Compaq ProLiant BL e-Class C-GbE Interconnect Switch

User Guide

Part Number 263682-001

March 2002 (First Edition)

Product Version: Version 1.0

This user guide provides installation and reference information about the Compaq ProLiant BL e-Class C-GbE Interconnect Switch.

Compaq ProLiant BL e-Class C-GbE Interconnect Switch User Guide

March 2002 (First Edition)
Part Number 263682-001

Contents

About This Guide

Chapter 1
Introduction

Chapter 2

Setting Up and Installing the Interconnect Switch

Chapter 3

Configuring the Switch Modules Using the Console Management Interface

Chapter 4
Configuring the Switch Modules Using the Web-Based Management Interface

Appendix A
Technical Specifications

Appendix B
RJ-45 Pin Specification

Appendix C
Runtime Switching Software Default Settings

Appendix D
Spanning Tree Protocol

Appendix E
SNMP/RMON MIBs Support

Appendix F
Upgrading Firmware through the Serial Port

Appendix G
Troubleshooting

Appendix H
Regulatory Compliance Notices

Index

List of Figures

List of Tables

About This Guide

This user guide can be used for reference when servicing the ProLiant BL e-Class C-GbE Interconnect Switch**.**

WARNING: To reduce the risk of personal injury from electric shock and hazardous energy levels, only authorized service technicians should attempt to repair this equipment. Improper repairs can create conditions that are hazardous.

Symbols in Text

These symbols may be found in the text of this guide. They have the following meanings.

WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or loss of life.

CAUTION: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or loss of information.

IMPORTANT: Text set off in this manner presents clarifying information or specific instructions.

NOTE: Text set off in this manner presents commentary, sidelights, or interesting points of information.

⚠ Important Safety Information

Before installing this product, read the *Important Safety Information* document provided.

Compaq Technician Notes

WARNING: Only authorized technicians trained by Compaq should attempt to repair this equipment. All troubleshooting and repair procedures are detailed to allow only subassembly/module-level repair. Because of the complexity of the individual boards and subassemblies, no one should attempt to make repairs at the component level or to make modifications to any printed wiring board. Improper repairs can create a safety hazard.

WARNING: To reduce the risk of personal injury from electric shock and hazardous energy levels, do not exceed the level of repairs specified in these procedures. Because of the complexity of the individual boards and subassemblies, do not attempt to make repairs at the component level or to make modifications to any printed wiring board. Improper repairs can create conditions that are hazardous.

WARNING: To reduce the risk of electric shock or damage to the equipment:

- **Disconnect power from the system by unplugging all power cords from the power supplies.**
- **Do not disable the power cord grounding plug. The grounding plug is an important safety feature.**
- **Plug the power cord into a grounded (earthed) electrical outlet that is easily accessible at all times.**

CAUTION: The computer is designed to be electrically grounded (earthed). To ensure proper operation, plug the AC power cord into a properly grounded AC outlet only.

NOTE: Any indications of component replacement or printed wiring board modifications may void any warranty.

Where to Go for Additional Help

In addition to this guide, the following information sources are available:

- User documentation
- *Compaq Service Quick Reference Guide*
- Service training guides
- Compaq service advisories and bulletins
- Compaq *QuickFind*™ information services
- *Compaq Insight Manager*™software

For additional copies, visit the Compaq website:

www.compaq.com

Telephone Numbers

For the name of your nearest Compaq authorized reseller:

- In the United States, call 1-800-345-1518.
- In Canada, call 1-800-263-5868.

For Compaq technical support:

- In the United States and Canada, call 1-800-OK COMPAQ.
- For Compaq technical support phone numbers outside the United States and Canada, visit the Compaq website:

  www.compaq.com

Text Conventions

This document uses the following conventions:

- *Italic type* is used for complete titles of published guides or variables. Variables include information that varies in system output, in command lines, and in command parameters in text.
- **Bold type** is used for emphasis, for onscreen interface components (window titles, menu names and selections, button and icon names, and so on), and for keyboard keys.
- `Monospace typeface` is used for command lines, code examples, screen displays, error messages, and user input.
- Sans serif typeface is used for uniform resource locators (URLs).

1

Introduction

Overview

The Compaq *ProLiant*™ BL e-Class C-GbE (Copper Gigabit Ethernet) Interconnect Switch uses 10/100/1000 Gigabit Layer 2 switch technology to provide up to a 40-to-1 reduction in the number of networking cables required for each ProLiant BL e-Class server blade enclosure. Each interconnect switch reduces forty 10Base-T/100Base-TX server networking ports to as few as one (up to four) RJ-45 10Base-T/100Base-TX/1000Base-T uplink ports.

