network Management Protocol (SNMP) provides a method for managing network devices. Devices supporting SNMP run a local software (agent).

The SNMP agents maintain a list of variables, which are used to manage the device. The variables are defined in the Management Information Base (MIB). The MIB contains the variables controlled by the agent. The SNMP protocol defines the MIB specification format, as well as the format used to access the information over the network.

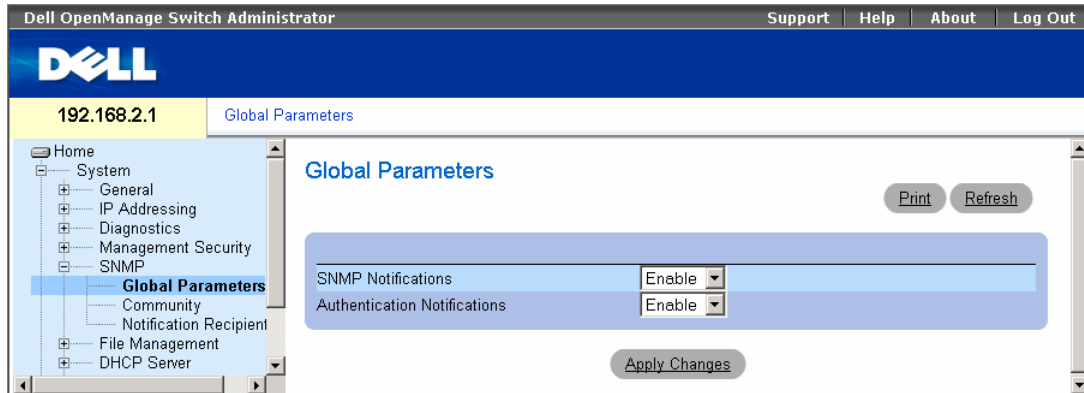
Access rights to the SNMP agents are controlled by access strings. To communicate with the device, the Embedded Web Server submits a valid community string for authentication. To open the SNMP page, click **System** → **SNMP** in the tree view.

This section contains information for managing the SNMP configuration.

Defining 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 6-15. Global Parameters



- **SNMP Notifications** — Enables or disables the device sending SNMP notifications.
- **Authentication Notifications** — Enables or disables the device 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.

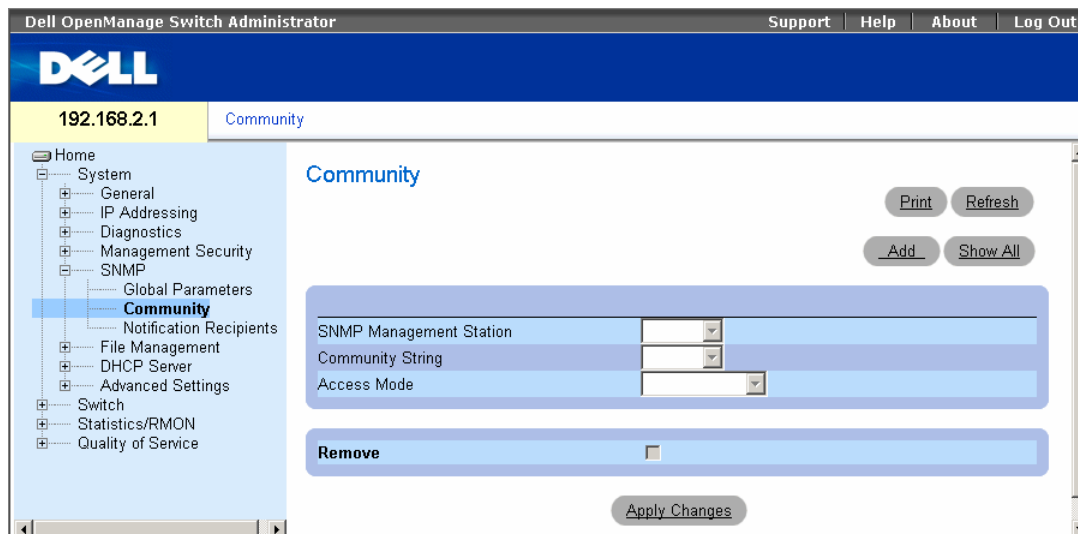
Enabling Authentication Notifications

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

Defining Communities

Access rights are managed by defining communities in the **Community Table**. When the community names are changed, access rights are also changed. To open the SNMP Community page, click **System** → **SNMP** → **Community** in the tree view.

Figure 6-16. SNMP Community



- **SNMP Management Station** — A list of management station IP addresses.
- **Community String** — Functions as a password and used to authenticate the selected management station to the device.
- **Access Mode** — Defines the access rights of the community. The possible field values are:
 - **Read Only** — The management access is restricted to read-only, for all MIBs except the community table, for which there is no access.
 - **Read Write** — The management access is read-write, for all MIBs except the community table, for which there is no access.
 - **SNMP Admin** — The management access is read-write for all MIBs, including the community table.
- **Remove** — Removes a community, when selected.

Defining a New Community

- 1 Open the **SNMP Community** page.
- 2 Click **Add**.

The **Add SNMP Community** page opens:

Figure 6-17. Add SNMP Community

[Refresh](#)

Add SNMPv1,2 SNMP Community

SNMP Management Station (X.X.X.X)
 All (0.0.0.0)

Community String (1-20 Characters)

Access Mode

- 3 Select one of the following:
 - **SNMP Management Station** — Defines an SNMP community for a specific management station.
 - **All** — Defines an SNMP community for all management stations.
- 4 Define the remaining fields.
- 5 Click **Apply Changes**.

The new community is saved, and the device is updated.

Displaying all Communities

- 1 Open the **SNMP Community** page.
- 2 Click **Show All**.

The **Community Table** opens:

Figure 6-18. Community Table

[Refresh](#)

Community Table

Basic Table

Management Station	Community String	Access Mode	Remove
1 1.1.1.1	SNMP Admin		<input type="checkbox"/>

[Apply Changes](#)

Deleting Communities

- 1 Open the **Community Table** page.
- 2 Click **Show All**.

The **Community Table** opens.
- 3 Select a community from the **Community Table**.

- 4 Select the **Remove** check box.
- 5 Click **Apply Changes**.

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

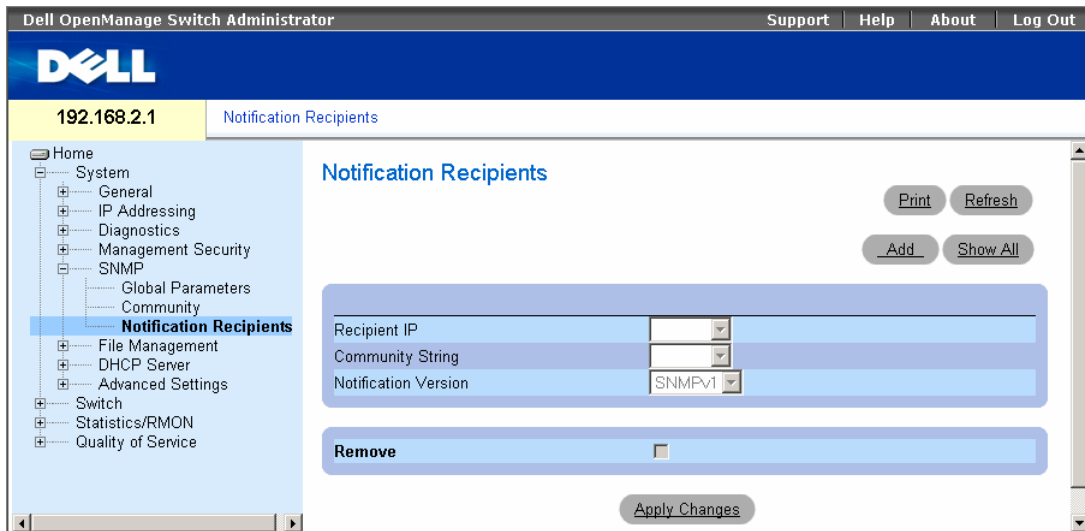
Defining SNMP Notification Recipients

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 6-19. Notification Recipients



- **Recipient IP** — Indicates the IP address to whom the traps are sent.
- **Community String** — Functions as a password and used to authenticate the selected management station to the device.
- **Notification Version** — Determines the trap type. The possible field values are:
 - **SNMPv1** — SNMP Version 1 traps are sent.

- SNMPv2 — SNMP Version 2 traps are sent.
- **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:

[Refresh](#)

Add Notification Recipient

Recipient IP (X.X.X.X)

Community String

Notification Version

[Apply Changes](#)

- 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 6-20. Notification Recipients Tables

Notification Recipients Table

[Refresh](#)

SNMPv1,2 Notification Recipient

Management Station	Community String	Notification Version	Remove

[Apply Changes](#)

Deleting Notification Recipients

- 1 Open Notification Recipients page.

2 Click **Show All**.

The **Notification Recipients Tables** page opens.

3 Select a notification recipient.

4 Check the **Remove** checkbox.

5 Click **Apply Changes**. The recipient is deleted, and the device is updated.

Managing Files

The **File Management** page contains fields for managing device software, the Image Files, and the Configuration Files. Files can be downloaded from a TFTP server.

The configuration file structure consists of the following configuration files:

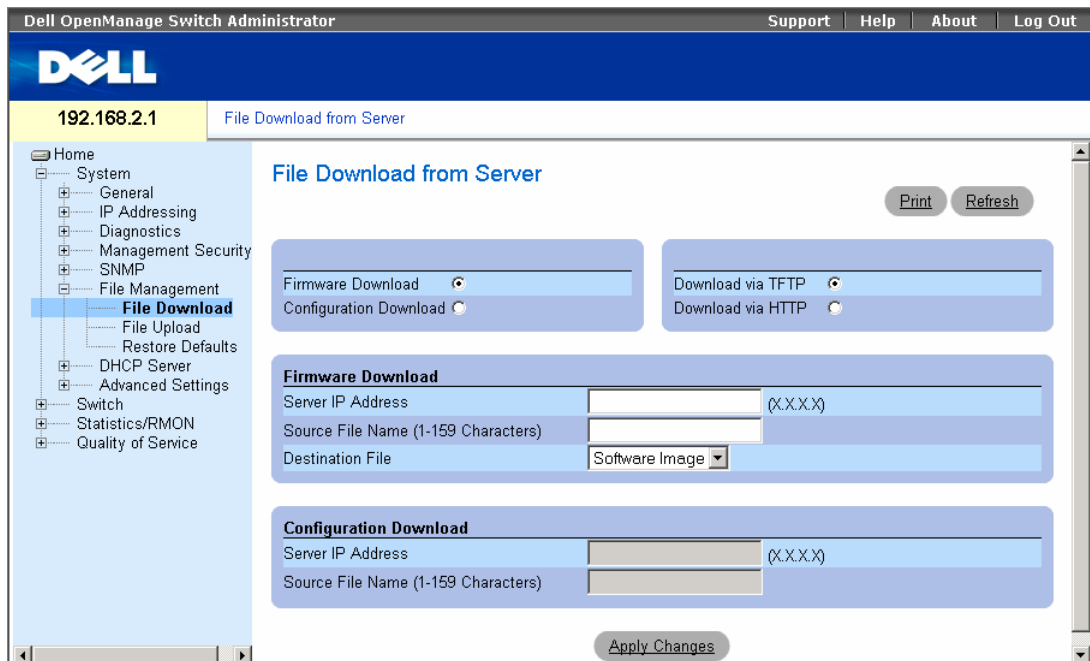
- **Startup Configuration File** — Contains the commands required to reconfigure the device to the same settings as when the device is powered down or rebooted.
- **Running Configuration File** — Contains all Startup file commands, as well as all commands entered during the current session. After the device is powered down or rebooted, all commands stored in the Running Configuration file are lost. During the startup process, all commands in the Startup file are copied to the Running Configuration File and applied to the device. During the session, all new commands entered are added to the commands existing in the Running Configuration file. Commands are not overwritten.
- **Image File** — System file images are saved in a Flash File called an image. The device boots and runs from the image.

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 or HTTP client to the device. To open the **File Download From Server** page, click **System** → **File Management** → **File Download** in the tree view.

Figure 6-21. File Download From Server



- **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.
- **Download via TFTP** — Enables initiating an image download via the TFTP server.
- **Download via HTTP** — Enables initiating an image download via the HTTP server.

Firmware Download

- **Server IP Address** — The 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 to which the configuration file is downloaded. The possible field values are:
 - **Software Image** — Downloads the software image file.
 - **Boot Code** — Downloads the boot file.

Configuration Download

- **Server IP Address** — The Server IP Address from which the configuration files are downloaded.

- **Source File Name (1-64 Characters)** — Indicates the configuration files to be downloaded.

During the image file download, a dialog box opens which displays the download progress.

Downloading Files

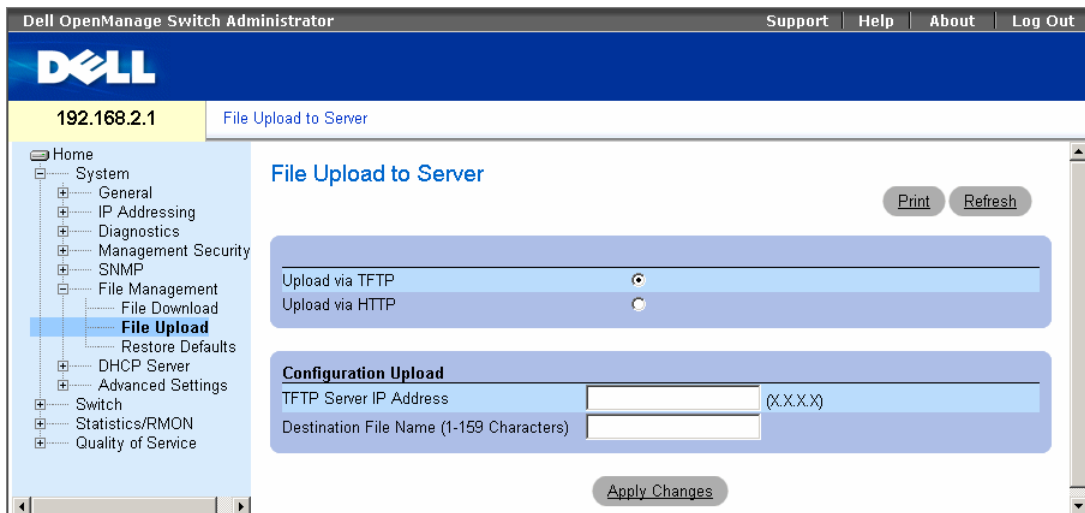
- 1 Open the **File Download From Server** page.
- 2 Define the fields.
- 3 Click **Apply Changes**.

The software is downloaded to the device.

Uploading Files

The **File Upload to Server** page contains fields for uploading the Configuration file from the device to the TFTP server. To open the **File Upload to Server** page, click **System** → **File Management** → **File Upload** in the tree view.

Figure 6-22. File Upload to Server



The **File Upload to Server** page contains the following fields:

- **Upload via TFTP** — Enables initiating a configuration file upload via the TFTP server.
- **Upload via HTTP** — Enables initiating a configuration file upload via the FTP server.
- **TFTP Server IP Address** — The Server IP Address to which the file is uploaded.
- **Destination File Name (1-64 Characters)** — Indicates the file path to which the file is uploaded.

Uploading Files

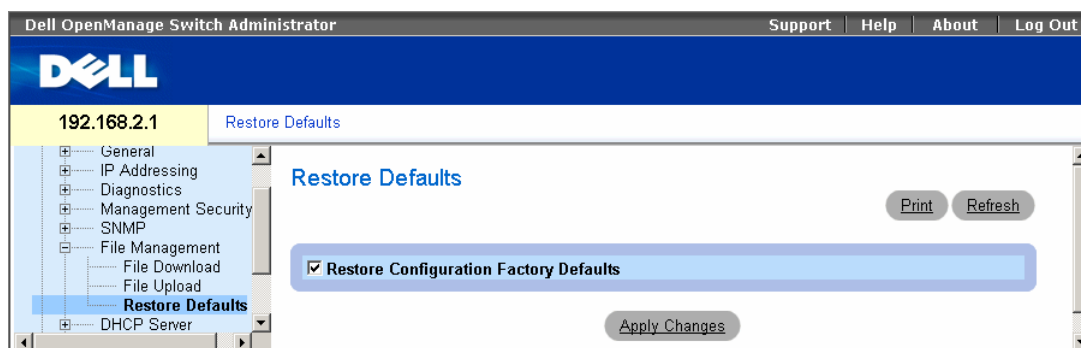
- 1 Open the File Upload to Server page.
- 2 Define the fields.
- 3 Click Apply Changes.

The software is uploaded to the device.

Restoring Default Settings

The Restore Defaults page allows you to restore the device settings to their factory default values. To open the Restore Defaults page, click System → File Management → Restore Defaults in the tree view.

Figure 6-23. Restore Defaults



The Restore Defaults page contains the following field:

- Restore Configuration Factory Defaults — Sets the device settings to their factory default values.

Restoring Default Settings

- 1 Open the Restore Defaults page.
- 2 Check the Restore Configuration Factory Defaults checkbox.
- 3 Click Apply Changes.

The settings are restored.

Defining DHCP Server Settings

The DHCP server is used mainly for centralized control over assignment of IP addresses to attached hosts.

A switch can operate as either a DHCP client (obtaining its own IP from a DHCP server) and as a DHCP server.

The DHCP server uses a defined pool of IP addresses (user-defined) from which it allocates IP addresses to DHCP clients.

The DHCP server can allocate IP addresses in three configuration modes:

- **Static allocation** — The network administrator maps the hardware address of a host to an IP address on the DHCP server.
- **Permanent allocation** — An IP address received through a standard request-reply mechanism is owned by a client permanently (unless changes in the network environment/connections take place, for any reason).
- **Dynamic allocation** — A network device obtains a leased IP address for a specified period of time. The IP address is revoked at the end of this period and the switch must request another IP address.

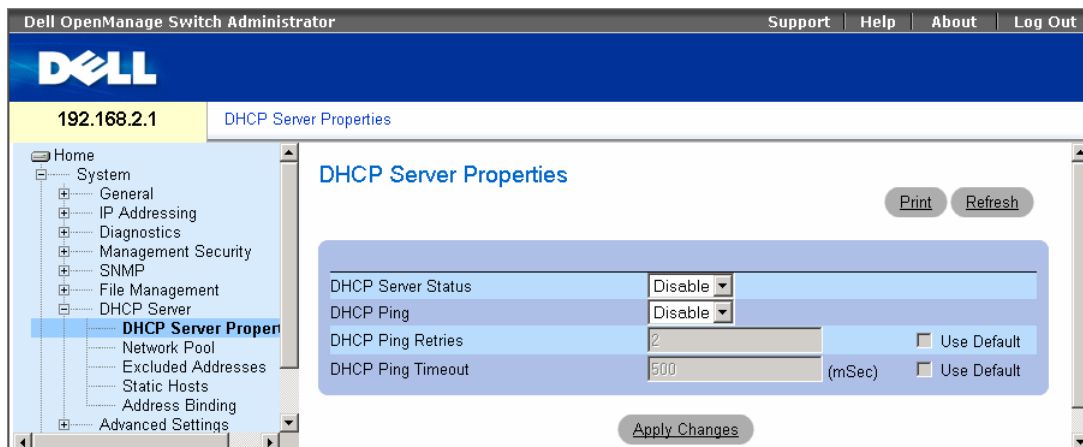
This section contains information for configuring a DHCP server on a DHCP-server-enabled switch.

To open the DHCP Server page, click **System** → **DHCP Server** in the tree view.

Configuring DHCP Properties

The **DHCP Server Properties** page contains fields for enabling the DHCP server and configuring ping capability. The DHCP Server pings a pool address before assigning this address to a requesting client. If the ping is unanswered, the DHCP Server assumes (with a high probability) that the address is not in use and assigns the address to the requesting client. To open the **DHCP Server Properties** page, click **System** → **DHCP Server** → **DHCP Server Properties** in the tree view.

Figure 6-24. DHCP Server Properties



- **DHCP Server Status** — Indicates if the DHCP server is enabled. The possible field values are:
 - **Enable** — Enables the DHCP server.
 - **Disable** — Disables the DHCP server. This is the default value.

- **DHCP Ping** — Indicates if the DHCP server is set to ping the offered IP address before responding to a client request, to ensure that the address is not in use. The possible field values are:
 - **Enable** — Enables ping on the DHCP server.
 - **Disable** — Disables ping on the DHCP server. This is the default value.
- **DHCP Ping Retries**— Optionally specifies the number of pings that are sent before an IP address can be assigned to a requesting client. The range is 1 to 10 and the default value is two.
 - **Use Default** — Reverts to the default Ping Retries setting (2 retries).
- **DHCP Ping Timeout**— Optionally specifies the amount of time (in milliseconds) the DHCP server waits for a ping reply before it stops attempting to reach a pool address, prior to assigning this address to a requesting client. Default timeout is 500 milliseconds.
 - **Use Default** — Reverts to the default Ping Timeout (500 milliseconds).

Enabling the DHCP Server

- 1 Open the **DHCP Server Properties** page.
- 2 Select **Enable** in the **DHCP Server Status** field.
- 3 Optionally, select **Enable** in the **DHCP Ping** field to enable ping globally.
- 4 Define the number of ping retries in the **DHCP Ping Retries** field, or click **Use Default** to select the default number of two retries.
- 5 Define the amount of time (in milliseconds) the DHCP server waits for a ping reply in the **DHCP Ping Timeout** field, or click **Use Default** to select the default timeout of 500 milliseconds.
- 6 Click **Apply Changes**.

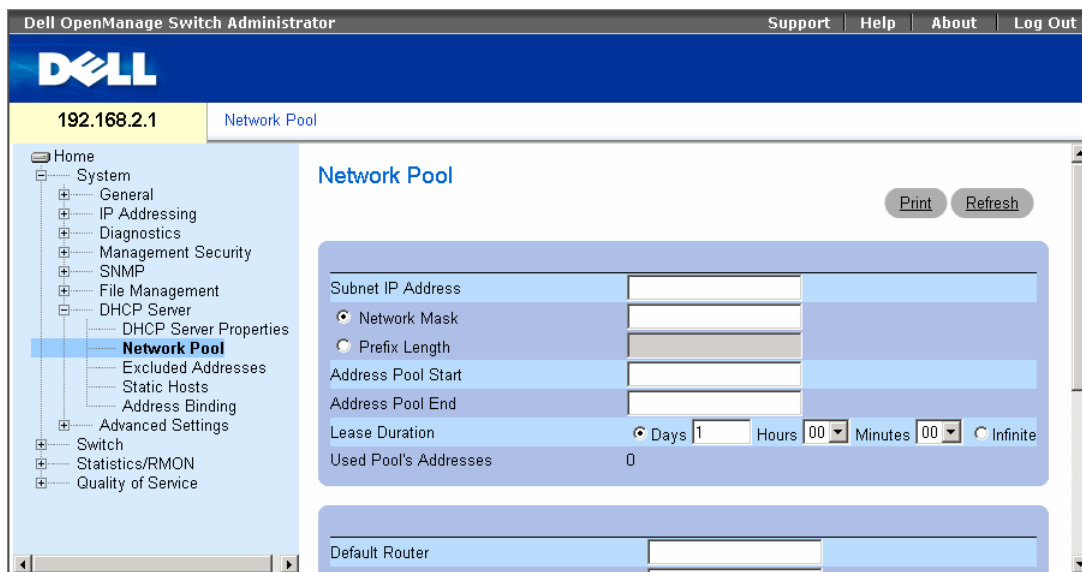
The server is enabled.

Defining Network Pool

The **Network Pool** page displays the DHCP Server's created pool name. The pool name, which is typically assigned to a network segment, consists of an IP address range from which the DHCP Server allocates IP addresses to DHCP clients. You can define the lease duration of the network pool.

To open the **Network Pool** page, click **System** → **DHCP Server** → **Network Pool** in the tree view.

Figure 6-25. Network Pool



- **Subnet IP Address** — Specifies the IP address of the subnet in which the network pool resides.
- **Network Mask** — Specifies the pool's network mask.
- **Prefix Length** — Specifies the number of bits that comprise the address prefix.
- **Address Pool Start** — Specifies the first IP address in the range of the network pool.
- **Address Pool End** — Specifies the last IP address in the range of the network pool.
- **Lease Duration** — Specifies the amount of time a DHCP client can use an IP address from this pool. The total lease duration is 4294967295 seconds, i.e. 49710.2696 days. Thus a lease of 49710 days, 0 hours, 0 minutes and 0 seconds is a legal value, while a lease of 49710 days, 23 hours, 59 minutes and 59 seconds results in an Out of Range alert.
 - **Days** — Specifies the duration of the lease in number of days. The range is 0 to 49710 days.
 - **Hours** — Specifies the number of hours in the lease. A days value must be supplied before an hours value can be added. The range is 0 to 23 hours.
 - **Minutes** — Specifies the number of minutes in the lease. A days value and an hours value must be added before a minutes value can be added. The range is 0 to 59 minutes.
 - **Infinite** — Specifies that the duration of the lease is unlimited.
- **Used Pool's Addresses** — Specifies the number of the pool's addresses that are currently used.
- **Default Router** — Specifies the default router for the DHCP client.
- **Domain Name Server** — Specifies the DNS server available to the DHCP client.

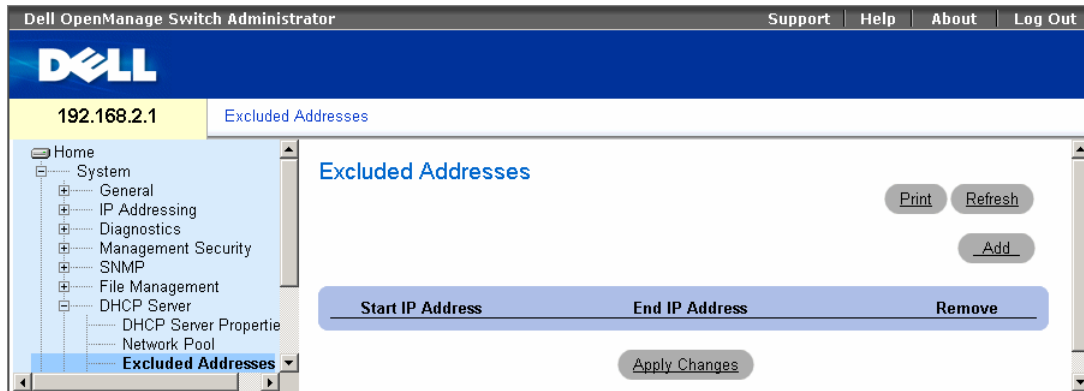
- **Domain Name** — Specifies the domain name for a DHCP client. The domain name may contain up to 32 characters.
- **NetBIOS WINS Server** — Specifies the NetBIOS WINS name server available to a DHCP client.
- **NetBIOS Node Type** — A parameter that informs the workstation how to resolve the NetBIOS name. Valid node types are:
 - **Blank** — The workstation is not informed as to what type of NetBIOS node the client is.
 - **Broadcast** — IP broadcast messages are used to register and resolve NetBIOS names to IP addresses.
 - **Peer-to-Peer** — Point-to-point communications with a NetBIOS name server are used to register and resolve computer names to IP addresses.
 - **Mixed** — A combination (mix) of b-node and p-node communications is used to register and resolve NetBIOS names. M-node first uses b-node; then, if necessary, p-node. M-node is typically not the best choice for larger networks because its preference for b-node broadcasts increases network traffic.
 - **Hybrid** — A hybrid combination of b-node and p-node is used. When configured to use h-node, a computer always tries p-node first and uses b-node only if p-node fails. This is the default.
- **SNTP Server** — Specifies the time server for the DHCP client.
- **Next Server** — Specifies the IP address of the next server in the boot process of a DHCP client. If the next server in the boot process is not configured, the DHCP Server uses inbound interface helper addresses as boot servers.
- **Next Server Name** — Specifies the name of the next server in the boot process. The server name may contain up to 64 characters.
- **Image File Name** — Specifies the name of the file that is used as a boot image. The file name may contain up to 128 characters.

Excluding Addresses

By default, the DHCP Server assumes that all pool addresses may be assigned to DHCP clients. The user can specify IP addresses that must not be used. These addresses are referred to as excluded addresses. A single IP address or a range of IP addresses can be excluded.

The **Excluded Addresses** page lists the excluded addresses. To open the **Excluded Addresses** page, click **System** → **DHCP Server** → **Excluded Addresses** in the tree view.

Figure 6-26. Excluded Addresses



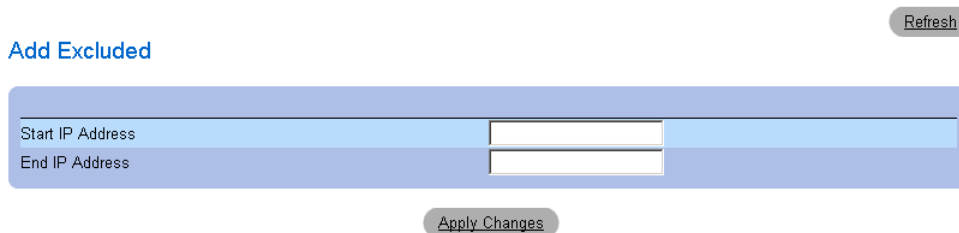
- **Start IP Address** — Displays the first IP address in the range of excluded IP addresses.
- **End IP Address** — Displays the last IP address in the range of excluded IP addresses.

Adding an Excluded Address

- 1 Open the **Excluded Addresses** page.
- 2 Click **Add**.

The **Add Excluded** page opens:

Figure 6-27. Add Excluded



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

The address is excluded, and the device is updated.

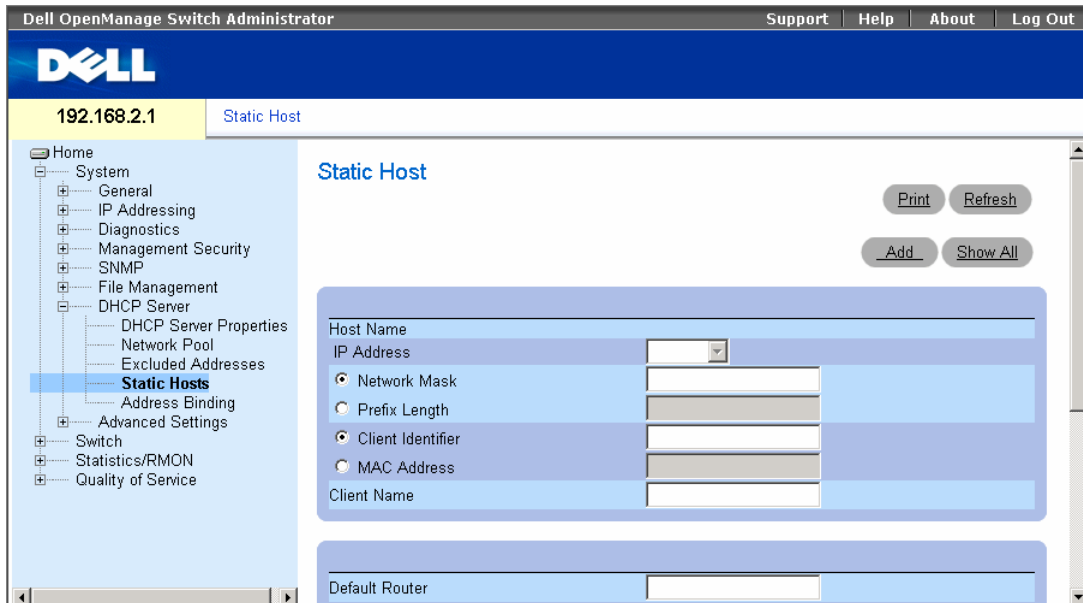
Deleting Excluded Addresses

- 1 Open the **Excluded Addresses** page.
- 2 Check the **Remove** checkbox next to an address.
- 3 Click **Apply Changes**. The address is deleted, and the device is updated.

Manually Allocating IP Addresses (Static Hosts)

The **Static Hosts** page is used to manually allocate IP addresses to network hosts. To open the **Static Hosts** page, click **System** → **DHCP Server** → **Static Hosts** in the tree view.

Figure 6-28. Static Hosts



- **Host Name** — Indicates the host pool name, which can be a string of symbols and an integer (for example, piy4). The range is up to 32 characters.
- **IP Address** — Specifies the IP address that was statically assigned to the host.
- **Network Mask** — Specifies the pool's network mask.
- **Prefix Length** — Specifies the number of bits that comprise the address prefix.
- **Client Identifier** — A unique identification of the client specified in dotted hexadecimal notation, e.g., 01b6.0819.6811.72.
- **MAC Address** — Specifies the MAC Address of DHCP static host.
- **Client Name** — Specifies the name of the client, using a standard set of ASCII characters. The client name must not include the domain name. The range is up to 32 characters.
- **Default Router** — Specifies the default router for the DHCP static host.
- **Domain Name Server** — Specifies the DNS server available to the DHCP client.
- **Domain Name** — Specifies the domain name for a DHCP static host. The domain name may contain up to 32 characters.

- **NetBIOS WINS Server** — Specifies the NetBIOS WINS name server available to a Microsoft DHCP static host.
- **NetBIOS Node Type** — Informs the workstation how to resolve the NetBIOS name. Valid node types are:
 - **Blank** — The workstation is not informed as to which type of NetBIOS node the client is.
 - **Broadcast** — IP broadcast messages are used to register and resolve NetBIOS names to IP addresses.
 - **Peer-to-Peer** — Point-to-point communications with a NetBIOS name server are used to register and resolve computer names to IP addresses.
 - **Mixed** — A combination (mix) of b-node and p-node communications is used to register and resolve NetBIOS names. M-node first uses b-node; then, if necessary, p-node. M-node is typically not the best choice for larger networks because its preference for b-node broadcasts increases network traffic.
 - **Hybrid** — A hybrid combination of b-node and p-node is used. When configured to use h-node, a computer always tries p-node first and uses b-node only if p-node fails. This is the default.
- **SNTP Server** — Specifies the time server for the DHCP static host.
- **Next Server** — Specifies the IP address of the next server in the boot process of a DHCP client. If the next server in the boot process is not configured, the DHCP Server uses inbound interface helper addresses as boot servers.
- **Next Server Name** — Specifies the name of the next server in the boot process. The server name may contain up to 64 characters.
- **Image File Name** — Specifies the name of the file that is used as a boot image. The file name may contain up to 128 characters.

Adding a new Static Host

- 1** Open the **Static Hosts** page.
- 2** Click **Add**.

The **Add Static Host** page opens:

Figure 6-29. Add Static Host

[Refresh](#)

Add Static Host

Host Name	<input type="text"/>
IP Address	<input type="text"/>
<input checked="" type="radio"/> Network Mask	<input type="text"/>
<input type="radio"/> Prefix Length	<input type="text"/>
<input checked="" type="radio"/> Client Identifier	<input type="text"/>
<input type="radio"/> MAC Address	<input type="text"/>
Client Name	<input type="text"/>

Default Router	<input type="text"/>
Domain Name Server	<input type="text"/>
Domain Name	<input type="text"/>
NetBIOS WINS Server	<input type="text"/>
NetBIOS Node Type	<input type="text"/>
SNTTP Server	<input type="text"/>
Next Server	<input type="text"/>
Next Server Name	<input type="text"/>
Image File Name	<input type="text"/>

[Apply Changes](#)

3 Define the relevant fields.

4 Click **Apply Changes**.

The static host is added, and the device is updated.

Displaying Static Hosts Tables

1 Open the **Static Hosts** page.

2 Click **Show All**.

The **Static Hosts Table** page opens:

Figure 6-30. Static Hosts Table

[Refresh](#)

Local User Table

Host Name	IP Address	Network Mask	Client ID Type	Client ID	Remove
-----------	------------	--------------	----------------	-----------	--------

[Apply Changes](#)

Deleting Static Hosts

- 1 Open the **Static Hosts** page.
- 2 Click **Show All**.

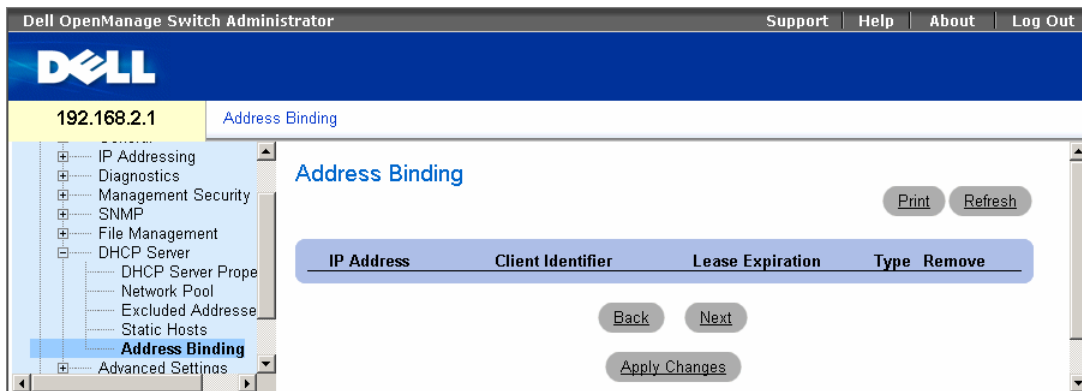
The **Static Hosts Table** page opens.

- 3 Check the **Remove** checkbox next to a static host.
- 4 Click **Apply Changes**. The host is deleted, and the device is updated.

Configuring Address Binding

The **Address Binding** page displays a list of the DHCP server's allocated IP addresses and each IP address's client identifier, lease expiration time, and allocation type. Open the **Address Binding** page, click **System** → **DHCP Server** → **Address Binding** in the tree view.

Figure 6-31. Address Binding



- **IP Address** — Displays the IP addresses of the clients whose bindings are displayed.
- **Client Identifier** — A unique identification of the client specified in dotted hexadecimal notation, e.g., 01b6.0819.6811.72.
- **Lease Expiration** — Displays the lease expiration date and time of the host's IP address.
- **Type** — Displays the manner in which the IP address was assigned to the host:
 - **Static allocation** — The network administrator maps the hardware address of a host to an IP address on the DHCP server.
 - **Permanent allocation** — An IP address received through a standard request-reply mechanism is owned by a client permanently (unless changes in the network environment/connections take place, for any reason).
 - **Dynamic allocation** — A network device obtains a leased IP address for a specified period of time. The IP address is revoked at the end of this period and the switch must request another IP address.

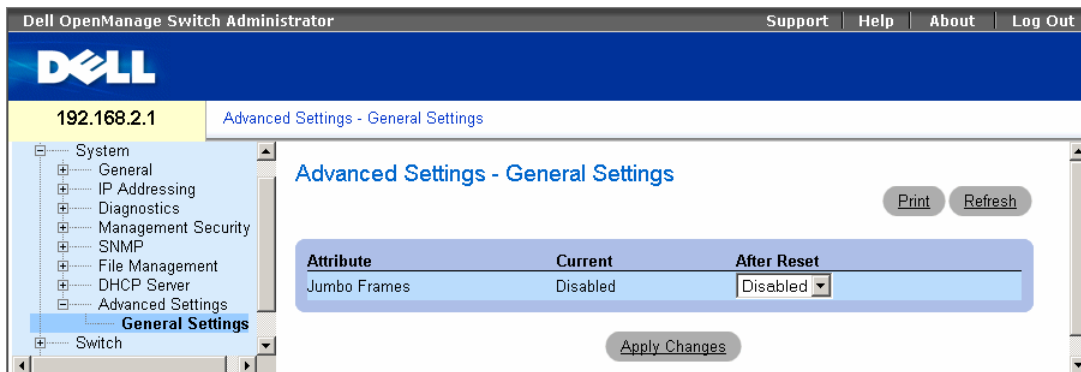
Defining Advanced Settings

The **Advanced Settings** page contains information for configuring general settings. Use **Advanced Settings** to set miscellaneous global attributes for the device. The changes to these attributes are applied only after the device is reset. To open the **Advanced Settings** page, click **System** → **Advanced Settings** in the tree view.

Configuring General Device Parameters

The **General Settings** page provides information for defining general device parameters. To open the **General Settings** page, click **System** → **Advanced Settings** → **General** in the tree view.

Figure 6-32. General Settings



- **Attribute** — The general setting attribute.
- **Current** — The currently configured value.
- **After Reset** — The future (after reset) value.
- **Jumbo Frames** — Enables or disables the Jumbo Frames feature. Jumbo Frames enable the transportation of identical data in fewer frames. This ensures less overhead, lower processing time, and fewer interrupts.

Configuring Device Switching

This section provides all system operation and general information for configuring network security, ports, Address tables, GARP, VLANs, Spanning Tree, Port Aggregation, and Multicast Support.

Configuring Network Security

The device enables network security through both Access Control Lists and Locked Ports.

Port Based Authentication (802.1x)

Port based authentication enables authenticating system users on a per-port basis via a external server. Only authenticated and approved system users can transmit and receive data. Ports are authenticated via the RADIUS server using the Extensible Authentication Protocol (EAP). Port Authentication includes:

- **Authenticators** — Specifies the port that is authenticated before permitting system access.
- **Supplicants** — Specifies host connected to the authenticated port requesting to access the system services.
- **Authentication Server** — Specifies the external server, for example, the RADIUS server that performs the authentication on behalf of the authenticator, and indicates whether the user is authorized to access system services.

Port based authentication creates two access states:

- **Controlled Access** — Permits communication between the user and the system, if the user is authorized.
- **Uncontrolled Access** — Permits uncontrolled communication regardless of the port state.

The device currently supports Port Based Authentication via RADIUS servers.

Advanced Port Based Authentication

Advanced Port Based Authentication enables multiple hosts to be attached to a single port. Advanced Port Based Authentication requires only one host to be authorized for all hosts to have system access. If the port is unauthorized all attached hosts are denied access to the network.

Advanced Port Based Authentication also enables user based authentication. Specific VLANs in the device are always available, even if specific ports attached to the VLAN are unauthorized. For example, Voice over IP does not require authentication, while data traffic requires authentication. VLANs for which authorization is not required can be defined. Unauthenticated VLANs are available to users, even if the ports attached to the VLAN are defined as authorized.

Advanced Port Based Authentication is implemented in the following modes:

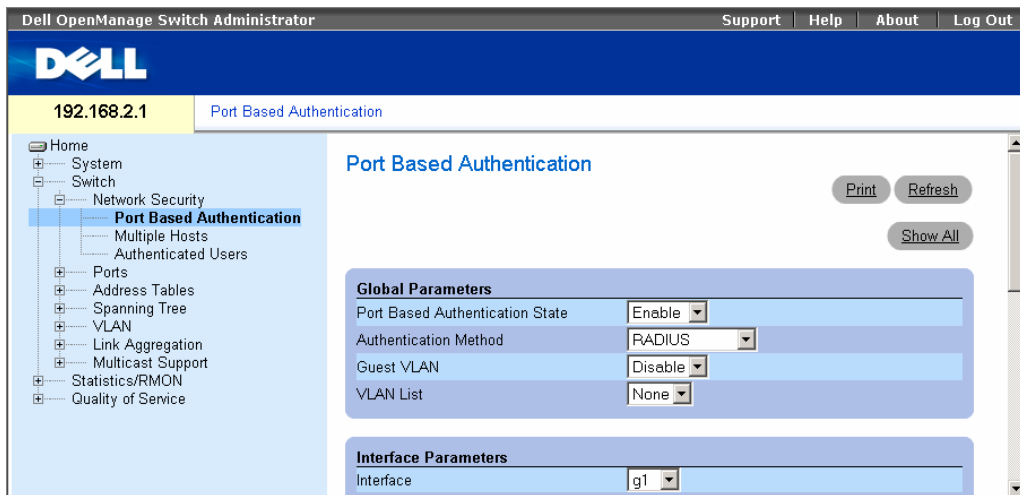
- **Single Host Mode** — Enables only the authorized host for single-session access to the port.
- **Multiple Host Mode** — Enables multiple hosts to be attached to a single port, for single-session access. Only one host must be authorized for all hosts to access the network. If the host authentication fails or an EAPOL-logoff message is received, all attached clients are denied network access.
- **Multiple Session Mode** — Enables only the authorized host for multiple-session access to the port.
- **Guest VLANs** — Provides limited network access to unauthorized 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.

To open the Network Security page select **Switch** → **Network Security**.

Configuring Port Based Authentication

The **Port Based Authentication** page contains fields for configuring port based authentication and for enabling Guest VLANs. To open the **Port Based Authentication** page, click **Switch** → **Network Security** → **Port Based Authentication**.