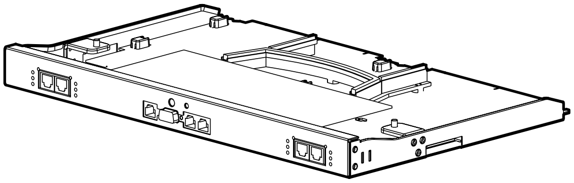


Figure 1-1: ProLiant BL e-Class C-GbE Interconnect Switch

Features

The ProLiant BL e-Class C-GbE Interconnect Switch is designed for easy installation and high performance in an environment where traffic on the network and the number of users increase continually.

Enterprise Class Performance

The ProLiant BL e-Class C-GbE Interconnect Switch features include:

- Up to a 40-to-1 reduction in networking cables and connections by:
    - Converting forty 10/100 Ethernet networking ports to as few as one (up to four) Gigabit Ethernet networking ports.
    - Allowing the use of only one of the four Gigabit Ethernet networking ports to dramatically reduce the number of network cables required for a ProLiant BL e-Class system.

  - Allowing use of the remaining Gigabit Ethernet ports to fit the bandwidth requirement.
  - Providing redundant networking paths to each ProLiant BL e-Class server blade through redundant switching modules.
- Preconfiguration for immediate use with the ProLiant BL e-Class server blade enclosure
- Industry standard protocols compatible with other widely-used networking components
- Support for up to sixty-four 802.1Q VLANs for server grouping and isolation
- A variety of management interfaces
- Uplink and management ports with link activity and speed indicators
- Extra ports for management debugging and port mirroring

Interconnect Switch Redundancy

The ProLiant BL e-Class C-GbE Interconnect Switch offers several redundancy and failover features. The interconnect switch can be configured for continued network access to each server blade in case of system failure. Interconnect switch redundancy features include:

- Two separate switch modules for each ProLiant BL e-Class C-GbE Interconnect Switch
- Two Gigabit Ethernet uplink ports per switch module, with a total of four per interconnect switch, for designing fully meshed uplink paths to the network backbone
- Server networking connections routed to both switch modules for redundant paths to tolerate a switch module or a port malfunction
- Redundant data path 10/100 Ethernet cross connections between switch modules
- Spanning Tree Protocol support which eliminates potential problems caused by redundant networking paths and provides for failover with secondary path, in case of primary path failure
- Power and cooling by the redundant hot-plug power supplies and fans within the ProLiant BL e-Class server blade enclosure

Configuration and Management

The ProLiant BL e-Class C-GbE Interconnect Switch provides the following configuration and management interfaces and tools:

- A menu-driven console interface allows local and Telnet access.
- A browser-based GUI allows remote access using a Web browser such as Microsoft Internet Explorer or Netscape Navigator.
- SNMP and RMON manageability and monitoring are supported. An SNMP-based scripting utility allows remote configuration of the interconnect switch.
- The interconnect switch functionality allows you to save and download interconnect switch configurations to a TFTP server, thus allowing the rapid deployment of multiple server blade systems, and providing robust backup and restore capabilities.

Diagnostic

The hardware, software, and firmware diagnostic tools that are available include:

- ProLiant BL e-Class Integrated Administrator
- *Compaq Insight Manager*™ 7
- Power-On Self Test (POST) built into the interconnect switch boot-up process
- C-GbE Interconnect Switch Management System and Utilities
- C-GbE Interconnect Switch port mirroring
- C-GbE Interconnect Switch LEDs for port status and speed

Interconnect Switch Architecture

The ProLiant BL e-Class C-GbE Interconnect Switch contains the ProLiant BL e-Class Integrated Administrator module and two redundant interconnect switch modules (Switch A and Switch B).