Figure 7-1. Port Based Authentication



- **Port Based Authentication State** — Permits port based authentication on the device. The possible field values are:
 - **Enable** — Enables port based authentication on the device.
 - **Disable** — Disables port based authentication on the device.
- **Authentication Method** — The Authentication method used. The possible field values are:

- **None** — No authentication method is used to authenticate the port.
- **RADIUS** — Port authentication is performed using the RADIUS server.
- **RADIUS, None** — Port authentication is performed first using the RADIUS server. If the port is not authenticated, then no authentication method is used, and the session is permitted.
- **Guest VLAN** — Specifies whether the Guest VLAN is enabled on the device. The possible field values are:
 - **Enable** — Enables using a Guest VLAN for unauthorized ports. If a Guest VLAN is enabled, the unauthorized port automatically joins the VLAN selected in the VLAN List field.
 - **Disable** — Disables using a Guest VLAN for unauthorized ports. This is the default.
- **VLAN List** — When Guest VLAN is enabled, this field specifies which VLAN the guest will belong to.
- **Interface** — Contains an interface list.
- **User Name** — The user name as configured in the RADIUS server.
- **Admin Interface Control** — Defines the port authorization state. The possible field values are:
 - **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.
 - **ForceAuthorized** — Indicates the interface is in an authorized state without being authenticated. The interface re-sends and receives normal traffic without client port-based authentication.
 - **ForceUnauthorized** — 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 currently configured port authorization state.
- **Authentication Type** — Specifies the type of authentication on the port. The possible field values are:
 - **802.1x Only** — Sets the authentication type to 802.1x based authentication only.
 - **MAC Only** — Sets the authentication type to MAC based authentication only.
 - **802.1x & MAC** — Sets the authentication type to 802.1x based authentication and MAC based authentication.
- **Dynamic VLAN Assignment** — Indicates whether dynamic VLAN assignment is enabled for this port. This feature allows network administrators to automatically assign users to VLANs during the RADIUS server authentication. When a user is authenticated by the RADIUS server, the user is automatically joined to the VLAN configured on the RADIUS server.
 - Port Lock and Port Monitor should be disabled when DVA is enabled.
 - Dynamic VLAN Assignment (DVA) can occur only if a RADIUS server is configured, and port authentication is enabled and set to 802.1x multi-session mode.
 - If the Radius Accept Message doesn't contain the supplicant's VLAN, the supplicant is rejected.
 - Authenticated ports are added to the supplicant VLAN as untagged.

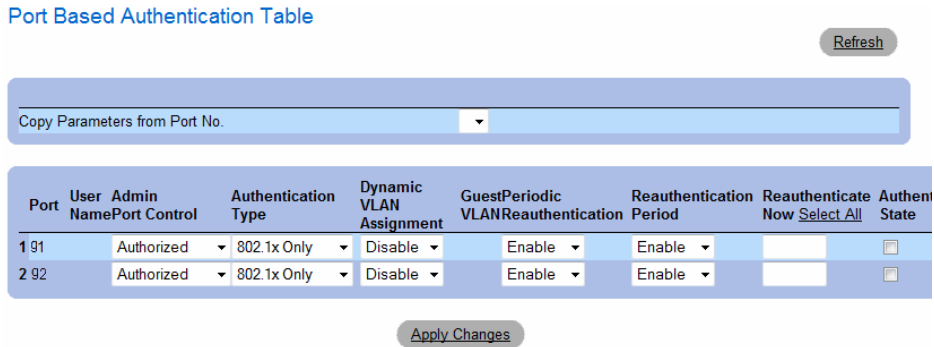
- Authenticated ports remain unauthenticated VLAN and Guest VLAN members. Static VLAN configuration is not applied to the port.
- The following list of VLANs cannot participate in DVA: an Unauthenticated VLAN, a Dynamic VLAN that was created by GVRP, a Voice VLAN, a Default VLAN and a Guest VLAN.
- Network administrators can delete the supplicant VLAN while the supplicant is logged in. The supplicant is authorized during the next re-authentication if this supplicant VLAN is re-created or a new VLAN is configured on the RADIUS server.
- **Guest VLAN** — Specifies whether the Guest VLAN is enabled on the interface.
- **Periodic Reauthentication** — Reauthenticates the selected port periodically, when enabled. The reauthentication period is defined in the **Reauthentication Period (300-4294967295)** field.
- **Reauthentication Period (300-4294967295)** — Indicate the time span in which the selected port is reauthenticated. The field value is in seconds. The field default is 3600 seconds.
- **Reauthenticate Now** — Permits immediate port reauthentication, when selected.
- **Authentication Server Timeout (1-65535)** — Defines the amount of time that lapses before the device resends a request to the authentication server. The field value is in seconds. The field default is 30 seconds.
- **Resending EAP Identity Request (30-65535)** — Defines the amount of time that lapses before EAP request are resent. The field default is 30 seconds.
- **Quiet Period (0-65535)** — The number of seconds that the device remains in the quiet state following a failed authentication exchange. The possible field range is 0-65535. The field default is 60 seconds.
- **Supplicant Timeout (1-65535)** — The amount of time that lapses before EAP requests are resent to the user. The field value is in seconds. The field default is 30 seconds.
- **Max EAP Requests (1-10)** — The total amount of EAP requests sent. If a response is not received after the defined period, the authentication process is restarted. The field default is 2 retries.

Displaying the Port Based Authentication Table

- 1 Display the **Port Based Authentication** page.
- 2 Click **Show All**.

The **Port Based Authentication Table** opens:

Figure 7-2. Port Based Authentication Table



Termination Cause — The reason for which the port authentication was terminated.

Copy To Checkbox — Copies port parameters from one port to the selected ports.

Select All — Selects all ports in the **Port Based Authentication Table**.

Copying Parameters in the Port Based Authentication Table

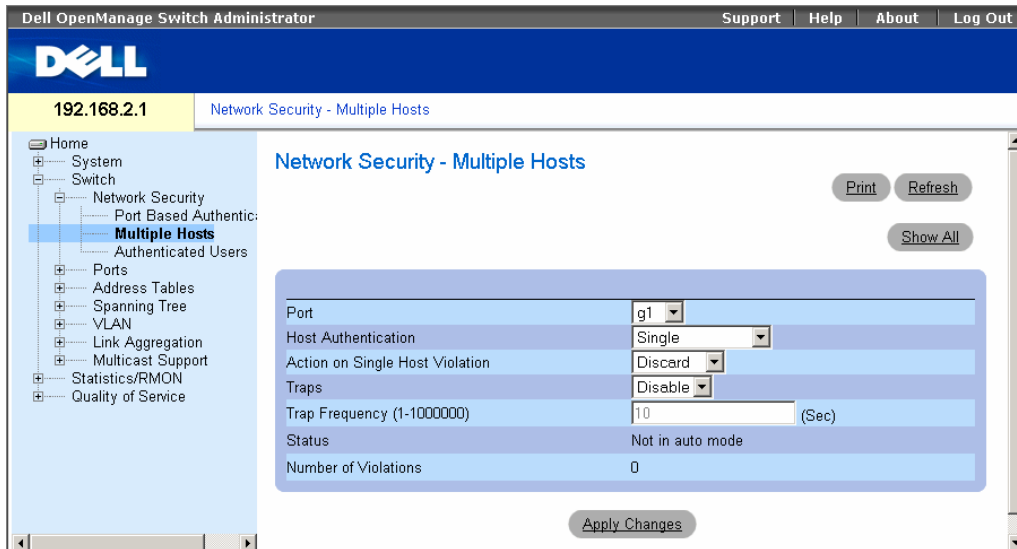
- 1 Open the **Port Based Authentication** page.
- 2 Click **Show All**.
The **Port Based Authentication Table** opens.
- 3 Select the interface in the **Copy Parameters from** field.
- 4 Select an interface in the **Port Based Authentication Table**.
- 5 Select the **Copy to** check box to define the interfaces to which the Port based authentication parameters are copied.
- 6 Click **Apply Changes**.

The parameters are copied to the selected port in the **Port Based Authentication Table**, and the device is updated.

Configuring Advanced Port Based Authentication

The Multiple Hosts page provides information for defining advanced port based authentication settings for specific ports. To open the Multiple Hosts, click Switch → Network Security → Multiple Hosts.

Figure 7-3. Multiple Hosts



- **Port** — The port number for which Advanced Port Based Authentication is enabled.
- **Host Authentication** — Defines the host authentication type. The possible fields are:
 - **Single** — Enables a single authorized host for single-session access to the system.
 - **Multiple Host** — Enables a single host to authorize multiple hosts for single-session access to the system.
 - **Multiple Session** — Enables a single authorized host for multiple-session access to the system.
- **Action on Single Host Violation** — Defines the action to be applied to packets arriving in single-host mode, from a host whose MAC address is not the client (supplicant) MAC address. The **Action on Single Host Violation** field can be defined only if the **Multiple Hosts** field is defined as **Disable**. The possible field values are:
 - **Forward** — Forwards the packets from an unknown source, however, the MAC address is not learned.
 - **Discard** — Discards the packets from any unlearned source. This is the default value.
 - **Shutdown** — Discards the packet from any unlearned source and locks the port. Ports remain locked until they are activated, or the device is reset.
- **Traps** — Enables or disables sending traps to the host if a violation occurs.

- **Trap Frequency (1-1000000) (Sec)** — Defines the time period by which traps are sent to the host. The **Trap Frequency (1-1000000)** field can be defined only if the **Multiple Hosts** field is defined as **Disable**. The default is 10 seconds.
- **Status** — The host status. The possible field values are:
 - **Unauthorized** — Clients (supplicants) have full port access.
 - **Authorized** — Cents (supplicants) have limited port access.
- **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

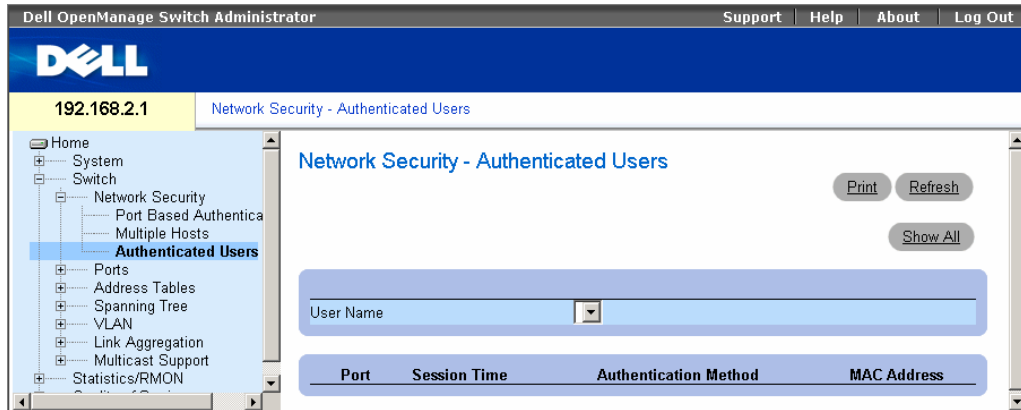
[Refresh](#)

Port	Host Authentication	Action on Violation	Enable Traps	Trap Frequency	Status	Number of Violations
1 g1	Single	Discard	<input type="checkbox"/>	10	Not in auto mode	0
2 g2	Single	Discard	<input type="checkbox"/>	10	Unauthorized	0
3 g3	Single	Discard	<input type="checkbox"/>	10	Unauthorized	0
4 n4	Single	Discard	<input type="checkbox"/>	10	Unauthorized	0

Authenticating Users

The **Authenticated Users** page displays user port access lists. To open the **Authenticated Users** page, click **Switch** → **Network Security** → **Authenticated Users**.

Figure 7-5. Authenticated Users



- **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 client (supplicant) MAC address.

Displaying the Authenticated Users Table

- 1 Open the **Add User Name** page.
- 2 Click **Show All**.

The **Authenticated Users Table** opens:

Figure 7-6. Authenticated Users Table

Authenticated Users Table

User Name	Port	Session Time	Authentication Method	MAC Address
-----------	------	--------------	-----------------------	-------------

[Refresh](#)

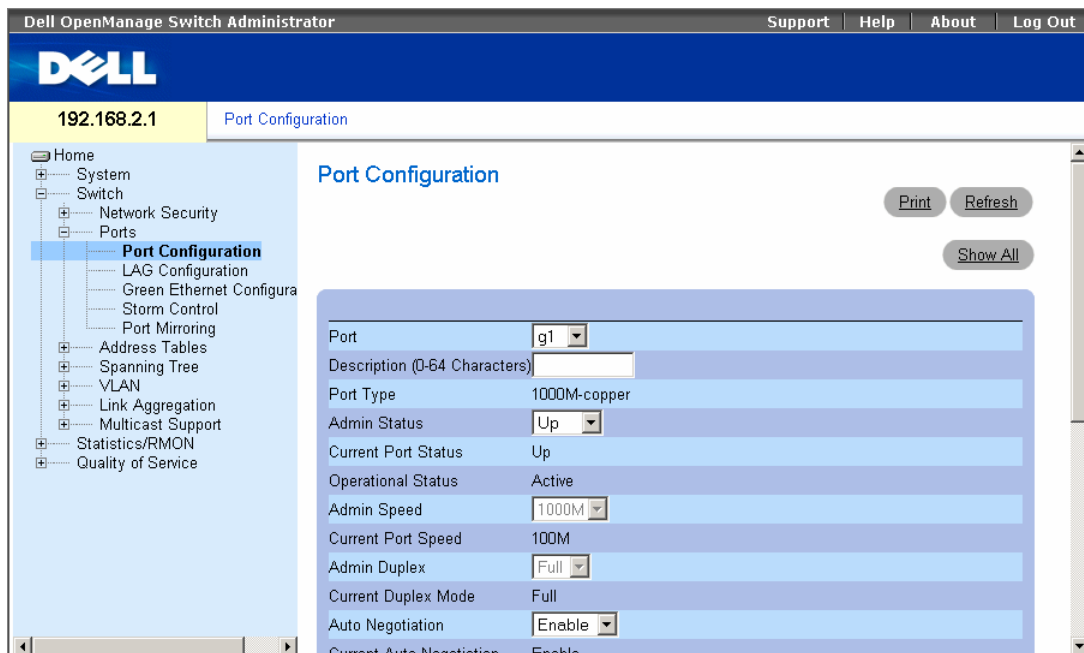
Configuring Ports

The **Ports** page contains links to port functionality pages including advanced features, such as Green Ethernet, Storm Control and Port Mirroring. To open the **Ports** page, click **Switch** → **Ports**.

Defining Port Parameters

The **Port Configuration** page contains fields for defining port parameters. To open the **Port Configuration** page, click **Switch** → **Ports** → **Port Configuration** in the tree view.

Figure 7-7. Port Configuration



- **Port** — The port number for which port parameters are defined.
- **Description (0-64 Characters)** — A brief interface description, such as Ethernet.
- **Port Type** — The type of port.
- **Admin Status** — Enables or disables traffic forwarding through the port. The new port status is displayed in the **Current Port Status** field.
- **Current Port Status** — Specifies whether the port is currently operational or non-operational.
- **Operational Status** — The port operational status. Possible field values are:
 - **Active** — The port is currently active and is currently receiving and transmitting traffic.
 - **Disable** — The port is currently disabled, and is not currently receiving or transmitting traffic.

- **Admin Speed** — The configured rate for the port. The port type determines what speed setting options are available. Admin speed can only be designated when auto negotiation is disabled on the configured port.
- **Current Port Speed** — The actual currently configured port speed (bps).
- **Admin Duplex** — The port duplex mode can be either **Full** or **Half**. **Full** indicates that the interface supports transmission between the device and its link partner in both directions simultaneously. **Half** indicates that the interface supports transmission between the device and the client in only one direction at a time.
- **Current Duplex Mode** — The currently configured port duplex mode.
- **Auto Negotiation** — Enables Auto Negotiation on the port. Auto Negotiation is a protocol between two link partners that enables a port to advertise its transmission rate, duplex mode and flow control abilities to its partner.
- **Current Auto Negotiation** — The currently configured Auto Negotiation setting.
- **Admin Advertisement** — The speed that the port advertises. Options include Maximum Capacity, 10 10 MB Full-Duplex, 100 MB Half-Duplex, 100 MB Full-Duplex and 1000 MB Full-Duplex.
- **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.
- **Current Back Pressure** — The currently configured Back Pressure setting.
- **Flow Control** — Enables or disables flow control or enables the auto negotiation of flow control on the port. Operates when port is in **Full** duplex mode.
- **Current Flow Control** — The currently configured Flow Control setting.
- **MDI/MDIX** — Allows the device to decipher between crossed and uncrossed cables.

Hubs and switches are deliberately wired opposite the way end stations are wired, so that when a hub or switch is connected to an end station, a straight through Ethernet cable can be used, and the pairs are match up properly. When two hubs/switches are connected to each other, or two end stations are connected to each other, a crossover cable is used ensure that the correct pairs are connected. The possible field values are:

- **Auto** — Used to automatically detect the cable type.
- **MDI (Media Dependent Interface)** — Used for end stations.
- **MDIX (Media Dependent Interface with Crossover)** — Used for hubs and switches.
- **Current MDI/MDIX**— The currently configured device MDI/MDIX settings.
- **LAG** — Specifies if the port is part of a LAG.

Defining Port Parameters

- 1 Open the **Port Configuration** page.
- 2 Select a port in the **Port** Field.
- 3 Define the remaining fields.
- 4 Click **Apply Changes**.

The port parameters are saved to the device.

Modifying Port Parameters

- 1 Open the **Port Configuration** page.
- 2 Select a port in the **Port** Field.
- 3 Modify the remaining fields.
- 4 Click **Apply Changes**.

The port parameters are saved to the device.

Displaying the Port Configuration Table:

- 1 Open the **Port Configuration** page.
- 2 Click **Show All**.

The **Ports Configuration Table** opens:

Figure 7-8. Ports Configuration Table

Port Configuration Table

Port	Port Type	Port Status	Port Speed	Duplex Mode	Auto Negotiation	Back Pressure
g1	1000M-copper	Up	1000M	Full	Enable	Disable
		Up	100M	Full	Enable	Disable
g2	1000M-copper	Up	1000M	Full	Enable	Disable
		Down				
g3	1000M-copper	Up	1000M	Full	Enable	Disable

Aggregating Ports

Load Balancing enables the even distribution of data and/or processing packets across available network resources. For example, load balancing may distribute the incoming packets evenly to all servers, or redirect the packets to the next available server. Load Balancing is configured on the "**LAG Configuration**" on page 106 page.

LAGs can be configured according to the following load balancing types: Layer 2, or Layer 2 and Layer 3 or Layer3.

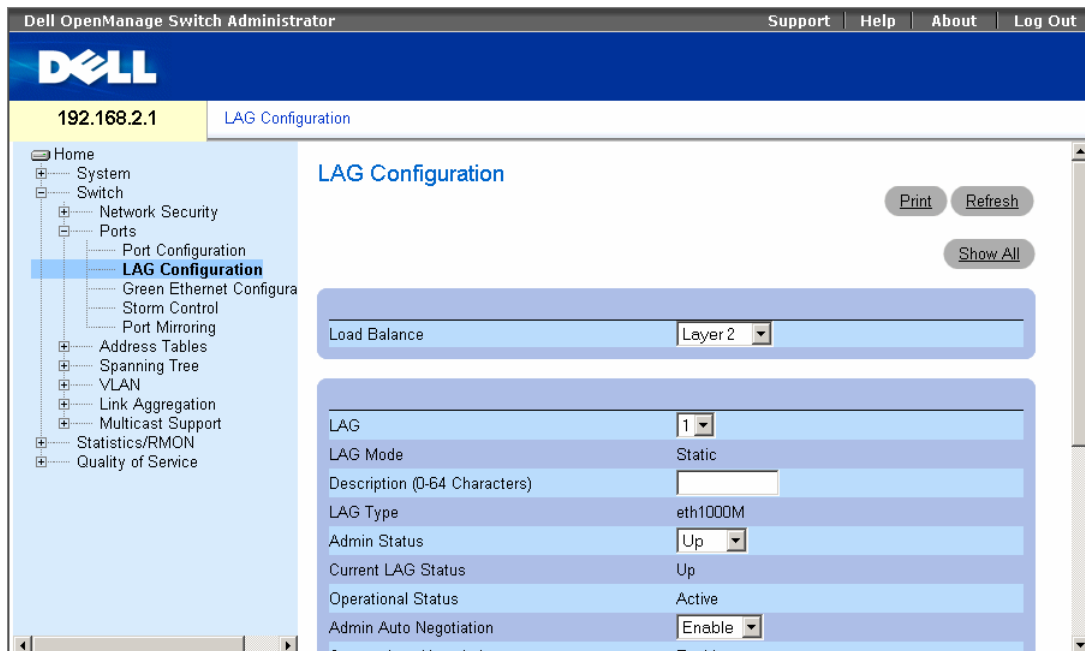
The LAG Configuration page contains fields for configuring parameters for configured LAGs. The device supports up to four LAGs, each having six members.

For information about Link Aggregated Groups and assigning ports to LAGs, refer to **Aggregating Ports**.

To open the LAG Configuration page, click **Switch**→**Ports**→**LAG Configuration** in the tree view.

If port configuration is modified while the port is a LAG member, the configuration change is only effective after the port is removed from the LAG.

Figure 7-9. LAG Configuration



The LAG Configuration page contains the following fields:

- **Load Balance** — Indicates the load balancing type enabled on the LAG. The possible field values are:
 - **Layer 2** — Enables load balancing based on static and dynamic MAC addresses.
 - **Layer 3** — Enables load balancing based on source and destination IP addresses.
 - **Layer 2-3** — Enables load balancing based on static and dynamic MAC addresses, and source and destination IP addresses.
- **LAG** — The LAG number.
- **LAG Mode** — Indicates that the LAG mode is static.
- **Description (0-64 Characters)** — Provides a user-defined description of the configured LAG.
- **LAG Type** — The port types that comprise the LAG.

- **Admin Status** — Enables or disables traffic forwarding through the selected LAG.
- **Current LAG Status** — Indicates if the LAG is currently operating.
- **Operational Status** — Operational status of the LAG.
- **Admin Auto Negotiation** — Enables or disables Auto Negotiation on the LAG. Auto-negotiation is a protocol between two link partners that enables a LAG to advertise its transmission rate and flow control (the flow control default is enabled) abilities to its partner.
- **Current Auto Negotiation** — The currently configured Auto Negotiation setting.
- **Admin Speed** — The speed at which the LAG is operating.
- **Current LAG Speed** — The currently configured speed at which the LAG is operating.
- **Admin Advertisement** — The speed that the LAG advertises. Options include Maximum Capacity, 10 MB Half-Duplex, 10 MB Full-Duplex, 100 MB Full-Duplex and 1000 MB Full-Duplex.
- **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.
- **Admin Flow Control** — Enables/disables flow control, or enables the auto negotiation of flow control on 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 7-10. LAG Configuration Table
LAG Configuration Table

LAG	Description	LAG Type	LAG Status	LAG Speed	Auto Negotiation	Flow Control
1		eth1000M	Up		Enable	Enable
2		eth1000M	Up	100M	Enable	On
3			Down		Enable	Enable
4			Up		Enable	Enable

Configuring Green Ethernet

Green Ethernet, also known as Energy Efficient Ethernet, is an effort to make networking equipment environmentally friendly, specifically by reducing power usage of Ethernet connections. The following methods are supported by the device:

- **Energy-Detect** — Auto-detection of inactivity on a port, and subsequent turning down of transmit power. It may take about 1 second for the cable to power-up when it becomes active again.
- **Short-Reach** — Reduction of power over Ethernet cables shorter than 40m. The cable length is detected automatically with an accuracy of +/- 10m.

These methods are relevant for copper cables only, and are incompatible with fiber cable or when the link is set to auto-selection of copper/fiber.

The short-reach method is only for a link established at 1 Gigabyte, and is not compatible with Fast Ethernet.

To open the **Green Ethernet Configuration** page, click **Switch**→ **Ports**→ **Green Ethernet Configuration** in the tree view.

Figure 7-11. Green Ethernet Configuration

Green Ethernet Configuration

Cumulative Energy Saved: 352 W * H

Link Down Energy Saving Mode: On

Link Short-Reach Energy Saving Mode: On

Current Power Consumption: mW

Power Saving: 15%

Green Ethernet Ports Table

Port	Energy-Detect			Short-Reach			Cable Length
	Admin	Oper	reason	Admin	Oper	reason	
1 g1	on	off	LinkType	on	off	LinkType	
1 g2	on	off	LinkUp	on	off	LinkSpeed	
1 g3	on	on		on	on		20

- **Cumulative Energy Saved** — The total amount of energy saved since the last reset. This amount is equal to the saved power multiplied by the time period in hours.
 - **Reset** — Click to set the Cumulative Power Saved counter back to 0.
- **Link Down Energy Saving Mode** — Indicates whether the Energy-Detect energy saving mode is on or off for the device ports.
- **Link Short-Reach Energy Saving Mode** — Indicates whether the Short-Reach energy saving mode is on or off for the device ports.
- **Current Power Consumption** — The power currently consumed by all ports (including both those with links up and links down).
- **Power Saving** — The percentage of power saved. For example, a Power Saving value of 14% indicates that just 86% of the power that would normally be used (without Green Ethernet) is currently being used.

The Green Ethernet Ports Table includes the following port energy saving information:

- **Port** — Indicates the port.
- **Energy-Detect** — The status of the Energy-Detect mode on the link:
 - **Admin** — Whether the Energy-Detect has been enabled for the port.
 - **Oper** — Whether Energy-Detect is currently in force for the port.
 - **Reason** — If Admin indicates that Energy-Detect is enabled and Oper indicates it is not in force, this column gives the reason. Reasons may include that the Link Type is not supported, or that the Port Link is up.
- **Short-Reach** — The status of the Short-Reach mode on the link:
 - **Admin** — Whether the Short-Reach has been enabled for the port.
 - **Oper** — Whether Short-Reach is currently in force for the port.
 - **Reason** — If Admin indicates that Short-Reach is enabled and Oper indicates it is not in force, this column gives the reason. Reasons may include that the Link Type is not supported, that the Link Speed is not supported (is fast Ethernet and therefore its cable length cannot be determined by VCT; cable length can be determined on Giga ports only), or that the Port Link is down.
- **Cable Length** — The automatically-detected length of the cable.

Enabling Green Ethernet on the Device

- 1** Open the **Green Ethernet Configuration** page.
- 2** Enable the desired energy saving methods.
- 3** Click **Apply Changes**.

Green Ethernet is enabled on the device.

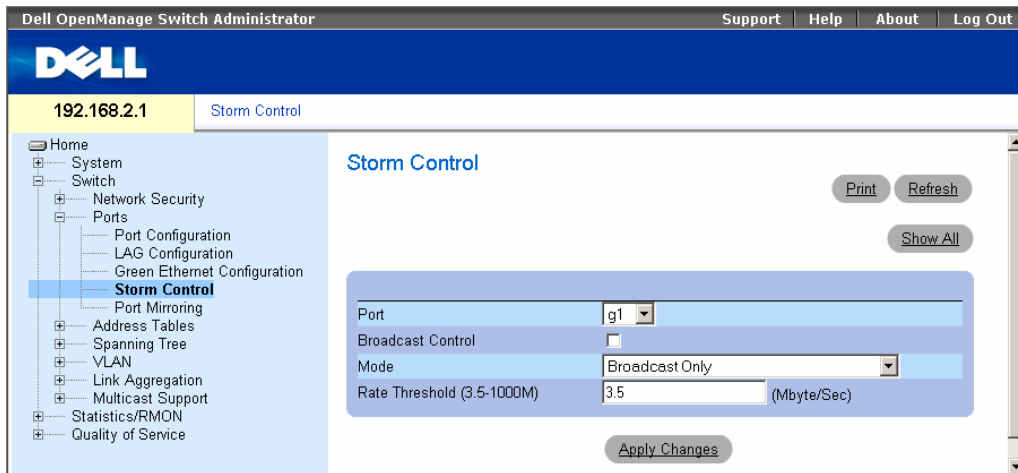
Enabling Storm Control

A Broadcast Storm is a result of an excessive amount of broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses are heaped onto the network, straining network resources or causing the network to time out.

The system measures the incoming unknown Unicast, Broadcast and Multicast frame rate separately on each port, and discard frames when the rate exceeds a user-defined rate.

The **Storm Control** page provides fields for enabling and configuring Storm Control. To open the **Storm Control** page, click **Switch**→ **Ports**→ **Storm Control** in the tree view.

Figure 7-12. Storm Control



- **Port** — The port from which storm control is enabled.
- **Broadcast Control** — Enables or disables forwarding broadcast packet types on the device.
- **Mode** — Specifies the Broadcast mode currently enabled on the device. The possible field value are:
 - **Unknown Unicast, Multicast & Broadcast** — Counts unknown Unicast, Multicast, and Broadcast traffic.
 - **Multicast & Broadcast** — Counts Broadcast and Multicast traffic together.
 - **Broadcast Only** — Counts only Broadcast traffic.
- **Rate Threshold (3.5-1000M)**— The maximum rate (Kbits/Sec) at which packets are forwarded. The range is 3.5-1000M.

Enabling Storm Control on the Device

- 1 Open the **Storm Control** page.
- 2 Select an interface on which to implement storm control.
- 3 Define the fields.
- 4 Click **Apply Changes**.

The Storm Control is enabled on the device.

Displaying the Storm Control Table

- 1 Open the **Storm Control** page.
- 2 Click **Show All**.

The **Storm Control Table** opens:

Figure 7-13. Storm Control Table

Storm Control Table

Refresh

Port	Broadcast Control	Mode	Rate Threshold
g1	Disable	Broadcast Only	3.5
g2	Disable	Broadcast Only	3.5
g3	Disable	Broadcast Only	3.5
g4	Disable	Broadcast Only	3.5
g5	Disable	Broadcast Only	3.5
g6	Disable	Broadcast Only	3.5
g7	Disable	Broadcast Only	3.5
g8	Disable	Broadcast Only	3.5
g9	Disable	Broadcast Only	3.5
g10	Disable	Broadcast Only	3.5
g11	Disable	Broadcast Only	3.5
g12	Disable	Broadcast Only	3.5
g13	Disable	Broadcast Only	3.5
g14	Disable	Broadcast Only	3.5
g15	Disable	Broadcast Only	3.5
g16	Disable	Broadcast Only	3.5
g17	Disable	Broadcast Only	3.5
g18	Disable	Broadcast Only	3.5
g19	Disable	Broadcast Only	3.5
g20	Disable	Broadcast Only	3.5
g21	Disable	Broadcast Only	3.5
g22	Disable	Broadcast Only	3.5
g23	Disable	Broadcast Only	3.5
g24	Disable	Broadcast Only	3.5

Defining Port Mirroring Sessions

Port mirroring monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from one port or a number of ports (source port or ports) to a monitoring (destination) port.

Port mirroring is configured by selecting a specific port to copy all packets, and different ports from which the packets copied. Before configuring Port Mirroring, note the following:

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.

Before configuring Port Mirroring, note the following:

- Monitored port cannot operate faster than the monitoring port.
- All the RX/TX packets should be monitored to the same port.

The following restrictions apply to ports configured to be destination ports:

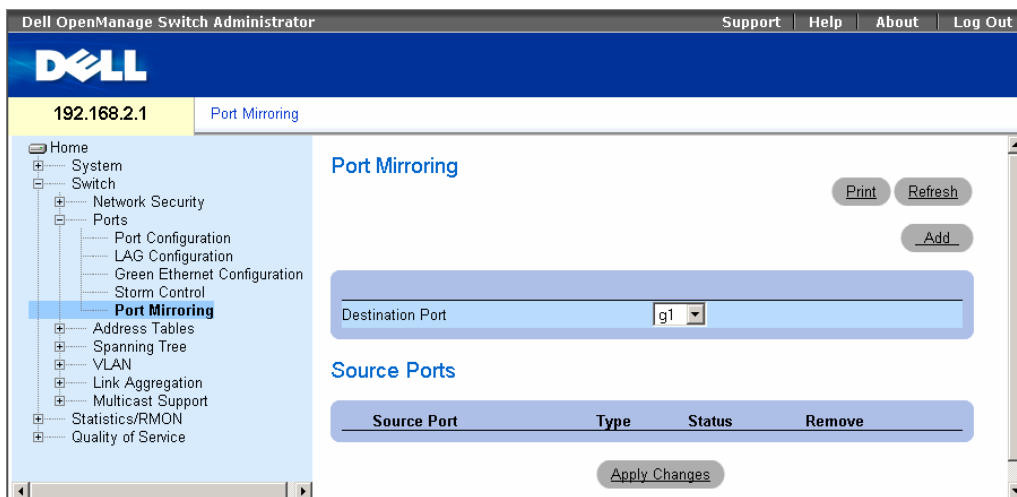
- Ports cannot be configured as a source port.
- Ports cannot be a LAG member.
- IP interfaces are not configured on the port.
- GVRP is not enabled on the port.
- The port is not a VLAN member.
- Only one destination port can be defined.

The following restrictions apply to ports configured to be source ports:

- Source Ports cannot be a LAG member.
- Ports cannot be configured as a destination port.
- All packets are transmitted tagged from the destination port.
- Monitored all RX/TX packets to the same port.

To open the **Port Mirroring** page, click **Switch**→**Ports**→**Port Mirroring** in the tree view.

Figure 7-14. Port Mirroring



- **Destination Port** — The port number to which port traffic is copied.
- **Source Port** — Defines the port number from which port traffic is mirrored.
- **Type** — Indicates if the source port is RX, TX, or both RX and TX.
- **Status** — Indicates if the port is currently monitored (**Active**) or not monitored (**notReady**). There are four monitoring sessions.
- **Remove** — When selected, removes the port mirroring session.

Adding a Port Mirroring Session

- 1 Open the **Port Mirroring** page.
- 2 Click **Add**.
The **Add Source Port** page opens.
- 3 Select the destination port from the **Destination Port** drop-down menu.
- 4 Select the source port from the **Source Port** drop-down menu.
- 5 Define the **Type** field.

6 Click **Apply Changes**.

The new source port is defined, and the device is updated.

Deleting a Copy Port from a Port Mirroring Session

- 1 Open the **Port Mirroring** page.
- 2 Select the **Remove** check box.
- 3 Click **Apply Changes**.

The selected port mirroring session is deleted, and the device is updated.

Configuring Address Tables

MAC addresses are stored in the Dynamic Address database. A packet addressed to a destination stored in the database is forwarded immediately to the port. The Dynamic Address Table can be sorted by interface, VLAN, and interface type. MAC addresses are dynamically learned as packets from sources arrive at the device. Addresses are associated with ports by learning the ports from the frame's source address. Frames addressed to a destination MAC address that is not associated with any port are flooded to all ports of the relevant VLAN. In order to prevent the bridging table from overflowing, dynamic MAC addresses, from which no traffic is seen for a certain period, are erased. To open the **Address Tables** page, click **Switch**→**Address Table** in the tree view.

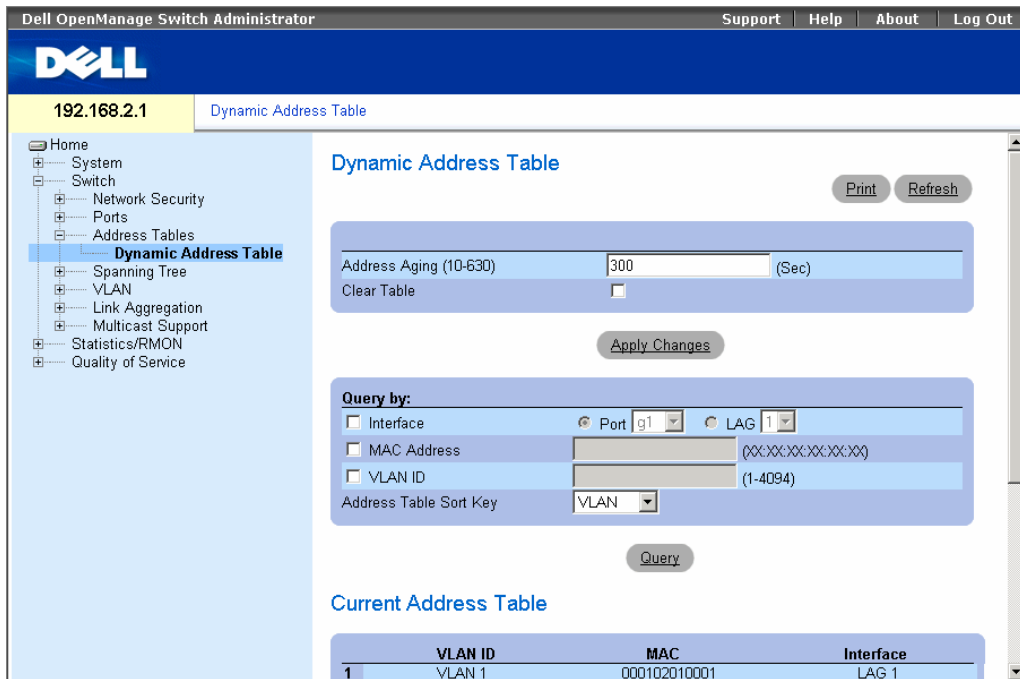
Viewing Dynamic Addresses

The **Dynamic Address Table** contains fields for querying information in the dynamic address table, including the interface type, MAC addresses, VLAN, and table sorting. Packets forwarded to an address stored in the address table are forwarded directly to those ports.

The **Dynamic Address Table** also contains information about the aging time before a dynamic MAC address is erased, and includes parameters for querying and viewing the Dynamic Address list. The **Current Address Table** contains dynamic address parameters by which packets are directly forwarded to the ports.

To open the **Dynamic Address Table**, click **Switch**→**Address Table**→**Dynamic Addresses Table** in the tree view.

Figure 7-15. Dynamic Address Table



- **Address Aging (10-630)** — Specifies the amount of time the MAC Address remains in the **Dynamic Address Table** before it is timed out if no traffic from the source is detected. The default value is 300 seconds.
- **Interface** — Specifies the interface for which the table is queried. There are two interface types from which to select.
 - **Port** — Specifies the port numbers for which the table is queried.
 - **LAG** — Specifies the LAG for which the table is queried.
- **MAC Address** — Specifies the MAC address for which the table is queried.
- **VLAN ID** — Specifies the VLAN ID for which the table is queried.
- **Address Table Sort Key** — Specifies the means by which the Dynamic Address Table is sorted.

Redefining the Aging Time

- 1 Open the **Dynamic Address Table**.
- 2 Define the **Aging Time** field.
- 3 Click **Apply Changes**.

The aging time is modified, and the device is updated.

Querying the Dynamic Address Table

- 1 Open the **Dynamic Address Table**.
- 2 Define the parameter by which to query the **Dynamic Address Table**.
Entries can be queried by **Port**, **MAC Address**, or **VLAN ID**.
- 3 Click **Query**.
The **Dynamic Address Table** is queried.

Sorting the Dynamic Address Table

- 1 Open the **Dynamic Address Table**.
- 2 From the **Address Table Sort Key** drop-down menu, select whether to sort addresses by address, VLAN ID, or interface.
- 3 Click **Query**.
The **Dynamic Address Table** is sorted.

Configuring the Spanning Tree Protocol

Spanning Tree Protocol (STP) provides tree topography for any arrangement of bridges. STP also provides one path between end stations on a network, eliminating loops.

Loops occur when alternate paths exist between hosts. Loops in an extended network can cause bridges to forward traffic indefinitely, resulting in increased traffic and reducing network efficiency.

The devices support the following Spanning Tree protocols:

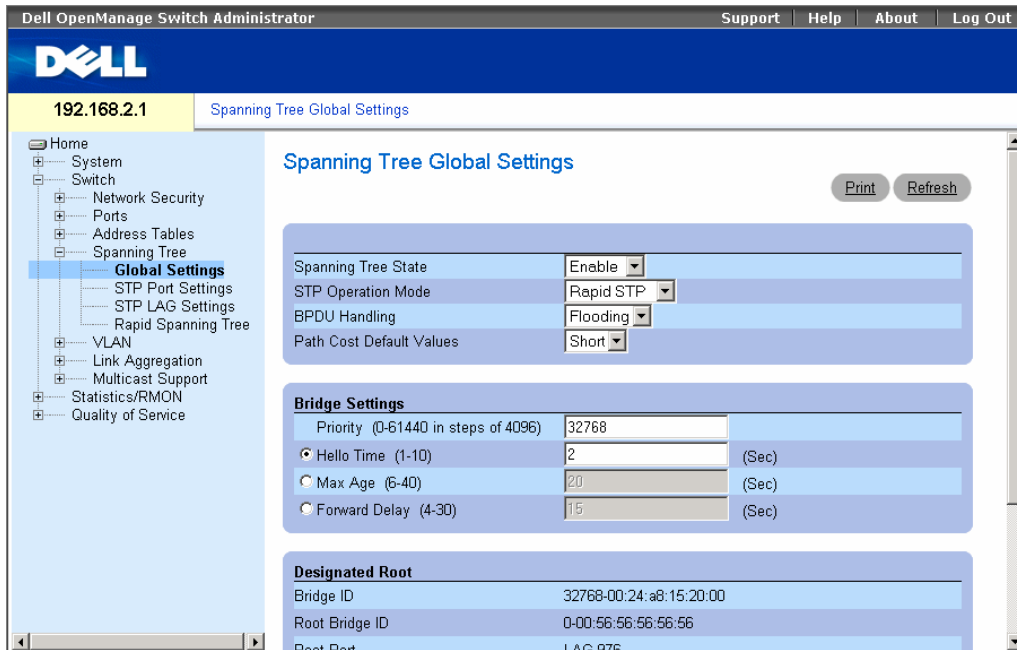
- **Classic STP** — Provides a single path between end stations, avoiding and eliminating loops. For more information on configuring Classic STP, see "Defining STP Global Settings" on page 116.
- **Rapid STP** — Detects and uses of network topologies that provide faster spanning tree convergence, without creating forwarding loops. For more information on configuring Rapid STP, see "Configuring Rapid Spanning Tree" on page 124.

To open the **Spanning Tree** pages, click **Switch**→**Spanning Tree** in the tree view.

Defining STP Global Settings

The **STP Global Settings** page contains parameters for enabling and configuring STP operation on the device. To open the **STP Global Settings** page, click **Switch**→**Spanning Tree** →**Global Settings** in the tree view.

Figure 7-16. STP Global Settings



- **Spanning Tree State** — Enables or disables Spanning Tree on the device. The possible field values are:
 - **Enable** — Enables Spanning Tree
 - **Disable** — Disables Spanning Tree
- **STP Operation Mode** — The STP mode by which STP is enabled on the device. The possible field values are:
 - **Classic STP** — Enables Classic STP on the device. This is the default value.
 - **Rapid STP** — Enables Rapid STP on the device.
- **BPDU Handling** — Determines how BPDU packets are managed when STP is disabled on the port/device. BPDUs are used to transmit spanning tree information. The possible field values are:
 - **Filtering** — Filters BPDU packets when spanning tree is disabled on an interface.
 - **Flooding** — Floods BPDU packets when spanning tree is disabled on an interface. This is the default value.
- **Port Cost Default Values** — Determines the Spanning Tree default path cost method. The possible field values are:
 - **Short** — Specifies 1 through 65535 range for port path costs. This is the default value.
 - **Long** — Specifies 1 through 200000000 range for port path costs.

- **Priority (0-61440 in steps of 4096)** — Specifies the bridge priority value. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the switch with the lowest priority value becomes the Root Bridge. The default value is 32768. The bridge priority value is provided in increments of 4096 (4K increments). For example, 0, 4096, 8192, etc.
- **Hello Time (1-10)** — Specifies the device Hello Time. The Hello Time indicates the amount of time in seconds a root bridge waits between configuration messages. The default is 2 seconds.
- **Max Age (6-40)** — Specifies the device Maximum Age Time. The Maximum Age Time indicates the amount of time in seconds a bridge waits before sending configuration messages. The default max age is 20 seconds.
- **Forward Delay (4-30)** — Specifies the device forward delay time. The Forward Delay Time indicates the amount of time in seconds a bridge remains in a listening and learning state before forwarding packets. The default is 15 seconds.
- **Bridge ID** — Identifies the Bridge priority and MAC address.
- **Root Bridge ID** — Identifies the Root Bridge priority and MAC address.
- **Root Port** — The port number that offers the lowest cost path from this bridge to the Root Bridge. It is significant when the Bridge is not the Root. The default is zero.
- **Root Path Cost** — The cost of the path from this bridge to the root.
- **Topology Changes Counts** — Specifies the total amount of STP state changes that have occurred since the last reboot.
- **Last Topology Change** — The amount of time that has elapsed since the bridge was initialized or reset, and the last topographic change occurred. The time is displayed in a day hour minute second format, for example, 0 day 1 hour 34 minutes and 38 seconds.