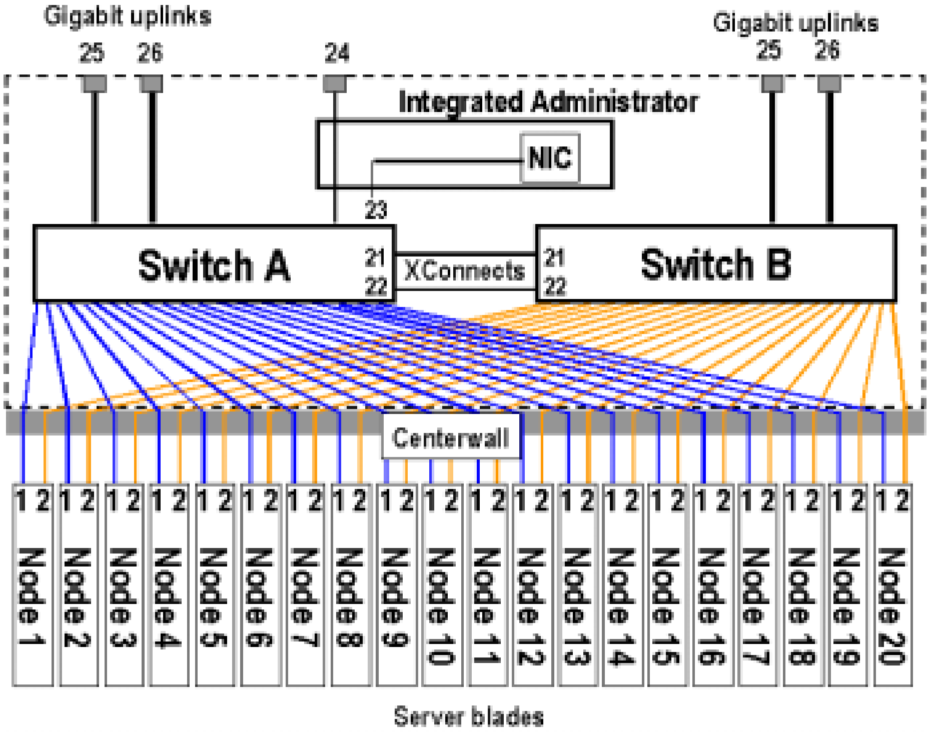


Figure 1-2: ProLiant BL e-Class C-GbE Interconnect Switch architecture

Integrated Administrator

The ProLiant BL e-Class Integrated Administrator provides centralized, remote management and monitoring for the ProLiant BL e-Class server blade enclosure, interconnect switch module, and 20 server blades. The Integrated Administrator acts as a combination terminal server and remote power controller, enabling out-of-band, secure, serial console connections to all server blades in the enclosure.

The Integrated Administrator serves as a single access point for administrative functions. It provides remote and local setup, deployment, and administrative support, as well as monitoring and health reporting of server blades, interconnect switch modules, and other components in the enclosure, such as power supplies and fans.

Interconnect Switch Modules

Two interconnect switch modules (Switch A and Switch B) in the interconnect switch provide switch redundancy and redundant paths to the network ports on the server blades.

Each interconnect switch has two GB uplink ports and direct connections to one of the two network interface cards (NICs) (PXE NIC 1 and NIC 2) on each server blade. The interconnect switch reduces as many as forty 10/100 Ethernet ports on the server blade into as few as one (up to four) Gigabit uplink ports on the back of the system.

Redundant Crosslinks

The two interconnect switch modules are connected through redundant 100-Mb crosslinks. These two crosslinks provide an aggregate throughput of 200 Mb for traffic between the switch modules.

Redundant Paths to Server Blades

The NICs of each server blade are routed through the enclosure’s centerwall assembly to different switch modules. By default, NIC 1 on each server blade is routed to Switch A and NIC 2 on each server blade is routed to Switch B. This configuration provides redundant paths to each server.

NOTE: On a heavily used system, using a single uplink port for all 40 NICs can cause a traffic bottleneck. For example, if uplink 1 on Switch A is the only uplink used, all traffic to and from NIC 2 on any of the server blades must travel over the crosslinks between Switch A and Switch B. This path to the server blade NICs is intended as a failover route and should not be used as a primary path. For optimum performance, use uplink ports from both switch modules.

Supported Technologies

The ProLiant BL e-Class C-GbE Interconnect Switch supports the following technologies. See Chapter 3 and Chapter 4 for more details on these features.

Layer 2-Based Packet Forwarding

The ProLiant BL e-Class C-GbE Interconnect Switch uses 10/100/1000 Gigabit Layer 2 switching technology. Layer 2 refers to the Data Link layer of the Open Systems Interconnection (OSI) model, which is concerned with moving data packets across a network by enforcing Carrier Sense Multiple Access with Collision Detection (CSMA/CD). This layer performs:

- Ethernet packet framing
- MAC addressing
- Physical medium transmission error detection
- Medium allocation (collision avoidance)
- Contention resolution (collision handling)

Layer 2 switch technology allows the interconnect switch to look into data packets and redirect them based on the destination MAC address. This technology reduces traffic congestion on the network, because packets, instead of being transmitted to all ports, are transmitted to the destination port only.