Defining STP Global Parameters

- 1 Open the **STP Global Settings** page.
- 2 Select the port that needs to be enabled from the **Select a Port** drop-down menu.
- 3 Select **Enable** in the **Spanning Tree State** field.
- 4 Select the STP mode in the **STP Operation Mode** field, and define the bridge settings.
- 5 Click **Apply Changes**.
STP is enabled on the device.

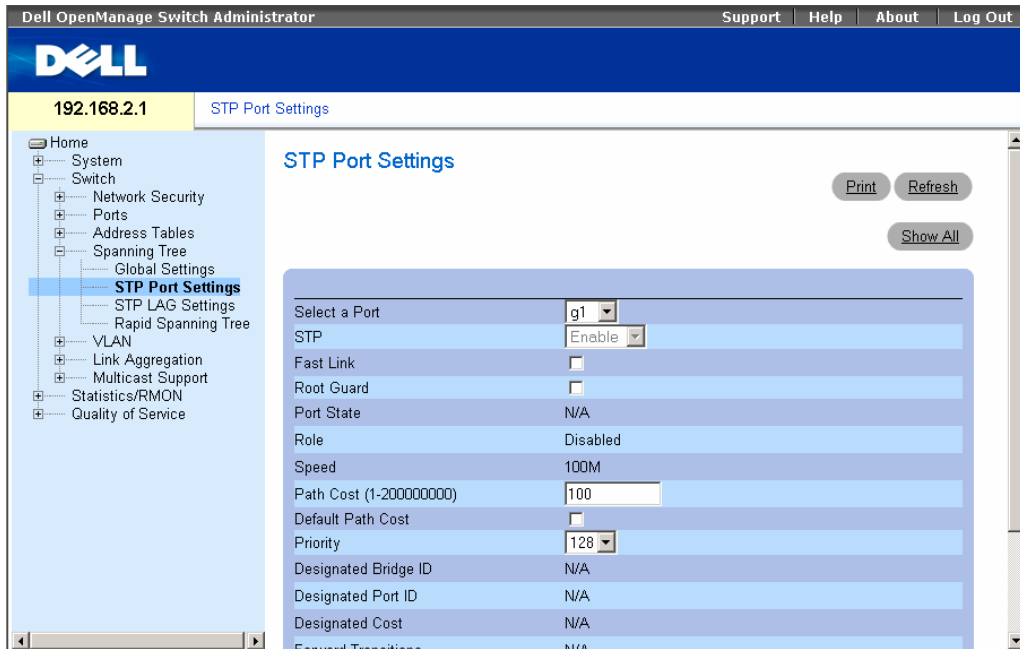
Modifying STP Global Parameters

- 1 Open the **STP Global Settings** page.
- 2 Define the fields in the dialog.
- 3 Click **Apply Changes**.
The STP parameters are modified, and the device is updated.

Defining STP Port Settings

The STP Port Settings page contains fields for assigning STP properties to individual ports. To open the STP Port Settings page, click Switch→ Spanning Tree→ Port Settings in the tree view.

Figure 7-17. STP Port Settings



- **Select a Port** — Port on which STP is enabled.
- **STP** — Enables or disables STP on the port.
- **Fast Link** — When selected, enables Fast Link mode for the port. If Fast Link mode is enabled for a port, the **Port State** is automatically placed in the **Forwarding** state when the port link is up. Fast Link mode optimizes the time it takes for the STP protocol to converge. STP convergence can take 30-60 seconds in large networks.
- **Root Guard** — When checked, prevents devices outside the network core from being assigned the spanning tree root.

- **Port State** — The current port STP state. If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are:
 - **Disabled** — The port link is currently down.
 - **Blocking** — The port is currently blocked and cannot be used to forward traffic or learn MAC addresses. Blocking is displayed when Classic STP is enabled.
 - **Listening** — The port is currently in the listening mode. The port cannot forward traffic nor can it learn MAC addresses.
 - **Learning** — The port is currently in the learning mode. The port cannot forward traffic however it can learn new MAC addresses.
 - **Forwarding** — The port is currently in the forwarding mode. The port can forward traffic and learn new MAC addresses.
- **Role** — Displays the port role assigned by the STP algorithm to provide to STP paths. The possible field values are:
 - **Root** — Provides the lowest cost path to forward packets to the root switch.
 - **Designated** — Indicates the port or LAG through 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, or when a LAN has two or more connections connected to a shared segment.
 - **Disabled** — 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 of the port is automatically set by the port speed and the default path cost method.

The default values for long path costs are:

- **Ethernet** - 2000000
- **Fast Ethernet** - 200000
- **Gigabit Ethernet** - 20000

The default values for short path costs (short path costs are the default) are:

- **Ethernet** - 100
- **Fast Ethernet** - 19
- **Gigabit Ethernet** - 4

- **Priority (0-240, in steps of 16)** — The priority value of the port. The priority value influences the port choice when a bridge has two ports connected in a loop. The priority value is between 0-240. The priority value is provided in increments of 16.
- **Designated Bridge ID** — The bridge priority and the MAC Address of the designated bridge.
- **Designated Port ID** — The selected port's priority and interface.
- **Designated Cost** — The cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
- **Forward Transitions** — The number of times the port has changed from the **Blocking** state to the **Forwarding** state.
- **LAG** — The LAG to which the port is attached.

Enabling STP on a Port

- 1 Open the **STP Port Settings** page.
- 2 Select **Enabled** in the **STP Port Status** field.
- 3 Define the **Fast Link**, **Path Cost**, and the **Priority** fields.
- 4 Click **Apply Changes**.

STP is enabled on the port.

Modifying STP Port Properties

- 1 Open the **STP Port Settings** page.
- 2 Modify the **Priority**, **Fast Link**, **Path Cost**, and the **Fast Link** fields.
- 3 Click **Apply Changes**.

The STP port parameters are modified, and the device is updated.

Displaying the STP Port Table

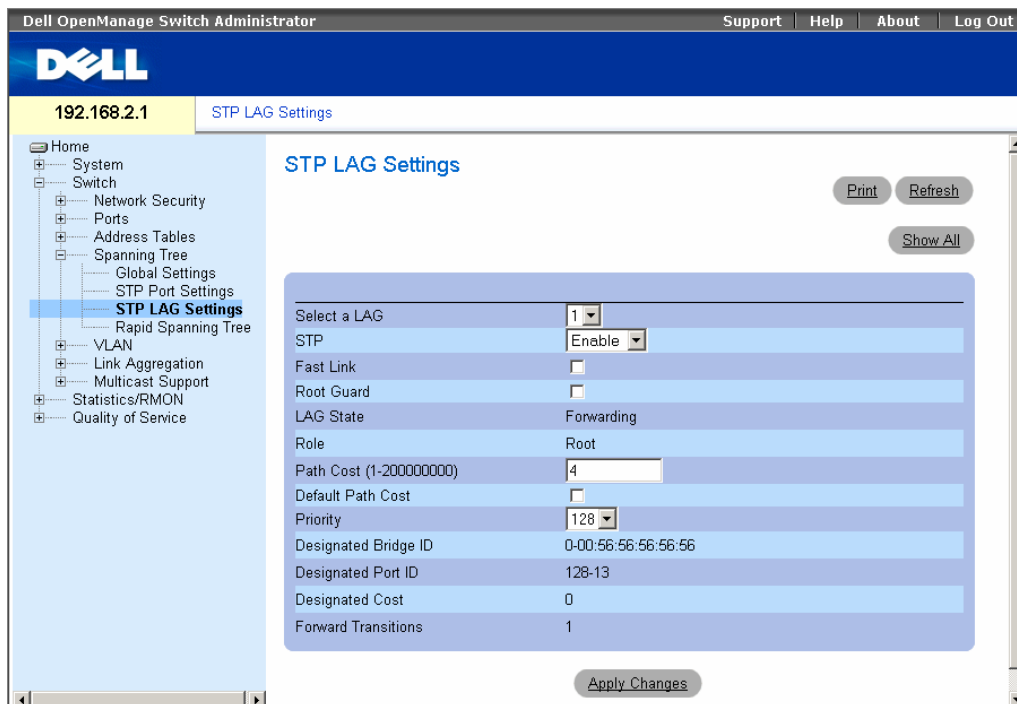
- 1 Open the **STP Port Settings** page.
- 2 Click **Show All**.

The **STP Port Table** opens.

Defining STP LAG Settings

The STP LAG Settings page contains fields for assigning STP aggregating port parameters. To open the STP LAG Settings page, click Switch→ Spanning Tree→ LAG Settings in the tree view.

Figure 7-18. STP LAG Settings



- **Select a LAG** — The user-defined LAG. For more information, see "Defining LAG Membership" on page 134.
- **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.
- **Root Guard** — When checked, prevents devices outside the network core from being assigned the spanning tree root.

- **LAG State** — Current STP state of a LAG. If enabled, the LAG state determines what forwarding action is taken on traffic. If the bridge discovers a malfunctioning LAG, the LAG is placed in the **Broken** state. Possible LAG states are:
 - **Disabled** — The LAG link is currently down.
 - **Blocking** — The LAG is blocked and cannot be used to forward traffic or learn MAC addresses.
 - **Listening** — The LAG is in the listening mode and cannot forward traffic or learn MAC addresses.
 - **Learning** — The LAG is in the learning mode and cannot forward traffic, but it can learn new MAC addresses.
 - **Forwarding** — The LAG is currently in the forwarding mode, and it can forward traffic and learn new MAC addresses.
 - **Broken** — The LAG is currently malfunctioning and cannot be used for forwarding traffic.
- **Role** — Displays the port role assigned by the STP algorithm to provide to STP paths. The possible field values are:
 - **Root** — Provides the lowest cost path to forward packets to the root switch.
 - **Designated** — Indicates the port or LAG through 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, or when a LAN has two or more connections connected to a shared segment.
 - **Disabled** — The port 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 being rerouted. The path cost has a value of 1 to 200000000. If the path cost method is short, the LAG cost default value is 4. If the path cost method is long, the LAG cost default value is 20000.
- **Default Path Cost** — When selected, the LAG path cost returns to its default value.
- **Priority** — The priority value of the LAG. The priority value influences the LAG choice when a bridge has two looped ports. The priority value is between 0-240, in increments of 16.
- **Designated Bridge ID** — The bridge priority and the MAC Address of the designated bridge.
- **Designated Port ID** — The port priority and interface number of the designated port.
- **Designated Cost** — The cost of the designated bridge.
- **Forward Transitions** — The number of times the **LAG State** has changed from the **Blocking** state to a **Forwarding** state.

Modifying the LAG STP Parameters

- 1 Open the **STP LAG Settings** page.
- 2 Select a LAG from the **Select a LAG** drop-down menu.
- 3 Modify the fields as desired.
- 4 Click **Apply Changes**.

The STP LAG parameters are modified, and the device is updated.

Configuring Rapid Spanning Tree

While Classic Spanning Tree guarantees preventing L2 forwarding loops in a general network topology, convergence can take up to 30-60 seconds. The convergence time is considered too long for many applications. When network topology allows, faster convergence may be possible. The Rapid Spanning Tree Protocol (RSTP) detects and uses of network topologies that provide faster convergence of the spanning tree, without creating forwarding loops.

RSTP has the following port states:

- Disabled
- Learning
- Discarding
- Forwarding

Rapid Spanning Tree is enabled on the **STP Global Settings** page. To open the **Rapid Spanning Tree (RSTP)** page, click **Switch**→**Spanning Tree**→**Rapid Spanning Tree** in the tree view.

Figure 7-19. Rapid Spanning Tree (RSTP)



- **Interface** — Port or LAG on which Rapid STP is enabled.
- **Role** — The port role assigned by the STP algorithm in order to provide to STP paths. The possible field values are:
 - **Root** — Provides the lowest cost path to forward packets to root device.
 - **Designated** — The port or LAG via which the designated device is attached to the LAN.
 - **Alternate** — Provides an alternate path to the root device from the root interface.
 - **Backup** — Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop. Backup ports also occur when a LAN has two or more connections connected to a shared segment.
 - **Disabled** — The port is not participating in the Spanning Tree (the port's link is down).
- **Mode** — Displays 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.
- **Fast Link Operational Status** — Indicates if Fast Link is enabled or disabled for the port or LAG. If Fast Link is enabled for a port, the port is automatically placed in the forwarding state.
- **Point-to-Point Admin Status** — Indicates whether a point-to-point link is established on the port. Ports defined as Full Duplex are considered Point-to-Point port links. The possible field values are:
 - **Enable** — Enables the device to establish point-to-point links.

- **Disable** — Device establishes shared, half duplex links.
- **Auto** — Device automatically determines the state.
- **Point-to-Point Operational Status** — Displays the point-to-point operating state which depends on a link partner.
- **Activate Protocol Migration Test** — Select to run a Protocol Migration Test. The test identifies the STP mode of the interface connected to the selected interface.
 - **Checked** — Runs a Protocol Migration Test on the interface after you click the Apply button.
 - **Unchecked** — Does not run a Protocol Migration Test.

Enabling RSTP

- 1 Open the **Rapid Spanning Tree (RSTP)** page.
- 2 Define the **Point-to-Point Admin**, **Point-to-Point Oper**, and the **Activate Protocol Migration** fields.
- 3 Click **Apply Changes**.
Rapid STP is enabled, and the device is updated.

Configuring VLANs

VLANs are logical subgroups of a Local Area Network (LAN) created via software rather than defining a hardware solution. VLANs combine user stations and network devices into a single domain regardless of the physical LAN segment to which they are attached. VLANs allow network traffic to flow more efficiently within subgroups. VLANs managed through software reduces the amount of time in which network changes are implemented.

VLANs have no minimum number of ports, and can be created per device or any other logical connection combination, as VLANs are software based and not defined by physical attributes.

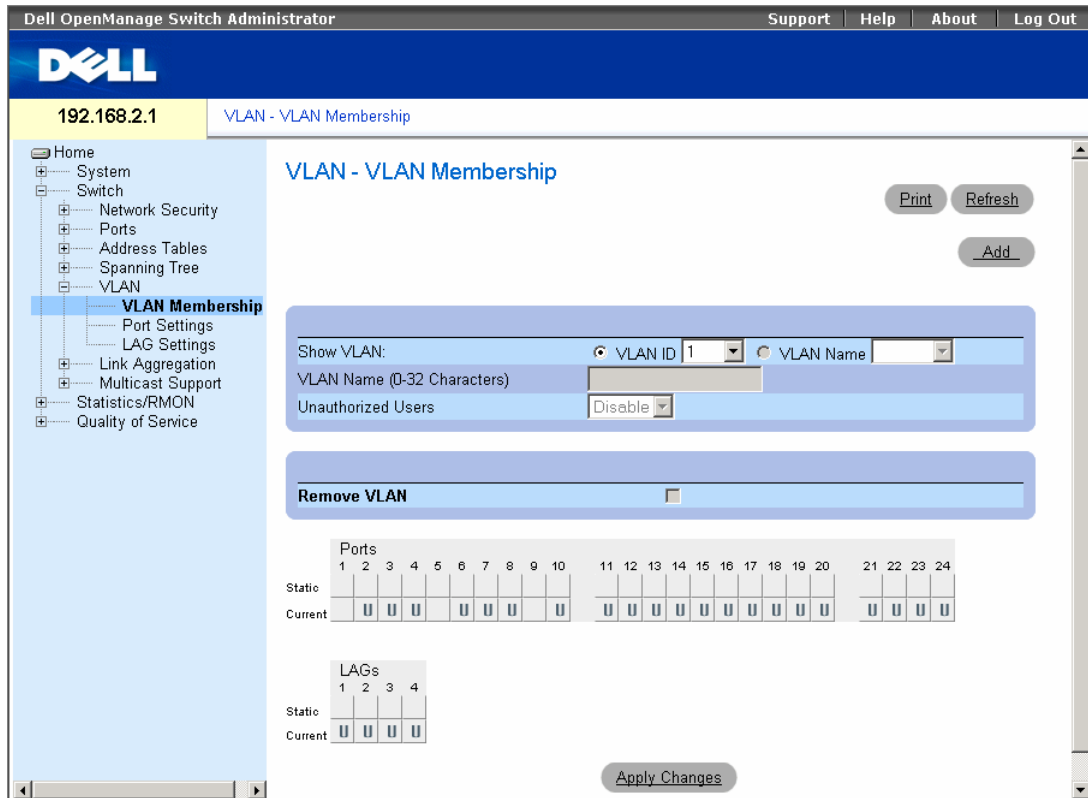
VLANs function at Layer 2. Since VLANs isolate traffic within the VLAN, a Layer 3 router functioning router is needed to allows traffic flow between VLANs. Layer 3 routers identify segments and coordinate with VLANs. VLANs are broadcast and Multicast domains. Broadcast and Multicast traffic is transmitted only in the VLAN in which the traffic is generated.

VLAN tagging provides a method of transferring VLAN information between VLAN groups. VLAN tagging attaches a tag to packet headers. The VLAN tag indicates to which VLAN the packet belongs. VLAN tags are attached to the packet by either the end station or by the network device. VLAN tags also contains VLAN network priority information. Combining VLANs and GVRP enables the automatic dispersal of VLAN information. To open the **VLAN** page, click **Switch**→**VLAN** in the tree view.

Defining VLAN Members

The **VLAN Membership** page contains fields for defining port membership in the VLAN. The device supports 64 VLANs. All ports must have a defined PVID. If no other value is configured the default VLAN PVID is used. VLAN number 1 is the default VLAN, and cannot be deleted from the system. To open the **VLAN Membership** page, click **Switch**→**VLAN**→**VLAN Membership** in the tree view.

Figure 7-20. VLAN Membership



- **Show VLAN** — Lists and displays specific VLAN information according to VLAN ID or VLAN name.
- **VLAN Name** — The user-defined VLAN name.
- **Unauthorized Users** — Enables or disables unauthorized users from accessing a VLAN.
- **Remove VLAN** — When selected, removes the VLAN from the VLAN Membership Table.

Adding New VLANs

- 1 Open the VLAN Membership page.
- 2 Click Add.
The Create New VLAN page opens.

Figure 7-21. Create New VLAN

Refresh

VLAN ID (2-4094)

VLAN Name (0-32 characters)

Authentication Not Required Disable ▾

Apply Changes

- 3 Enter the VLAN ID and name.
- 4 Click **Apply Changes**.
The new VLAN is added, and the device is updated.

Modifying VLAN Membership Groups

- 1 Open the **VLAN Membership** page.
- 2 Select a VLAN from the **Show VLAN** drop-down menu.
- 3 Modify the fields as desired.
- 4 Click **Apply Changes**.
The VLAN membership information is modified, and the device is updated.

Deleting VLAN Membership Groups

- 1 Open the **VLAN Membership** page.
- 2 Select a VLAN in the **Show VLAN** field.
- 3 Select the **Remove VLAN** check box.
- 4 Click **Apply Changes**.
The selected VLAN is deleted, and the device is updated.

VLAN Port Membership Table

The **VLAN Port Membership Table** contains a Port Table for assigning ports to VLANs. Ports are assigned VLAN membership by toggling through the Port Control settings. Ports can have the following values:

Table 7-1. 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.

Table 7-1. VLAN Port Membership Table

Port Control	Definition
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. Ports which are LAG members are not displayed in the **VLAN Port Membership Table**.

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

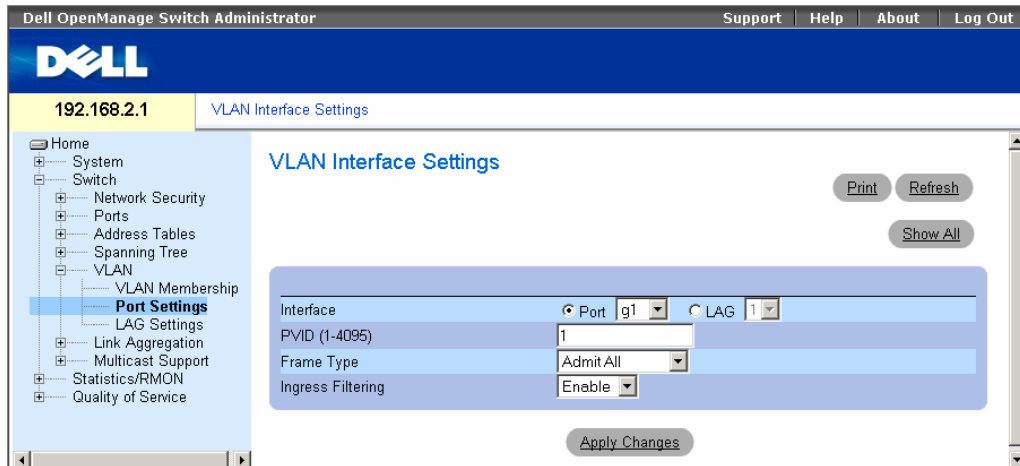
- 1 Open the **VLAN Membership** page.
- 2 Click the **VLAN ID** or **VLAN Name** option button and select a VLAN from the drop-down menu.
- 3 Select the **Remove VLAN** check box.
- 4 Click **Apply Changes**.
The selected VLAN is deleted, and the device is updated.

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 7-22. VLAN Port Settings



- **Port** — The port number included in the VLAN.
- **PVID (1-4095)**— Assigns a VLAN ID to untagged packets. The possible values are 1-4094. VLAN 4095 is defined as per standard and industry practice as the discard VLAN. Packets classified to the Discard VLAN are dropped.
- **Frame Type** — Packet type accepted on the port. Possible values are:
 - **Admit Tag Only** — Only tagged packets are accepted on the port.
 - **Admit All** — Both tagged and untagged packets are accepted on the port.
- **Ingress Filtering** — Enables or disables Ingress filtering on the port. Ingress filtering discards packets that are destined to VLANs of which the specific port is not a member.

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.

Figure 7-23. VLAN Port Table

VLAN Interface Settings Table

Refresh

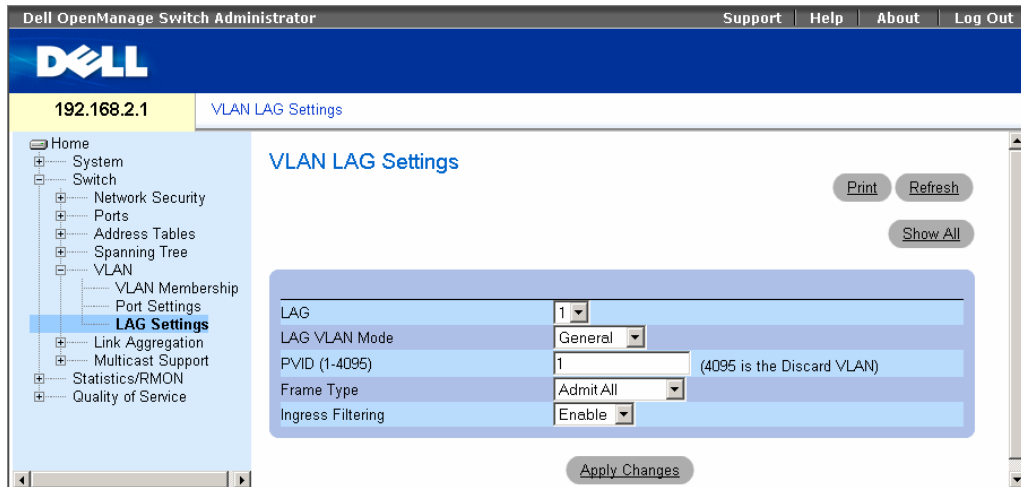
<<Previous 1 2 3 4 LAG Next>>

Interface	PVID	Frame Type	Ingress Filtering
g1	1	Admit All	Enable
g2	1	Admit All	Enable
g3	1	Admit All	Enable
g4	1	Admit All	Enable
g5	1	Admit All	Enable
g6	1	Admit All	Enable
g7	1	Admit All	Enable
g8	1	Admit All	Enable
g9	1	Admit All	Enable
g10	1	Admit All	Enable
g11	1	Admit All	Enable
g12	1	Admit All	Enable

Defining VLAN LAG Settings

The VLAN LAG Setting page provides parameters for managing LAGs that are part of a VLAN. VLANs can either be composed of individual ports or of LAGs. Untagged packets entering the device are tagged with the LAGs ID specified by the PVID. To open the VLAN LAG Setting page, click **Switch**→ **VLAN**→ **LAG Settings** in the tree view.

Figure 7-24. VLAN LAG Setting



- **LAG** — The LAG number included in the VLAN.
- **PVID** — Assigns a VLAN ID to untagged packets. The possible field values are 1-4095. VLAN 4095 is defined as per standard and industry practice, as the discard VLAN. Packets classified to this VLAN are dropped.
- **Frame Type** — Packet type accepted by the LAG. Possible values are:
 - **Admit Tag Only** — Only tagged packets are accepted by the LAG.
 - **Admit All** — Tagged and untagged packets are both accepted by the LAG.
- **Ingress Filtering** — Enables or disables Ingress filtering by the LAG. Ingress filtering discards packets that are destined to VLANs of which the specific LAG is not a member.

Assigning VLAN LAG Settings:

- 1 Open the VLAN LAG Setting page.
- 2 Select a LAG from the LAG drop-down menu and complete the fields on the page.
- 3 Click **Apply Changes**.
The VLAN LAG parameters are defined, and the device is updated.

Displaying the VLAN LAG Table

- 1 Open the VLAN LAG Setting page.
- 2 Click **Show All**.
The VLAN LAG Table opens.

Aggregating Ports

Port Aggregation optimizes port usage by linking a group of ports together to form a single Link Aggregated Group (LAG). Port Aggregation multiplies the bandwidth between the devices, increases port flexibility, and provides link redundancy. The device supports up to four LAGs, each having six members.

Each LAG is composed of ports of the same speed, set to full-duplex operations. Ports in a LAG, can be of different media types (UTP/Fiber, or different fiber types), provided they operate at the same speed.

The device provides LAG Load Balancing based on both source MAC addresses and destination MAC addresses.

Aggregated Links are treated by the system as a single logical port. Specifically, the Aggregated Link has similar port attributes to a non-aggregated port, including auto-negotiation, speed, etc.

The following guidelines should be followed when adding ports to a LAG:

- There is no Layer 3 interface defined on the port.
- The port does not belong to any VLAN.
- The port does not belong to any other LAG.
- The port is not a mirrored port.
- The port's 802.1p priority is equal to LAG's 802.1p priority.
- QoS Trust is not disabled on the port.
- GVRP is not enabled.

The device uses a hash function to determine which frames are carried on which aggregated-link member. The hash function statistically load-balances the aggregated link members. The device considers an Aggregated Link as a single logical port.

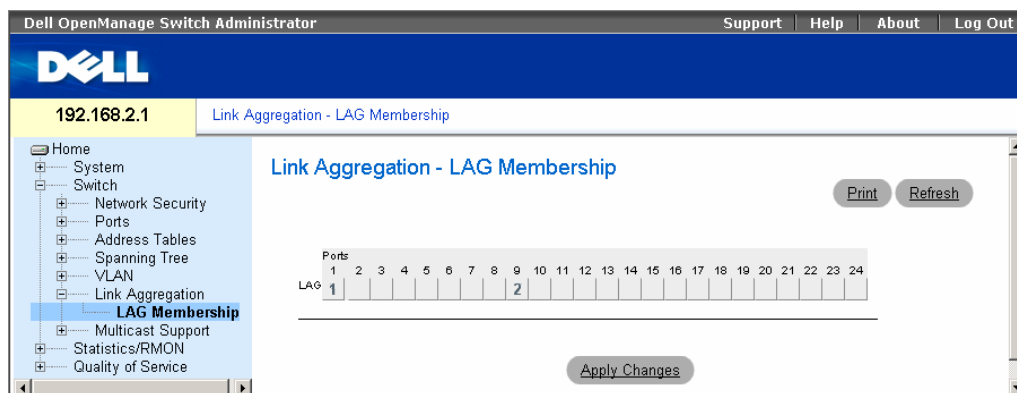
Each Aggregated Link has an Aggregated Link Port Type, including Gigabit Ethernet ports. Ports can be added to an Aggregated Link only if they are the same port type. When ports are removed from an Aggregated Link, the ports revert to the original port settings. To open the **Link Aggregation** page, click **Switch**→ **Link Aggregation** in the tree view.

Defining LAG Membership

The **LAG Membership** page contains fields for assigning ports to LAGs. LAGs can include up to 6 ports. When a port is added to a LAG, the port acquires the LAG's properties. If the port cannot be configured with the LAG properties, a trap is generated and the port operates with its default settings.

The **LAG Membership** page contains fields for assigning ports to LAGs. To open the **LAG Membership** page, click **Switch**→**Link Aggregation**→**LAG Membership** in the tree view.

Figure 7-25. LAG Membership



- **LAG** — Adds a port to a LAG, and indicates the specific LAG to which the port belongs.

Configuring a Port to a LAG

- 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 Click **Apply Changes**.

The port is added to the LAG, and the device is updated.

Multicast Forwarding Support

Multicast forwarding allows a single packet to be forwarded to multiple destinations. L2 Multicast service is based on L2 switch receiving a single packet addressed to a specific Multicast address. Multicast forwarding creates copies of the packet, and transmits the packets to the relevant ports.

Filtering L2 Multicast packets enables forwarding of Layer 2 packets to interfaces. If Multicast filtering is disabled, Multicast packets are flooded to all relevant ports. Forwarding L2 Multicast packets is enabled by default, and not configurable. The system supports Multicast filtering for 64 Multicast groups.

To open the **Multicast Support** page, click **Switch**→**Multicast Support** in the tree view.

Defining Multicast Global Parameters

Layer 2 switching forwards Multicast packets to all relevant VLAN ports by default, treating the packet as a Multicast transmission. While this is functional, in the sense that all relevant ports/nodes receive a copy of the frame, it is potentially wasteful as ports/nodes may receive irrelevant frames only needed by a subset of the ports of that VLAN. Multicast forwarding filters enable forwarding of Layer 2 packets to port subsets, defined in the Multicast filter database.

When IGMP snooping is enabled globally, the switching ASIC is programmed to forward all IGMP packets to the CPU. The CPU analyzes the incoming packets and determines which ports are to join which Multicast groups, which ports have Multicast routers generating IGMP queries, and what routing protocols are forwarding packets and Multicast traffic. Ports requesting to join a specific Multicast group issues an IGMP report specifying that Multicast group. This results in the creation of the Multicast filtering database.

The **Multicast Global Parameters** page contains fields for enabling Bridge Multicast Filtering and IGMP Snooping on the device. To open the **Multicast Global Parameters** page, click **Switch**→**Multicast Support**→**Global Parameters** in the tree view.

Figure 7-26. Multicast Global Parameters



- **Bridge Multicast Filtering** — Enables or disables bridge Multicast filtering. Disabled is the default value. IGMP Snooping can be enabled only if **Bridge Multicast Filtering** is enabled.
- **IGMP Snooping Status** — Enables or disables IGMP Snooping on the device. Disabled is the default value.

Enabling Bridge Multicast Filtering on the Device

- 1 Open the **Multicast Global Parameters** page.
- 2 Select **Enable** in the **Bridge Multicast Filtering** field.
- 3 Click **Apply Changes**.

Bridge Multicast is enabled on the device.

Enabling IGMP Snooping on the Device

- 1 Open the Multicast Global Parameters page.
- 2 Select Enable in the IGMP Snooping Status field.
- 3 Click Apply Changes.

IGMP Snooping is enabled on the device.

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 7-27. Bridge Multicast Group

The screenshot shows the Dell OpenManage Switch Administrator interface. The top navigation bar includes 'Support', 'Help', 'About', and 'Log Out'. The user is logged in as '192.168.2.1' and is viewing the 'Multicast Support - Bridge Multicast Group' page. The left-hand navigation tree shows the following structure:

- Home
 - System
 - Switch
 - Network Security
 - Ports
 - Address Tables
 - Spanning Tree
 - VLAN
 - Link Aggregation
 - Multicast Support
 - Global Parameters
 - Bridge Multicast Group**
 - Bridge Multicast Forward All
 - IGMP Snooping
 - Statistics/RMON
 - Quality of Service

The main content area is titled 'Multicast Support - Bridge Multicast Group' and contains the following configuration fields:

- VLAN ID: 1
- Bridge Multicast Address: 224-239.133|5.5.5
- Remove:

Below the configuration fields are two tables for selecting ports and LAGs:

Ports																								
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Static																								
Current																								

LAGs				
	1	2	3	4
Static				
Current				

Buttons for 'Print', 'Refresh', 'Add', and 'Apply Changes' are also visible.

- **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:

D	The port/LAG has joined the Multicast group dynamically in the Current Row.
F	The port/LAG is excluded from this Multicast group.
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.
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 7-28. Add Bridge Multicast Group

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

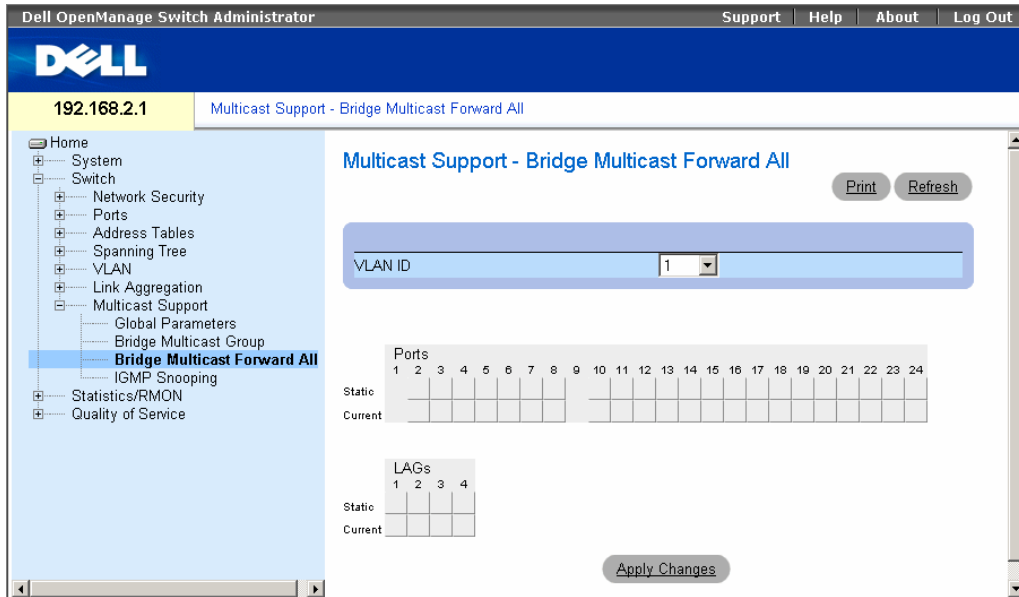
- 1 Open the **Bridge Multicast Group** page.
- 2 Define the **VLAN ID** and the **Bridge Multicast Address** fields.
- 3 Toggle the LAG to **S** to join the LAG to the selected Multicast group.
- 4 Toggle the LAG to **F** to forbid adding specific Multicast addresses to a specific LAG.
- 5 Click **Apply Changes**.
The LAG is assigned to the Multicast group, and the device is updated.

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 7-29. Bridge Multicast Forward All



- **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 contains the settings for managing router and port settings.

Port Control	Definition
F	The port/LAG is excluded from this Multicast group.
S	Attaches the port to the Multicast router or switch as a static port.
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.

IGMP Snooping

The IGMP Snooping page contains fields for adding IGMP members. To open the IGMP Snooping page, click Switch→ Multicast Support→ IGMP Snooping in the tree view.

Figure 7-30. IGMP Snooping

VLAN ID	1
IGMP Snooping Status	Enable
Auto Learn	Enable
IGMP Querier Status	Disable
Querier IP Address	1.0.2.4
Host Timeout (1-2147483647)	60 (Sec)
Multicast Router Timeout (1-2147483647)	100 (Sec)
Leave Timeout (0-2147483647)	<input type="radio"/> Immediate Leave

- **VLAN ID** — Specifies the VLAN ID.
- **IGMP Snooping Status** — Enables or disables IGMP snooping on the VLAN.
- **Auto Learn** — Enables or disables Auto Learn on the device.
- **IGMP Querier Status** — Enables or disables the IGMP Querier. The IGMP Querier simulates the behavior of a multicast router, allowing snooping of the layer 2 multicast domain even though there is no multicast router.
- **Querier IP Address** — IP address of the IGMP Querier. Use either use the VLAN's IP Interface address or define a unique IP address which will be used as a source address of Querier.
- **Host Timeout (1-2147483647)** — Time before an IGMP snooping entry is aged out. The default time is 260 seconds.
- **Multicast Router Timeout (1-2147483647)** — Time before aging out a Multicast router entry. The default value is 300 seconds.
- **Leave Timeout (0-2147483647)** — Time, in seconds, after a port leave message is received before the entry is aged out. **User-defined** enables a user-definable timeout period, and **Immediate Leave** specifies an immediate timeout period. The default timeout is 10 seconds.

Enabling IGMP Snooping on the Device

- 1 Open the IGMP Snooping page.
- 2 Select the VLAN ID for the device on which IGMP snooping needs to be enabled.
- 3 Select **Enable** in the IGMP Snooping Status field.
- 4 Complete the fields on the page.
- 5 Click **Apply Changes**.
IGMP snooping is enabled on the device.

Displaying the IGMP Snooping Table

- 1 Open the IGMP Snooping.
- 2 Click **Show All**.
The IGMP Snooping Table opens.

Figure 7-31. IGMP Snooping Table

IGMP Snooping Table

Refresh

VLAN ID	IGMP Status	Auto Learn	IGMP Querier Status	Querier IP Address	IGMP Querier Oper Status	Oper IP Address	Host Timeout	Multicast Router Timeout	Leave Timeout
1	Enable	Enable	Enable						

Apply Changes

Viewing Statistics

The **Statistic** pages contains links to device information for RMON, and CPU utilization.

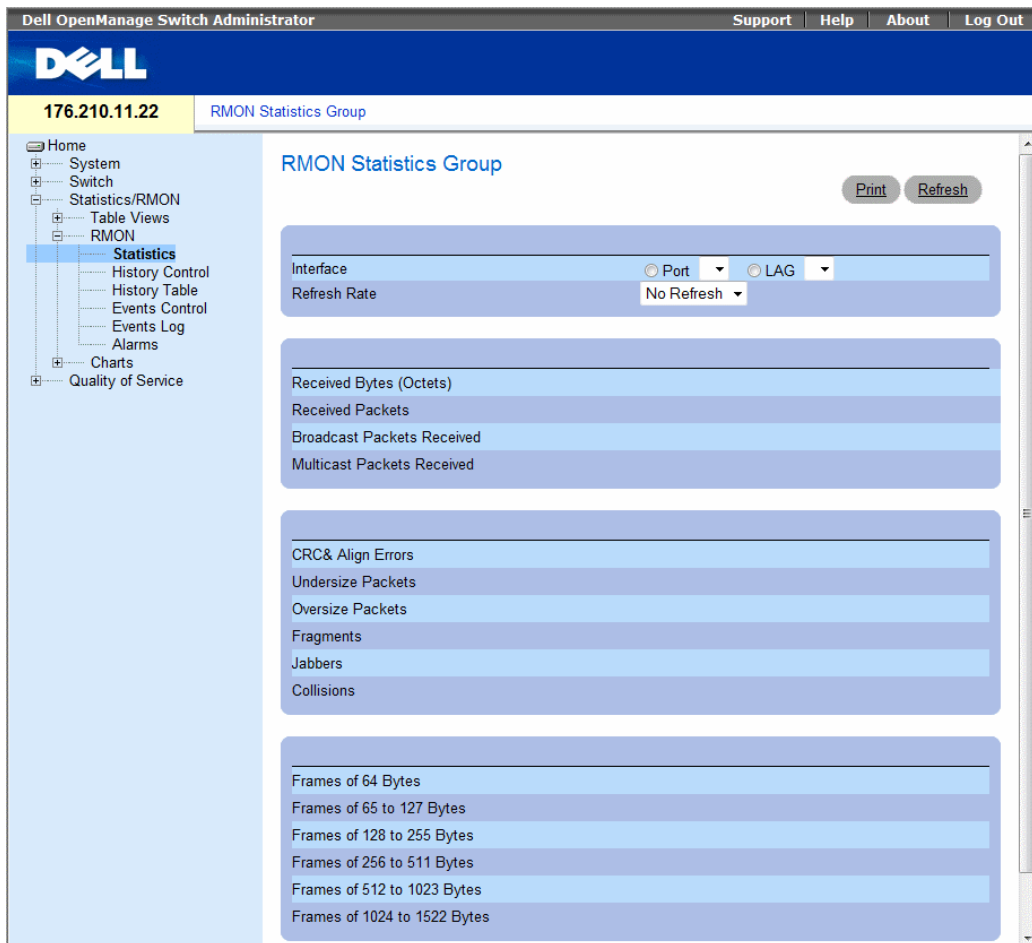
Viewing RMON Statistics

Remote Monitoring (RMON) contains links for viewing network information from a remote location. To open the RMON page, click **Statistics/RMON**→ **RMON** in the tree view.

Viewing RMON Statistics Group

The RMON Statistics Group page contains fields for viewing information about device utilization and errors that occurred on the device. To open the RMON Statistics Group page, click **Statistics/RMON**→ **RMON**→ **Statistics** in the tree view.

Figure 8-1. RMON Statistics Group



- **Interface** — Specifies the port or LAG for which statistics are displayed.
- **Refresh Rate** — Amount of time that passes before the statistics are refreshed.
- **Drop Events** — Number of dropped events that have occurred on the interface since the device was last refreshed.
- **Received Bytes (Octets)** — Number of octets received on the interface since the device was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.
- **Received Packets** — Number of packets received on the interface, including bad packets, Multicast and broadcast packets, since the device was last refreshed.
- **Broadcast Packets Received** — Number of good broadcast packets received on the interface since the device was last refreshed. This number does not include Multicast packets.
- **Multicast Packets Received** — Number of good Multicast packets received on the interface since the device was last refreshed.
- **CRC & Align Errors** — Number of CRC and Align errors that have occurred on the interface since the device was last refreshed.
- **Undersize Packets** — Number of undersized packets (less than 64 octets) received on the interface since the device was last refreshed.
- **Oversize Packets** — Number of oversized packets (over 1518 octets) received on the interface since the device was last refreshed.
- **Fragments** — Number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received on the interface since the device was last refreshed.
- **Jabbers** — Number of jabbers (packets longer than 1518 octets) received on the interface since the device was last refreshed.
- **Collisions** — Number of collisions received on the interface since the device was last refreshed.
- **Frames of *xx* Bytes** — Number of *xx*-byte frames received on the interface since the device was last refreshed.

Viewing Interface Statistics

- 1 Open the **RMON Statistics Group** page.
- 2 Select an interface type and number in the **Interface** field.
The interface statistics are displayed.

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.

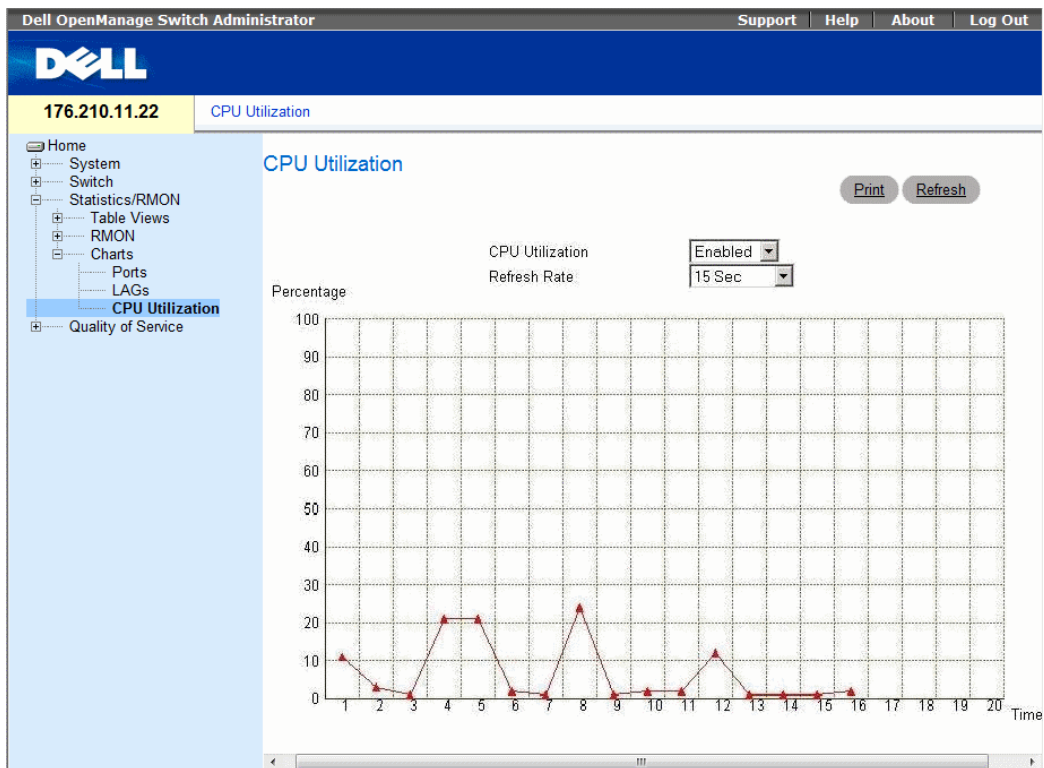
Viewing the CPU Utilization

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.