IEEE 802.1Q-Based Virtual Local Area Network

The ProLiant BL e-Class C-GbE Interconnect Switch provides support for up to sixty-four 802.1Q Virtual Local Area Networks (VLANs) for server grouping and isolation. A VLAN is a network segment configured according to a logical scheme rather than a physical layout. VLANs can be used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN. VLANs also logically segment the physical network into different broadcast domains so that packets are forwarded only between ports within the VLAN. This technology enhances performance by conserving bandwidth and improves security by limiting traffic to specific domains.

Spanning Tree Protocol

The interconnect switch supports Spanning Tree Protocol (STP), which allows the blocking of links that form loops between switches in a network. When multiple links between switches are detected, a primary link is established. Duplicated links are blocked from use and become standby links. If the primary link fails, the standby link is activated. See Appendix D for more information.

Simple Network Management Protocol and Remote Monitoring

Each switch module can be configured and monitored remotely from a Simple Network Management Protocol (SNMP)/Remote Monitoring (RMON) based Network Management Station. The switch modules support industry-standard SNMP Management Information Bases (MIBs), Compaq Switch MIBs, and RMON groups 1 (statistics), 2 (History), 3 (Alarm), and 9 (Event) for fault detection, configuration, and monitoring of switch functionality.

To secure the management interface, the switch administrator can configure community strings with various levels of access. Access can be restricted to a limited number of Management Stations by configuring a list of IP addresses of those stations that can access the interconnect switch. See Appendix E for more information.

Port Mirroring

The interconnect switch allows the user to mirror a port to another port for network monitoring and troubleshooting purposes. This technology offers a way for network packet analyzers to view the traffic moving through the switch modules by providing a copy of the traffic that is currently being passed through any other port. The packets are normally sent to a network packet analyzer or other monitoring device attached to the mirror port.

Trunking

The interconnect switch port trunking feature allows several ports to be grouped together and act as a single logical link called a trunk. This feature provides a bandwidth that is a multiple of a single link’s bandwidth. It also improves reliability since a configurable way of load balancing is automatically applied to the ports in the trunked group. A link failure within the group causes the network traffic to be directed to the remaining links in the group.

Trivial File Transfer Protocol Support

The Trivial File Transfer Protocol (TFTP) service feature allows the interconnect switch firmware to be upgraded by downloading a new firmware file from a TFTP server to the switch modules. A configuration file can also be loaded into a switch module from a TFTP server, configuration settings can be saved to the TFTP server, and a history log can be uploaded from the switch module to the TFTP server.

Store and Forward Switching Scheme

The interconnect switch provides a store and forward switching scheme that allows each packet to be buffered (stored) before it is forwarded to its destination. While this method creates latency, it improves reliability in a heavily used interconnect switch. Packets that cannot be forwarded are saved immediately, rather than dropped, and packets behind it are less likely to be dropped in periods of heavy usage.

IEEE 802.1p-Based Class of Service for Packet Prioritization

Class of Service (CoS) for packet prioritization allows switch administrators to set priority levels on the interconnect switch for forwarding packets based on the priority setting information in the packets. The interconnect switch supports four classes of traffic (buffers or queues) for implementing priority. The interconnect switch allows administrators to map eight priority levels to four classes. Traffic from a specific server port can be given priority over packets from other devices according to this range of priority levels. For example, with multiple packets in a buffer, the packet with the highest priority would be forwarded first, regardless of when it was received.

Internet Group Management Protocol Snooping

Internet Group Management Protocol (IGMP) snooping, when enabled and configured properly, manages multicast traffic in a switch module by allowing directed switching of the IP multicast traffic. The interconnect switch can use IGMP Snooping to configure switch module ports dynamically, so that IP multicast traffic is forwarded only to those ports associated with IP multicast hosts.

IGMP Snooping allows the switch module to recognize IGMP queries and reports sent between network stations or devices and an IGMP host that belong to a specific multicast group. When enabled for IGMP Snooping, the switch module can open or close a port to a specific device based on IGMP messages passing through the module. This feature further limits unnecessary broadcasts.

Dynamic Host Configuration Protocol or Bootstrap Protocol

A switch module can be configured to obtain an IP address from a Dynamic Host Configuration Protocol (DHCP) or Bootstrap Protocol (BOOTP) server during the boot process. The IP settings can be manually configured through the console interface. The IP settings are also configurable from other interfaces, such as the Web, but since the connection is based on an IP address for these interfaces, users have to reconnect with the newly assigned IP address.

User Account Management

For increased security, separate user accounts can be set up with various levels of permission.

External Components

This section describes the external panel and LED indicators of the ProLiant BL e-Class C-GbE Interconnect Switch.

External Panel

The external panel of each interconnect switch has four RJ-45 connectors with Gigabit Ethernet uplink connectivity for network cabling. In addition, there are two Integrated Administrator connectors (one RJ-45 and one serial port) that support remote and local out-of-band management of the interconnect switch through a browser, SNMP/RMON, and Telnet console interfaces.

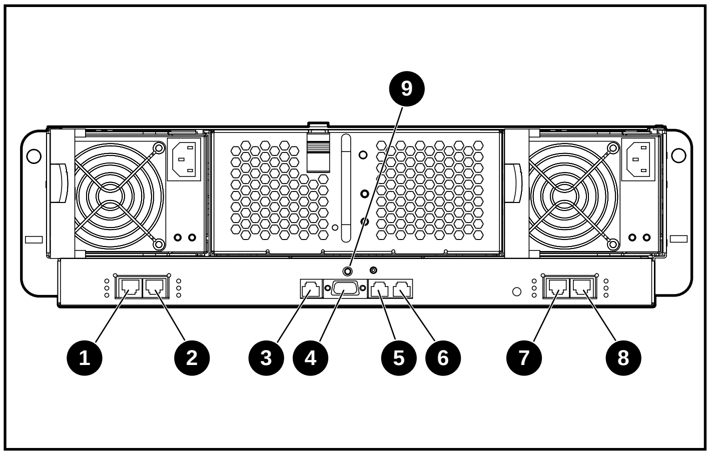


Figure 1-3: Interconnect switch external panel

Table 1-1: Interconnect Switch External Panel

Item	Description	Location
1	Gigabit Ethernet port 26 connector on Switch B	Interconnect switch
2	Gigabit Ethernet port 25 connector on Switch B	Interconnect switch
3	Integrated Administrator management RJ-45 connector (Switch A Port 24—10/100 Ethernet)	Integrated Administrator module
4	Integrated Administrator console connector (serial)	Integrated Administrator module
5	Reserved for future use	Integrated Administrator module
6	Reserved for future use	Integrated Administrator module
7	Gigabit Ethernet port 26 connector on Switch A	Interconnect switch
8	Gigabit Ethernet port 25 connector on Switch A	Interconnect switch
9	Combined interconnect switch and Integrated Administrator Reset button (see the statement on the following page)	Integrated Administrator module

⚠ **CAUTION:** Do not use the enclosure link (RJ-45) connectors (see items 5 and 6 in Table 1-1) on the Integrated Administrator module. Connecting an external device to these enclosure link (RJ-45) connecters can damage the external device.

IMPORTANT: Resetting the interconnect switch disconnects the server blades from the network while the switch is rebooting. To reset the interconnect switch, press the **Reset** button for at least four seconds. To reset only the Integrated Administrator module, press the **Reset** button for less than four seconds.

LED Indicators

The ProLiant BL e-Class C-GbE Interconnect Switch LEDs provide information about switch health, link speed and activity, and stacking status.

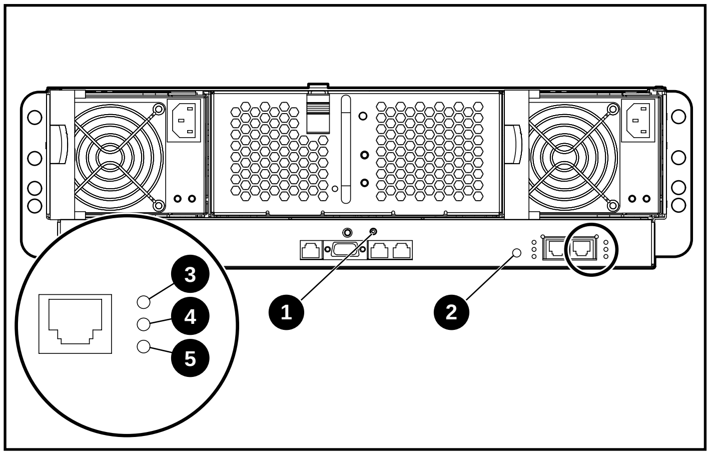


Figure 1-4: Interconnect switch external panel LEDs

Table 1-2: Interconnect Switch External Panel LEDs

Item	LED Description	Status
1	Integrated Administrator module health	Green = Enclosure on, Integrated Administrator health good
		Amber = Integrated Administrator health degraded
		Red = Integrated Administrator health critical
		Off = Enclosure off, Integrated Administrator health good
2	Interconnect switch health	Green = Enclosure on, interconnect switch health good
		Amber = Interconnect switch health degraded
		Red = Interconnect switch health critical
		Off = Enclosure off or booting, interconnect switch health good