The range of the utilization 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 traveling through the interface. The maximum reading for a half duplex connection is 100%.

To open the **CPU Utilization** page, click **Statistics/RMON**→**Charts**→**CPU Utilization** in the tree view.

Figure 8-2. CPU Utilization



The **CPU Utilization** page contains the following information:

- **Refresh Rate** — Amount of time that passes before the statistics are refreshed.

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.

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 (VPT) and DSCP (DiffServ Code Point).

VPT Tag Classification Information

VLAN Priority Tags are used to classify the packets by mapping packets to one of the output queues. VLAN Priority Tag to queue assignments are user-definable. The table below details the VPT to queue default settings:

Table 9-1. CoS to Queue Mapping Table Default values

CoS Value	Forwarding Queue Values
0	q2
1	q1
2	q1
3	q2
4	q3
5	q3
6	q4
7	q4

Packets arriving untagged are assigned a default VPT that is set on a per port basis. The assigned VPT is used to map the packet to the output queue and as the egress VPT.

DSCP values can be mapped to priority queues. The following table contains the default DSCP mapping to forwarding queue values:

Table 9-2. DSCP to Queue Mapping Table Default Values

DSCP Value	Forwarding Queue Values
0-15	q1
16-31	q2
32-47	q3
48-63	q4

DSCP mapping is enabled on a per-system basis.

CoS Services

After packets are assigned to a specific queue, CoS services can be assigned to the queue(s). Output queues are configured with a scheduling scheme by one of the following methods:

- **Strict Priority** — Ensures that time-sensitive applications are always forwarded through an expedited path. Strict Priority allows the prioritization of mission-critical, time-sensitive traffic over less time-sensitive applications.
For example, under Strict Priority, voice over IP traffic is forwarded before FTP or e-mail (SMTP) traffic.
The strict priority queue is emptied before the traffic in the remaining queues is forwarded.
- **Weighted Round Robin** — Ensures that a single application does not dominate the device forwarding capacity. Weighted Round Robin (WRR) forwards entire queues in a Round Robin order. Queue priorities are defined by the queue length. The longer the queue length, the higher the queue's forwarding priority.
For example, if four queues have queue weights of 1, 2, 4 and 8, packets with the highest forwarding priority are assigned to queue 4, and packets with the lowest forwarding priority assigned to queue 1. By providing highest forwarding priorities across 4 queues, WRR processes higher priority traffic, and ensures that low-priority traffic is forwarded satisfactorily.

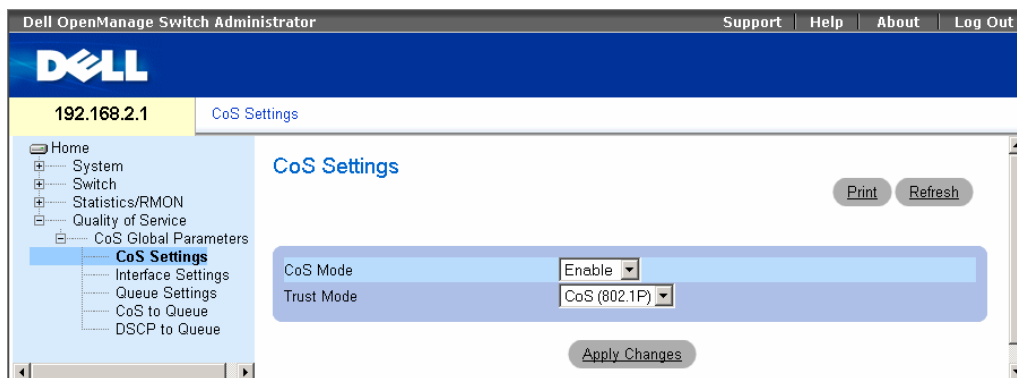
The scheduling scheme is enabled system-wide. Queues assigned to the strict priority policy are automatically assigned to the highest priority queue. By default, all values are set as Strict Priority. Queue weight values can be assigned in any order using WRR, and WRR values can be assigned system-wide. Best effort traffic is always assigned to the first queue.

Defining CoS Global Parameters

Class of Service (CoS) global parameters are set from the CoS Settings page.

To open the CoS Settings page, click **Quality of Service** → **CoS Global Parameters** → **CoS Settings** in the tree view.

Figure 9-1. CoS Settings



- **CoS Mode** — Enables or disables managing network traffic using Quality of Service.
- **Trust Mode** — Determines which packet fields to use for classifying packets entering the device. When no rules are defined, the traffic containing the predefined packet field (CoS or DSCP) is mapped according to the relevant trust modes table. Traffic not containing a predefined packet field is mapped to best effort. The possible Trust mode field values are:
 - **CoS (802.1P)** — The output queue assignment is determined by the IEEE802.1p VLAN priority tag (VPT) or by the default VPT assigned to a port.
 - **DSCP** — The output queue assignment is determined by the DSCP field. Interface Trust settings override the global Trust mode setting.

Enabling Quality of Service:

- 1 Open the CoS Settings page.
- 2 Select **Enable** in the CoS Mode field.
- 3 Click Apply Changes.
Class of Service is enabled on the device.

Selecting Trust:

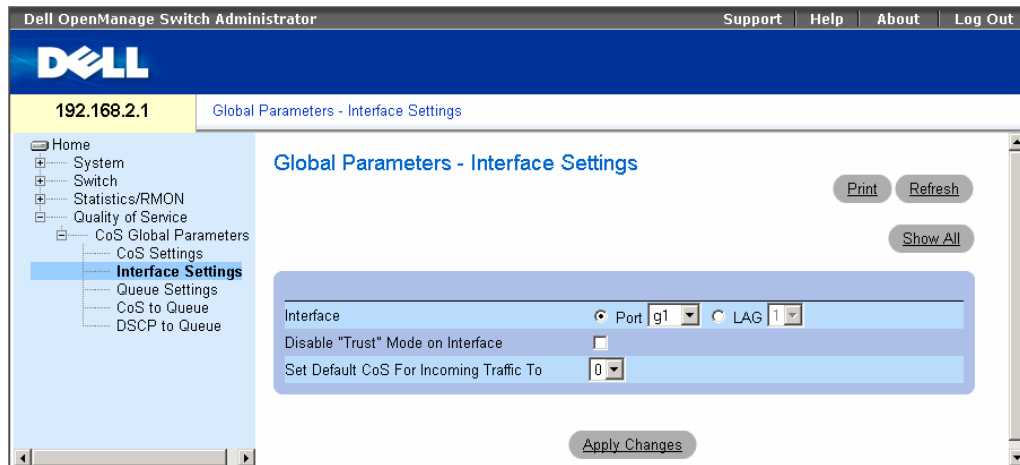
- 1 Open the CoS Settings page.
- 2 Select **Trust** in the Trust Mode field.
- 3 Click Apply Changes.

Trust is selected.

Defining QoS Interface Settings

The **Interface Settings** page contains fields for defining, per interface, if the selected Trust mode is to be activated. The default priority for incoming untagged packets is also selected in the **Interface Settings** page. To open the **Interface Settings** page, click **Quality of Service** → **CoS Global Parameters** → **Interface Settings** in the tree view.

Figure 9-2. Interface Settings



- **Interface** — The specific port or LAG to configure.
- **Disable "Trust" Mode on Interface** — Disables the 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 value for packets with no value in VPT field. The CoS tag values are 0–7. The default value is 0.

Assigning QoS/CoS 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 the QoS Interface Settings Table:

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

2 Click Show All.

The **QoS Interface Settings Table** page opens:

Figure 9-3. QoS Interface Settings Table

Interface Table

Interface	Trust Mode	Default CoS for Incoming Traffic
1 g1	Enable	0
2 g2	Enable	0
3 g3	Enable	0
4 g4	Enable	0
5 g5	Enable	0
6 g6	Enable	0

Defining Queue Settings

The **QoS Queue Settings** page contains fields for configuring the scheduling method by which the queues are maintained. To open the **QoS Queue Settings** page click **Quality of Service**→ **CoS Global Parameters**→ **Queue Settings** in the tree view.

Figure 9-4. QoS Queue Settings

The screenshot shows the Dell OpenManage Switch Administrator interface. The main content area is titled "QoS Queue Settings" and contains a table with the following structure:

Queue	Scheduling		WRR Weights	WRR percentage
	Strict Priority	WRR		
1	<input checked="" type="radio"/>	<input type="radio"/>		
2	<input checked="" type="radio"/>	<input type="radio"/>		
3	<input checked="" type="radio"/>	<input type="radio"/>		
4	<input checked="" type="radio"/>	<input type="radio"/>		
5	<input checked="" type="radio"/>	<input type="radio"/>		
6	<input checked="" type="radio"/>	<input type="radio"/>		
7	<input checked="" type="radio"/>	<input type="radio"/>		
8	<input checked="" type="radio"/>	<input type="radio"/>		

Buttons for "Print", "Refresh", and "Apply Changes" are visible on the page.

- **Queues** — The **Queue** number.
- **Strict Priority** — Specifies if traffic scheduling is based strictly on the queue priority. The default is enabled.

- **WRR** — Specifies if traffic scheduling is based on the Weighted Round Robin (WRR) weights to egress queues. The default values are:
 - 8 for Queue 1
 - 4 for Queue 2
 - 2 for Queue 3
 - 1 for Queue 4
- **WRR Weights** — The WRR weight assigned to each queue.
- **WRR Percentage** — The WRR percentage of each queue.

Defining the Queue Settings

When Strict Priority and Weighted Round Robin are both used, begin Strict Priority assignment from the queues with the highest priority.

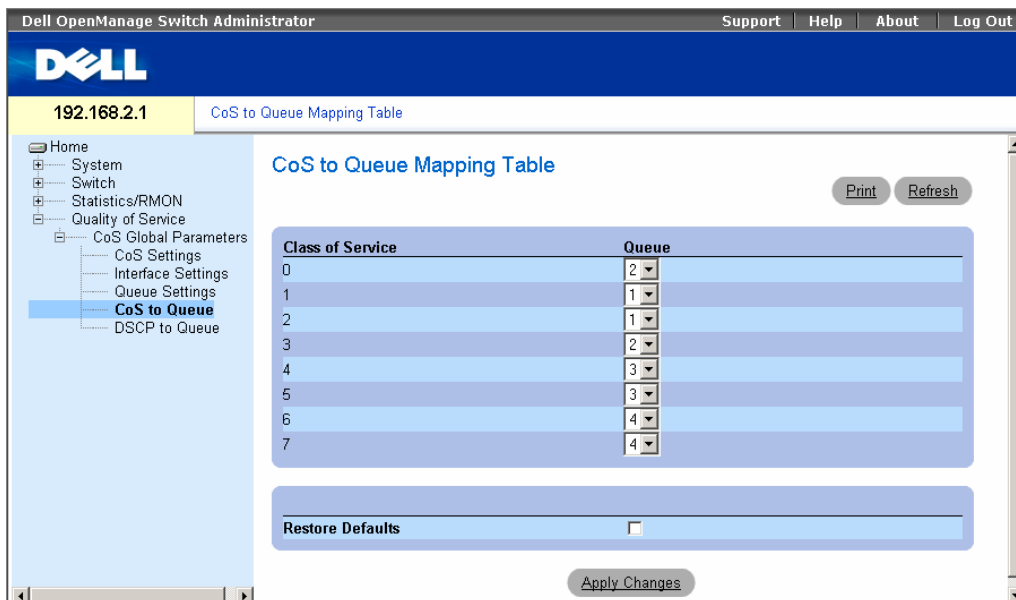
- 1** Open the **QoS Queue Settings** page.
- 2** Define the fields.
- 3** Click **Apply Changes**.

The queue settings are defined, and the device is updated.

Mapping CoS Values to Queues

The CoS to Queue Mapping Table page contains fields for classifying CoS settings to traffic queues. To open the CoS to Queue Mapping Table page, click **Quality of Service**→**CoS Global Parameters**→**CoS to Queue** in the tree view.

Figure 9-5. CoS to Queue Mapping Table



- **Class of Service** — Specifies the CoS priority tag values, where zero is the lowest value and 7 is the highest value.
- **Queue** — The traffic forwarding queue to which the CoS priority is mapped. Four traffic priority queues are supported.
- **Restore Defaults** — Restores the device factory defaults for mapping CoS values to a forwarding queue.

Mapping a CoS value to a Queue

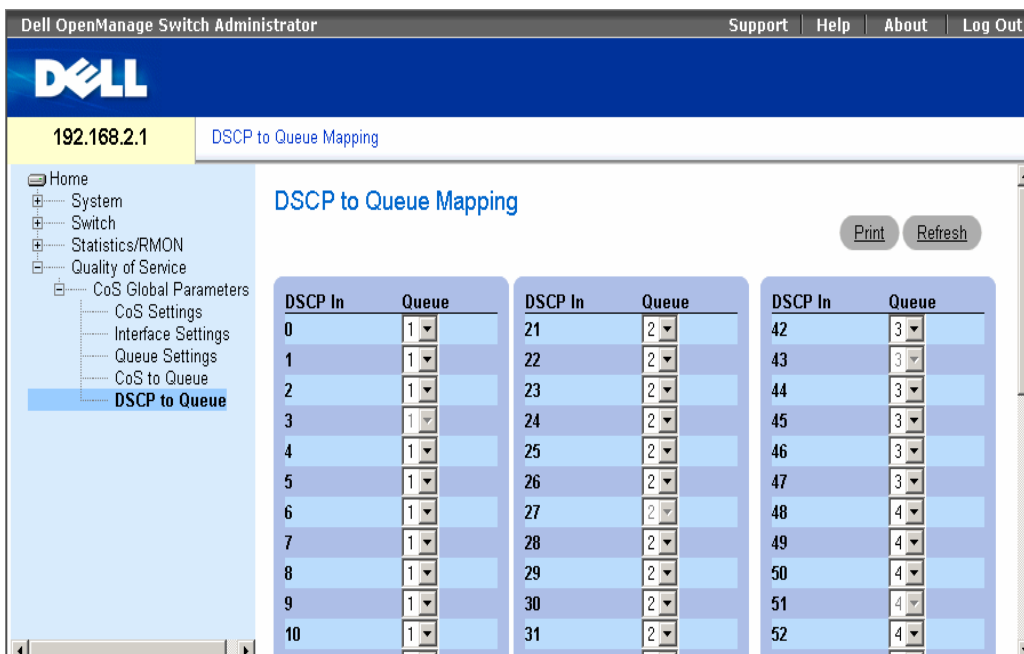
- 1 Open the CoS to Queue Mapping Table page.
- 2 Select a CoS entry.
- 3 Define the queue number in the Queue field.
- 4 Click Apply Changes.

The CoS value is mapped to a queue, and the device is updated.

Mapping DSCP Values to Queues

The DSCP to Queue page provides fields for defining output queue to specific DSCP fields. For the list of the DSCP default queue settings, see "DSCP to Queue Mapping Table Default Values" on page 148. To open the DSCP to Queue page, click **Quality of Service** → **CoS Global Parameters** → **DSCP to Queue** in the tree view.

Figure 9-6. DSCP to Queue



- **DSCP In** — The values of the DSCP field within the incoming packet.
- **Queue** — The queue to which packets with the specific DSCP value is assigned. The values are 1–4, where one is the lowest value and four is the highest.

Mapping a DSCP value and assigning priority queue:

- 1 Open the DSCP to Queue page.
- 2 Select a value in the DSCP In column.
- 3 Define the Queue fields.
- 4 Click Apply Changes.

The DSCP is overwritten, and the value is assigned to a forwarding queue.

Restoring default values:

- 1** Open the **DSCP to Queue** page.
- 2** Check the **Restore Defaults** checkbox.
- 3** Click **Apply Changes**.

The default values are restored.


Managing the Device Using the CLI


A limited number of CLI commands are available for managing the device. These commands are a subset of the options available via the web interface.

Accessing the Device Through the CLI

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

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

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

 **NOTE:** CLI can be used to manage the device only when the device is in Managed mode. For more information about management modes, see "Management Modes" on page 49.

Console Connection

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

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

Telnet Connection

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

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

To start a Telnet session:

- 1 Select **Start > Run**.

The **Run** window opens.

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

Using the CLI

This section provides information for using the CLI.

Command Mode Overview

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

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

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

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

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

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

User EXEC Mode

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

```
console>
```



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

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

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

Privileged EXEC Mode

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

To access and list the Privileged EXEC Mode commands:

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

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

```
console#
```

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

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

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

```
console>enable
Enter Password: *****
console#
console#disable
console>
```

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

Global Configuration Mode

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

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

```
console(config)#
```

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

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

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

```
console#  
console#configure  
console(config)#exit  
console#
```

Interface Configuration Mode

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

Interface Mode

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

```
console> enable  
console# configure  
console(config)# interface ethernet g18  
console(config-if)#
```

VLAN Mode

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

```
Console (config)# interface vlan 1  
Console (config-if)#
```

Port Channel Mode

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

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


CLI Commands

Command: **asset-tag**

To specify the device's asset tag, use the **asset-tag** command.

asset-tag *asset-tag*

Syntax Description

- *asset-tag* — The asset-tag to be assigned to the device.

Parameters range

- *asset-tag* — Word: 1-16 characters.

Command: **copy**

To copy any file from a source to a destination, use the **copy** Privileged EXEC command.

copy *source-url destination-url*

Syntax Description

- *source-url* — The location URL or reserved keyword of the source file to be copied.
- *destination-url* — The destination URL or reserved keyword of the destination file.

Parameters Range

- *source-url* — 1 - 160 characters
- *destination-url* — 1 - 160 characters

The following table shows keywords and URL prefixes:

Table A-1. Source and Destination Keywords

Keyword	Source or Destination
image	If source file, represent the active image file. If destination file, represent the non-active image file.
boot	Boot file.
tftp:	Source or destination URL for a TFTP network server. The syntax for this alias is tftp://host/[directory]/filename . The <i>host</i> can be IPv4 address. An out-of-band IP address can be specified as described in the usage guidelines.
xmodem:	Source for the file from a serial connection that uses the Xmodem protocol.
null:	Null destination for copies or files. You can copy a remote file to null to determine its size.

Command Mode

Privileged EXEC

Usage Guidelines

The location of a file system dictates the format of the source or destination URL.

The entire copying process may take several minutes and differs from protocol to protocol and from network to network.

If the egress interface is not specified, the default interface will be selected. Specifying interface zone=0 is equal to not defining an egress interface.

Understanding Invalid Combinations of Source and Destination

Some invalid combinations of source and destination exist. Specifically, you cannot copy the following:

- If the source file and destination file are the same file.
- **xmodem**: can't be destination. Can be copied to **image**, **boot** and **null**: only.
- **tftp**: can't be source and destination on the same copy.
- *.prv files can't be copied.
- Copy to or from the slave units is for image and boot files only.

copy Character Descriptions

Table A-2. Source and Destination Keywords

Character	Description
!	For network transfers, an exclamation point indicates that the copy process is taking place. Each exclamation point indicates the successful transfer of ten packets (512 bytes each).
.	For network transfers, a period indicates that the copy process timed out. Many periods in a row typically mean that the copy process may fail.

Command: debug-mode

To switch to debug mode, use the **debug-mode** command in Privileged EXEC mode.

debug-mode

Syntax Description

This command has no arguments or keywords.

Command Mode

Privileged EXEC

Command: do

To execute an EXEC-level command from global configuration mode or any configuration submode, use the **do** command in any configuration mode.

do command

Syntax Description

command— The EXEC command to be executed.

Command modes

All configuration modes

Command: end

To end the current configuration session and return to privileged EXEC mode, use the **end** global configuration command.

end

Syntax Description

This command has no arguments or key words

Command Mode

All configuration modes

Default value

This command has no default setting.

Example

```
Console(config-if)# end
```

```
Console#
```

Command: exit (configuration)

To exit any configuration mode to the next highest mode in the CLI mode hierarchy, use the **exit** command in any configuration mode.

exit

Syntax Description

This command has no arguments or key words

Command Mode

All configuration modes

Default value

This command has no default setting.

Examples

```
Console(config-if)# exit
```

```
Console(config)# exit
```

```
Console#
```

Command: exit (EXEC)

To close an active terminal session by logging off the router, use the **exit** command in EXEC mode.
exit

Syntax Description

This command has no arguments or key words

Command Mode

EXEC

Default value

This command has no default setting.

Example

```
Console> exit
```

Command: help

To display a brief description of the help system, enter the **help** command.
help

Syntax Description

This command has no arguments or key words

Command Mode

All command modes.

Default value

This command has no default setting.

Command: interface ethernet

To configure an interface type and enter interface configuration mode, use the **interface ethernet** global configuration command.

```
interface ethernet interface
```

Syntax Description

- *interface* — The full syntax is: *port*.

Parameters range

- *interface* — Valid Ethernet port.

Command Modes

Global Configuration

Example

```
Console(config)# interface ethernet g1  
Console(config-if)#
```

Command: interface port-channel

To configure a port-channel type and enter port-channel configuration mode, use the *interface port-channel* global configuration command.

```
interface port-channel port-channel-number
```

Syntax Description

- *port-channel-number* — Port channel index.

Parameters range

- *port-channel-number* — Valid port channel

Command Modes

Global configuration

Usage Guidelines

Commands under the interface range context are executed independently on each interface in the range: If the command returns an error on one of the interfaces, it will not stop the execution of the command on other interfaces.