continued

Table 1-2: Interconnect Switch External Panel LEDs *continued*

Item	LED Description	Status

3	Stacking status*	Green = Base unit
		Yellow = Slave unit
		Off = No stacking

4	Link activity	Green = Network link
		Flashing green = Network activity
		Yellow = Port disabled
		Off = No network link

5	Link speed	Yellow = 1000
		Green = 100
		Off = 10 or no network link

*****Stacking functionality support is planned for a future release of the interconnect switch firmware.

2

Setting Up and Installing the Interconnect Switch

Overview

This chapter describes how to set up and install the ProLiant BL e-Class C-GbE Interconnect Switch and connect it to your network.

The setup and installation procedure includes the following tasks:

1. Installing the interconnect switch hardware
2. Planning the interconnect switch configuration
3. Cabling the interconnect switch tray to the network
4. Configuring the Integrated Administrator module
5. Accessing the switch modules

NOTE: The ProLiant e-Class C-GbE Interconnect Switch tray consists of the ProLiant BL e-Class Integrated Administrator module and two interconnect switch modules (Switch A and Switch B).

Installing Interconnect Switch Hardware

This section describes how to install the interconnect switch tray in a new switch deployment, as a replacement for an existing interconnect switch, and as an upgrade from a patch panel.

Installing a New Interconnect Switch Tray in a New ProLiant BL e-Class Server Blade Enclosure

To install a new interconnect switch tray:

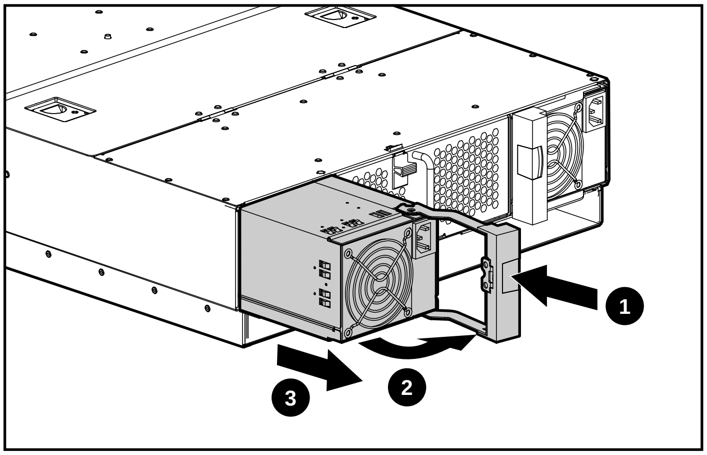


Figure 2-1: Removing a hot-plug power supply

1. Press the port-colored latch to release one hot-plug power supply (1).

   NOTE: Port-color indicates hot-plug components.

2. Pull the handle to its open position (2).
3. Slide the hot-plug power supply out of the server blade enclosure (3).
4. Repeat steps 1 through 3 to remove the other hot-plug power supply.

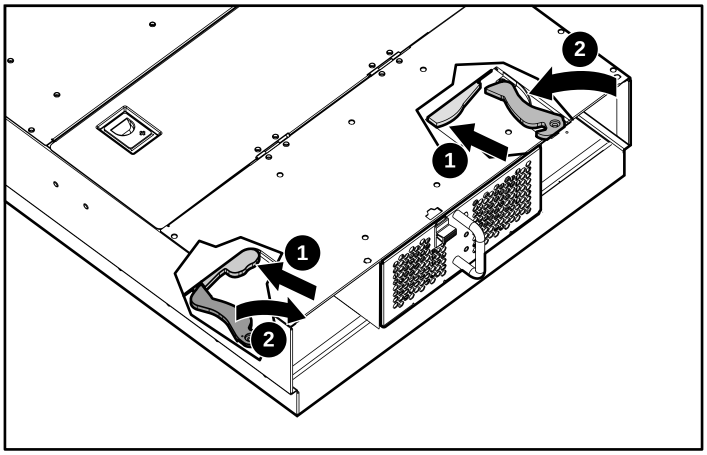


Figure 2-2: Pulling the interconnect tray ejector levers

5. Press both interconnect tray release buttons (1).
6. Simultaneously pull both slate blue ejector levers toward the rear of the server blade enclosure (2).

NOTE: Slate blue indicates internal touch point components.

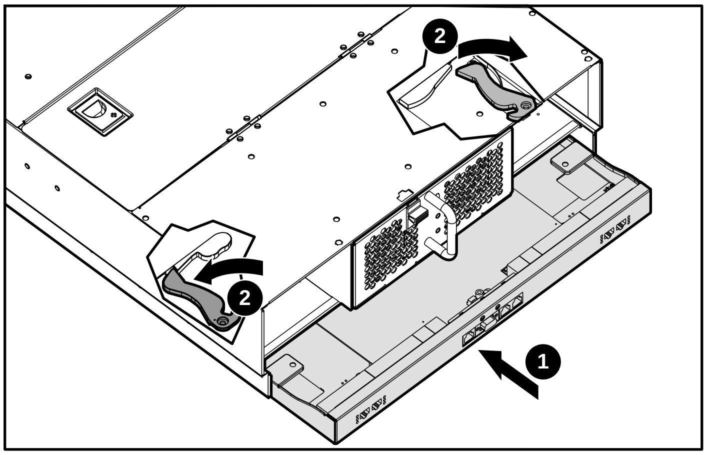


Figure 2-3: Inserting the interconnect switch tray and engaging the interconnect tray levers

7. Insert the interconnect switch tray into the server blade enclosure (1).
8. Simultaneously rotate both ejector levers to the locked position (2).

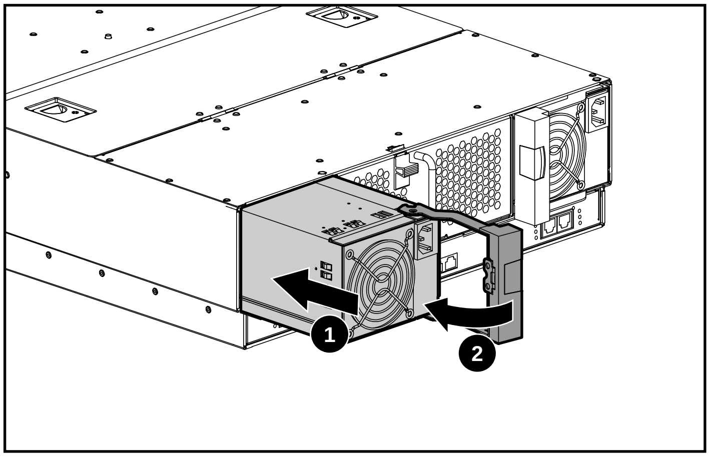


Figure 2-4: Installing a hot-plug power supply

9. Install the hot-plug power supplies (1).
10. Push the power supply handles to the closed position (2).

Replacing an Existing Interconnect Switch Tray

To replace an existing interconnect switch tray:

1. Upload the current switch configuration to a TFTP server. See the “Saving Settings to a TFTP Server” sections in Chapter 3 (for console management interface) and Chapter 4 (Web-based management interface).

   NOTE: Compaq recommends saving the switch module configuration to a TFTP server once the switch module configuration is complete or has changed.

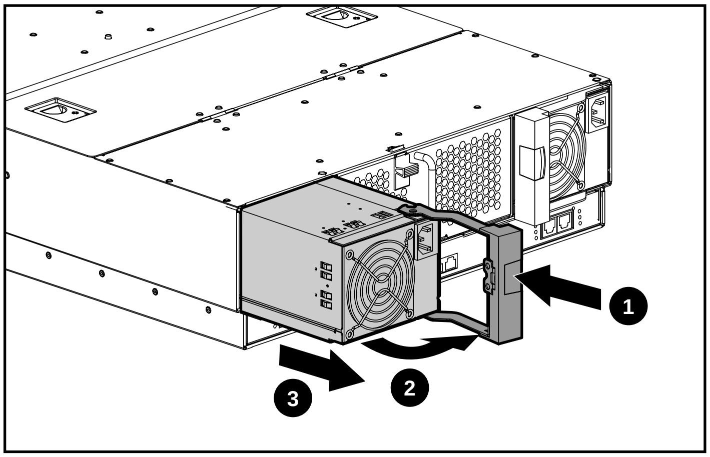


Figure 2-5: Removing a hot-plug power supply

2. Press the port-colored latch to release one hot-plug power supply (1).

   NOTE: Port-color indicates hot-plug components.