Example

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

Command: interface vlan

To configure a vlan type and enter interface configuration mode, use the **interface vlan** global configuration command.

```
interface vlan vlan-id
```

Syntax Description

- *vlan-id*—VLAN ID

Parameters range

- *vlan-id*—Valid VLAN

Command Modes

Global Configuration

Usage Guidelines

In case the VLAN doesn't exist ("ghost VLAN") only partial list of the commands would be available under the interface VLAN context.

The commands that are supported for VLAN that doesn't exist are:

- 1 IGMP snooping control
- 2 Bridge multicast configuration

"Example

In the following example, for VLAN 1, the address is 131.108.1.27 and the subnet mask is 255.255.255.0:

```
Console (config)# interface vlan 1  
Console (config-if)# ip address 131.108.1.27 255.255.255.0
```

Command: ip address

To set the IP address of a device interface, use the **ip address** interface configuration command.

```
ip address ip-address
```

Syntax Description

- *ip-address*—The IP address to be assigned to the interface.

Parameters range

- *ip-address* — Valid IP address in the form A.B.C.D.

Command: ip default-gateway

To define a default gateway (router), use the **ip default-gateway** global configuration command. To remove the default gateway use the **no** form of this command.

```
ip default-gateway ip-address
```

```
no ip default-gateway
```

Syntax Description

ip-address — IP address of the default gateway.

Parameters range

ip-address — Valid IP address

Defaults

No default gateway is defined.

Command Modes

Global configuration

Interface configuration

Command: login

To change a login username, use the **login** command in EXEC mode.

```
login
```

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Command: ping

Use the **ping** command to send ICMP echo request packets to another node on the network.

```
ping {ip-address | hostname} [size packet_size] [count packet_count] [timeout time_out]
```

Syntax Description

- *ip-address* — IP address to ping.

- *hostname* — Hostname to ping.
- *packet_size* — Number of bytes in a packet. The default is 56 bytes. The actual packet size will be eight bytes larger than the size specified because the switch adds header information.
- *packet_count* — Number of packets to send, from 1 to 65535 packets. The default is 4 packets. If 0 is entered it pings until stopped.
- *time_out* — Timeout in milliseconds to wait for each reply, from 50 to 65535 milliseconds. The default is 2000 milliseconds.

Parameters range

- *hostname* — 1 - 158 characters (Max label size: 63)
- *packet_size* — IPv4: 56 - 1472
- *packet_count* — 0 - 65535
- *time_out* — 50 - 65535

Command Mode

EXEC

Default value

This command has no default setting.

Usage Guidelines

Press Esc to stop pinging. Following are sample results of the **ping** command:

Destination does not respond-If the host does not respond, a "*no answer from host*" appears in ten seconds.

Destination unreachable-The gateway for this destination indicates that the destination is unreachable.

Network or host unreachable-The switch found no corresponding entry in the route table.

Examples

```
Console> ping 10.1.1.1
```

```
Pinging 10.1.1.1 with 64 bytes of data:
```

```
64 bytes from 10.1.1.1: icmp_seq=0. time=11 ms
```

```
64 bytes from 10.1.1.1: icmp_seq=1. time=8 ms
```

```
64 bytes from 10.1.1.1: icmp_seq=2. time=8 ms
```

```
64 bytes from 10.1.1.1: icmp_seq=3. time=7 ms
```



```
----10.1.1.1 PING Statistics----  
4 packets transmitted, 4 packets received, 0% packet loss  
round-trip (ms) min/avg/max = 7/8/11
```

```
Console> ping yahoo.com
```

```
Pinging yahoo.com [66.218.71.198] with 64 bytes of data:
```

```
64 bytes from 10.1.1.1: icmp_seq=0. time=11 ms  
64 bytes from 10.1.1.1: icmp_seq=1. time=8 ms  
64 bytes from 10.1.1.1: icmp_seq=2. time=8 ms  
64 bytes from 10.1.1.1: icmp_seq=3. time=7 ms
```

```
----10.1.1.1 PING Statistics----  
4 packets transmitted, 4 packets received, 0% packet loss  
round-trip (ms) min/avg/max = 7/8/11
```

Command: reload

To reload the operating system, use the **reload EXEC** command.

```
reload
```

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Default value

This command has no default setting.

Command: show tech-support command

To display system and configuration information you can provide to the Technical Assistance Center when reporting a problem, use the **show tech-support** command.

show tech-support [config] [memory]

Syntax Description

- *memory*— (Optional) Displays memory and processor state data.
- *config*— (Optional) Displays switch configuration within the CLI commands supported on the device.

Defaults

By default, this command displays the output for technical-support-related **show** commands. Use keywords to specify the type of information to be displayed. If you do not specify any parameters, the system displays all configuration and memory data.

Command Modes

EXEC

Usage Guidelines

NOTE: Avoid running multiple show tech-support commands on a switch or multiple switches on the network segment. Doing so may cause starvation of some time sensitive protocols, like STP.

The **show tech-support** command output is continuous; it does not display one screen at a time. To interrupt the output, press **Esc**.

If you specify the **config** keyword, the **show tech-support** command displays the output:

show clock

show system

show version

show system mode

show ip interface

show interfaces configuration

show interfaces status

show interfaces port-channel

show vlan

show interfaces switchport

show spanning tree

show bridge multicast address-table

show ip igmp snooping groups

show dot1x

show dot1x users

show interfaces counters
show users
show sessions
show logging file
show logging

If you specify the **memory** keyword, the **show tech-support** command displays the output:

flash info (dir if existed, or flash mapping)
buffers info (like print os buff)
memory info (like print os mem)
proc info (like print os tasks)

Command: snmp-server community

Use the **snmp-server community** command to set up the community access string to permit access to the Simple Network Management Protocol command. Use the **no** form of this command removes the specified community string.

```
snmp-server community community [ro | rw | su] [ipv4-address]  
no snmp-server community community [ipv4-address]
```

Syntax Description

- *community* — Community string that acts like a password and permits access to the SNMP protocol.
- **ro** — Specifies read-only access (Default)
- **rw** — Specifies read-write access
- **su** — Specifies SNMP administrator access
- *ipv4-address* — Management station IPv4 address. Default is all IP addresses.

Parameters range

- *community* — 1 - 20 chars
- *ip-address* — Valid IP address

Default

No community is defined

Command Mode

Global configuration

Usage Guidelines

The logical key of the command is the pair (community, ip-address). If ip-address is omitted then the key is (community, All-Ips).

Examples

```
Switch(conf)# snmp-server community public
```

Command: username

To establish a username-based authentication system, use the **username** command in global configuration mode. Use the **no** form to remove a user name.

```
username name [password password] [level level] [encrypted]
```

```
no username name
```

Syntax Description

- *name* — The name of the user.
- *password* — The authentication password for the user.
- *level* — Specifies the user level. If not specified the privilege level is 1.
- **encrypted** — Encrypted password you enter, copied from another device configuration.

Parameters range

- *name* — 1 - 20 characters.
- *password* — 1 - 159
- *level* — 1 - 15

Default

No user is defined.

Command modes

Global Configuration

Example

```
Console (config)# username bob password lee privilege 15
```

Glossary

This glossary contains key technical words of interest.

A B C D E F G H I J L M N O P Q R S T U V W

A

Access Mode

Specifies the method by which user access is granted to the system.

Access Profiles

Allows network managers to define profiles and rules for accessing the device. Access to management functions can be limited to user groups, which are defined by the following criteria:

- Ingress interfaces
- Source IP address and/or Source IP subnets

ARP

Address Resolution Protocol. A TCP/IP protocol that converts IP addresses into physical addresses.

ASIC

Application Specific Integrated Circuit. A custom chip designed for a specific application.

Asset Tag

Specifies the user-defined device reference.

Authentication Profiles

Sets of rules which that enables login to and authentication of users and applications.

Auto-negotiation

Allows 10/100 Mbps or 10/100/1000 Mbps Ethernet ports to establish for the following features:

- Duplex/ Half Duplex Mode
- Flow Control
- Speed

B

Back Pressure

A mechanism used with Half Duplex mode that enables a port not to receive a message.

Backplane

The main BUS that carries information in the device.

Bandwidth

Bandwidth specifies the amount of data that can be transmitted in a fixed amount of time. For digital devices, bandwidth is defined in Bits per Second (bps) or Bytes per Second.

Bandwidth Assignments

The amount of bandwidth assigned to a specific application, user, and/or interface.

Baud

The number of signaling elements transmitted each second.

Best Effort

Traffic is assigned to the lowest priority queue, and packet delivery is not guaranteed.

Boot Version

The boot version.

BootP

Bootstrap Protocol. Enables a workstation to discover its IP address, an IP address of a BootP server on a network, or a configuration file loaded into the boot of a device.

BPDU

Bridge Protocol Data Unit. Provide bridging information in a message format. BPDUs are sent across device information with in Spanning Tree configuration. BPDUs packets contain information on ports, addresses, priorities, and forwarding costs.

Bridge

A device that connect two networks. Bridges are hardware specific, however they are protocol independent. Bridges operate at Layer 1 and Layer 2 levels.

Broadcast Domain

Devices sets that receive broadcast frames originating from any device within a designated set. Routers bind Broadcast domains, because routers do not forward broadcast frames.

Broadcasting

A method of transmitting packets to all ports on a network.

Broadcast Storm

An excessive amount of broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses are heaped onto the network, overloading network resources or causing the network to time out.

For more information about broadcast storms, see "Configuring Load Balancing".

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.

An overlapping transmission of two or more packets that collide. The data transmitted cannot be used, and the session is restarted.

Combo Ports

A single logical port with two physical connections, including an RJ-45 connection and an SFP connection.

CLI

Command Line Interface. A set of line commands used to configure the system.

Communities

Specifies a group of users which retains the same system access rights.

CPU

Central Processing Unit. The part of a computer that processes information. CPUs are composed of a control unit and an ALU.

D

DHCP Client

An Internet host using DHCP to obtain configuration parameters, such as a network address.

DSCP

DiffServe Code Point (DSCP). DSCP provides a method of tagging IP packets with QoS priority information.

Domain

A group of computers and devices on a network that are grouped with common rules and procedures.

Duplex Mode

Permits simultaneous transmissions and reception of data. There are two different types of duplex mode:

- **Full Duplex Mode** — Permits for bisynchronous communication, for example, a telephone. Two parties can transmit information at the same time.

- **Half Duplex Mode** — Permits asynchronous communication, for example, a walkie-talkie. Only one party can transmit information at a time.

Dynamic VLAN Assignment (DVA)

Allows automatic assignment of users to VLANs during the RADIUS server authentication. When a user is authenticated by the RADIUS server, the user is automatically joined to the VLAN configured on the RADIUS server.

E

Egress Ports

Ports from which network traffic is transmitted.

End System

An end user device on a network.

Ethernet

Ethernet is standardized as per IEEE 802.3. Ethernet is the most common implemented LAN standard. Supports data transfer rates of Mpbs, where 10, 100 or 1000 Mbps is supported.

EWS

Embedded Web Server. Provides device management via a standard web browser. Embedded Web Servers are used in addition to or in place of a CLI or NMS.

F

FFT

Fast Forward Table. Provides information about forwarding routes. If a packet arrives to a device with a known route, the packet is forwarded via a route listed in the FFT. If there is not a known route, the CPU forwards the packet and updates the FFT.

FIFO

First In First Out. A queuing process where the first packet in the queue is the first packet out of the packet.

Flapping

Flapping occurs when an interfaces state is constantly changing. For example, an STP port constantly changes from listening to learning to forwarding. This may cause traffic loss.

Flow Control

Enables lower speed devices to communicate with higher speed devices, that is, that the higher speed device refrains from sending packets.

Fragment

Ethernet packets smaller than 576 bits.

Frame

Packets containing the header and trailer information required by the physical medium.

G

GARP

General Attributes Registration Protocol. Registers client stations into a Multicast domain.

Gigabit Ethernet

Gigabit Ethernet transmits at 1000 Mbps, and is compatible with existing 10/100 Mbps Ethernet standards.

GVRP

GARP VLAN Registration Protocol. Registers client stations into a VLANs.

H

HOL

Head of Line. Packets are queued. Packets at the head of the queue are forwarded before packets at the end of the line.

Host

A computer that acts as a source of information or services to other computers.

HTTP

HyperText Transport Protocol. Transmits HTML documents between servers and clients on the internet.

I

IC

Integrated Circuit. Integrated Circuits are small electronic devices composed from semiconductor material.

ICMP

Internet Control Message Protocol. Allows gateway or destination host to communicate with a source host, for example, to report a processing error.

IEEE

Institute of Electrical and Electronics Engineers. An Engineering organization that develops communications and networking standards.

IEEE 802.1d

Used in the Spanning Tree Protocol, IEEE 802.1d supports MAC bridging to avoid network loops.

IEEE 802.1p

Prioritizes network traffic at the data-link/MAC sublayer.

IEEE 802.1Q

Defines the operation of VLAN Bridges that permit the definition, operation, and administration of VLANs within Bridged LAN infrastructures.

Image File

The system image is saved in a Flash sector called image.

Ingress Port

Ports on which network traffic is received.

IP

Internet Protocol. Specifies the format of packets and their addressing method. IP addresses packets and forwards the packets to the correct port.

IP Address

Internet Protocol Address. A unique address assigned to a network device with two or more interconnected LANs or WANs.

IPX

Internetwork Packet Exchange. Transmits connectionless communications.

J

Jumbo Frames

Enables transporting the identical data in fewer frames. Jumbo Frames reduce overhead, lower processing time, and ensure 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 connection and ensures that all data arrives to their destination. Packets inspected at the Layer 4 level are analyzed and forwarding decisions based on their applications.

Load Balancing

Enables the even distribution of data and/or processing packets across available network resources. For example, load balancing may distribute the incoming packets evenly to all servers, or redirect the packets to the next available server.

M

MAC Address

Media Access Control Address. The MAC Address is a hardware specific address that identifies each network node.

MAC Address Learning

MAC Address Learning characterizes a learning bridge, in which the packet's source MAC address is recorded. Packets destined for that address are forwarded only to the bridge interface on which that address is located. Packets addressed to unknown addresses are forwarded to every bridge interface. MAC Address Learning minimizes traffic on the attached LANs.

MAC Layer

A sub-layer of the *Data Link Control* (DTL) layer.

Mask

A filter that includes or excludes certain values, for example parts of an IP address.

For example, Unit 2 is inserted in the first minute of a ten-minute cycle, and Unit 1 is inserted in fifth minute of the same cycle, the units are considered the same age.

MD5

Message Digest 5. An algorithm that produces a 128-bit hash. MD5 is a variation of MD4, and increases MD4 security. MD5 verifies the integrity of the communication, authenticates the origin of the communication.

MDI

Media Dependent Interface. A cable used for end stations.

MDIX

Media Dependent Interface with Crossover (MDIX). A cable used for hubs and switches.

MIB

Management Information Base. MIBs contain information describing specific aspects of network components.

Multicast

Transmits copies of a single packet to multiple ports.

N

NMS

Network Management System. An interface that provides a method of managing a system.

Node

A network connection endpoint or a common junction for multiple network lines. Nodes include:

- Processors
- Controllers
- Workstations

O

OID

Object Identifier. Used by SNMP to identify managed objects. In the SNMP Manager/ Agent network management paradigm, each managed object must have an OID to identify it.

P

Packets

Blocks of information for transmission in packet switched systems.

PDU

Protocol Data Unit. A data unit specified in a layer protocol consisting of protocol control information and layer user data.

PING

Packet Internet Groper. Verifies if a specific IP address is available. A packet is sent to another IP address and waits for a reply.

Port

Physical ports provide connecting components that allow microprocessors to communicate with peripheral equipment.

Port Mirroring

Monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from one port to a monitoring port.

Port Speed

Indicates port speed of the port. Port speeds include:

- Ethernet 10 Mbps

- Fast Ethernet 100Mbps
- Gigabit Ethernet 1000 Mbps

Protocol

A set of rules that governs how devices exchange information across networks.

Q

QoS

Quality of Service. QoS allows network managers to decide how and what network traffic is forwarded according to priorities, application types, and source and destination addresses.

Query

Extracts information from a database and presents the information for use.

R

RADIUS

Remote Authentication Dial-In User Service. A method for authenticating system users, and tracking connection time.

RMON

Remote Monitoring. Provides network information to be collected from a single workstation.

Router

A device that connects to separate networks. Routers forward packets between two or more networks. Routers operate at a Layer 3 level.

RSTP

Rapid Spanning Tree Protocol. Detects and uses network topologies that allow a faster convergence of the spanning tree, without creating forwarding loops.

Running Configuration File

Contains all Startup file commands, as well as all commands entered during the current session. After the device is powered down or rebooted, all commands stored in the Running Configuration file are lost.

S

Segmentation

Divides LANs into separate LAN segments for bridging and routing. Segmentation eliminates LAN bandwidth limitations.

Server

A central computer that provides services to other computers on a network. Services may include file storage and access to applications.

SNMP

Simple Network Management Protocol. Manages LANs. SNMP based software communicates with network devices with embedded SNMP agents. SNMP agents gather network activity and device status information, and send the information back to a workstation.

SNTP

Simple Network Time Protocol. SNTP assures accurate network switch clock time synchronization up to the millisecond.

SoC

System on a Chip. An ASIC that contains an entire system. For example, a telecom SoC application can contain a microprocessor, digital signal processor, RAM, and ROM.

Spanning Tree Protocol

Prevents loops in network traffic. The Spanning Tree Protocol (STP) provides tree topography for any arrangement of bridges. STP provides one path between end stations on a network, eliminating loops.

Startup Configuration

Retains the exact device configuration when the device is powered down or rebooted.

Subnet

Sub-network. Subnets are portions of a network that share a common address component. On TCP/IP networks, devices that share a prefix are part of the same subnet. For example, all devices with a prefix of 157.100.100.100 are part of the same subnet.

Subnet Mask

Used to mask all or part of an IP address used in a subnet address.

Switch

Filters and forwards packets between LAN segments. Switches support any packet protocol type.

T

TCP/IP

Transmissions Control Protocol. Enables two hosts to communicate and exchange data streams. TCP guarantees packet delivery, and guarantees packets are transmitted and received in the order their sent.

Telnet

Terminal Emulation Protocol. Enables system users to log in and use resources on remote networks.

TFTP

Trivial File Transfer Protocol. Uses User Data Protocol (UDP) without security features to transfer files.

Trap

A message sent by the SNMP that indicates that system event has occurred.

Trunking

Link Aggregation. Optimizes port usage by linking a group of ports together to form a single trunk (aggregated groups).

U

UDP

User Data Protocol. Transmits packets but does not guarantee their delivery.

Unicast

A form of routing that transmits one packet to one user.

V

VLAN

Virtual Local Area Networks. Logical subgroups with a Local Area Network (LAN) created via software rather than defining a hardware solution.

W

WAN

Wide Area Networks. Networks that cover a large geographical area.

Wildcard Mask

Specifies which IP address bits are used, and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all the bits are important.

Index

Numerics

802.1d, 15

A

Access mode, 76
Address Resolution Protocol, 173
Aggregated link, 133
AH, 173
ARP, 173
Asset, 59
Auto-Negotiation, 36

B

Boot Version, 174
BootP, 174
BPDU, 174
Bridge Protocol Data Unit, 174
Buttons, 56

C

Cables, 65, 67
CIDR, 174
Command Mode Overview, 158

Community table, 76
CoS, 150

D

Defining device information, 59
Device installation, 30
Device representation, 54
Device view, 53-54
DHCP, 15
Dimensions, 21
Downloading software, 80
DSCP, 147, 175
DVMRPI, 175
Dynamic Address List, 115
Dynamic VLAN Assignment, 97

E

EAP, 95
EPG, 175
Extensible Authentication Protocol, 95

F

Fast Link, 15

Fast link, 119
File Transfer Protocol, 176
Filtering, 130, 132, 134
Firmware, 81
Flow Control, 36
FTP, 176

G

GARP, 176
GARP VLAN Registration Protocol, 176
GBIC, 176
General Attributes Registration Protocol, 176
GRE, 176
GVRP, 176

H

Hardware version, 61
Height, 21
HMP, 176
HOL, 176

I

ICMP, 176
IDRP, 177

IEEE, 177
IEEE 802.1d, 177
IEEE 802.1p, 177
IEEE 802.1Q, 177
IGMP, 177
Image File, 80, 177
Ingress, 177
Interface mode, 160
Internetwork Packet
Exchange, 177
IP, 177
IPM, 177
IPX, 177
ISIS, 177

J

Jumbo frames, 177

L

L2TP, 177
LAG, 106, 177
LAGs, 138
Local User Database, 69
Loops, 116

M

MAC Address, 178
MAC address, 114

Management Information
Base., 178
Management security, 69
Master Election/Topology
Discovery Algorithm, 178
MD5, 178
MDI, 12, 104, 178
MDI/MDIX, 36
MDIX, 12, 104, 178
MDU, 178
Message Digest 5, 178
MIB, 74, 178
Multicast, 138

N

Network Management
System., 178
Network security, 95

O

OSPF, 179

P

Package Contents, 28
Package contents, 28
Passwords, 56
PDU, 179
PING, 179
Port aggregation, 133

Port LEDs, 22
Ports, 55, 103
PVID, 130, 132

Q

QoS, 150, 179
Quality of Service, 147, 179
Queue, 151

R

RADIUS, 71-73, 179
Rapid Spanning Tree
Protocol, 180
RDP, 179
Remote Authentication Dial-
In User Service, 179
Reset, 62-64
RMON, 144, 179
RSTP, 15, 180
Running Configuration
file, 80
RVSP, 180

S

Security, 69, 95
Simple Network Management
Protocol, 74, 180
SNMP, 74, 76-77, 180
Software version, 61

Spanning Tree Protocol, 116,
124
Startup file, 80
Storm control, 110
STP, 15, 117, 125
System, 59

T

TFTP, 181
Time Domain
 Reflectometry, 65
Tree view, 53
Trivial File Transfer
 Protocol, 181
Trunk Configuration
 Page, 106
Trust, 150

U

UDP, 181
Understanding the
 interface, 53
Uploading files, 82
User Data Protocol, 181

V

Virtual Local Area
 Networks, 181
VLAN, 126, 130, 138, 181
VLAN ID, 115

VLAN membership, 126
VLAN Port Membership
 Table, 128
VLAN priority, 147
VLANs, 126

W

Web management system
 icons, 55
Weighted Round Robin, 151
Width, 21

Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>