3. Pull the handle to its open position (2).
4. Slide the hot-plug power supply out of the server blade enclosure (3).
5. Repeat steps 2 through 4 to remove the other hot-plug power supply.

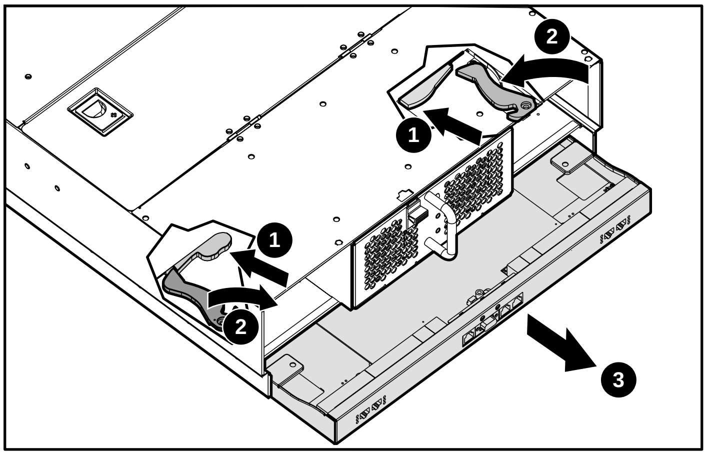


Figure 2-6: Removing the old interconnect switch tray

6. Press both interconnect tray release buttons (1).
7. Simultaneously pull both slate blue ejector levers toward the rear of the server blade enclosure (2).

   NOTE: Slate blue indicates internal touch point components.

8. Pull the existing interconnect switch tray out of the server blade enclosure.

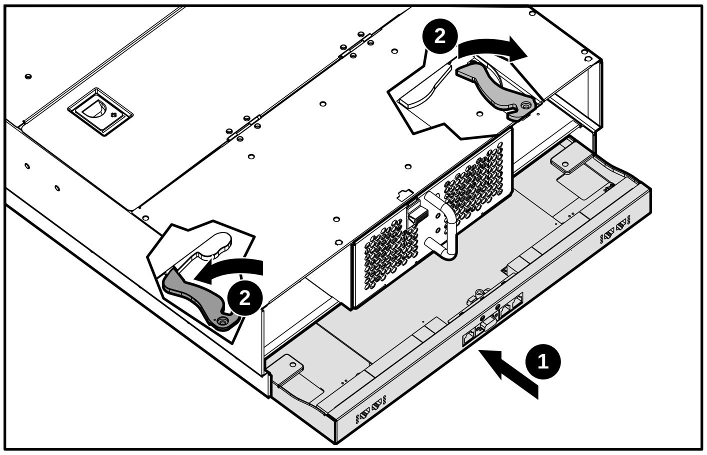


Figure 2-7: Inserting the new interconnect switch tray and engaging the interconnect tray levers

9. Insert the new interconnect switch tray into the server blade enclosure (1).
10. Simultaneously rotate both ejector levers to the locked position (2).

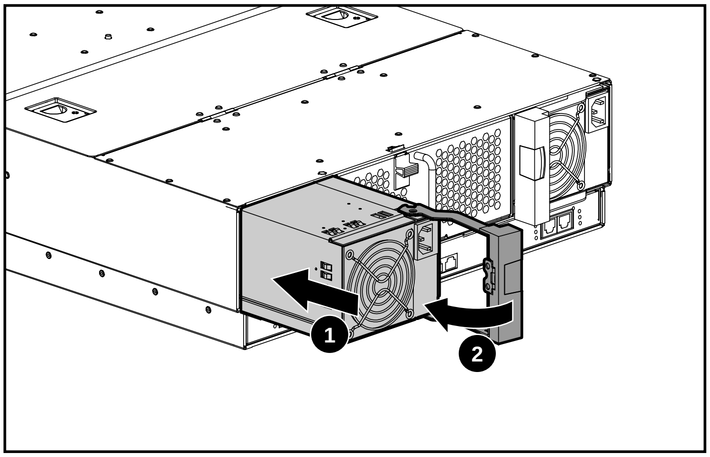


Figure 2-8: Installing a hot-plug power supply

11. Install the hot-plug power supplies (1).
12. Push the power supply handles to the closed position (2).
13. Download the switch configuration file from the TFTP server. See the “Downloading Configuration File on a TFTP Server” sections in Chapter 3 (for console management interface) and Chapter 4 (for web-based management interface). If no configuration file is available, reconfigure the switch modules.

Replacing a Patch Panel Tray

To remove the patch panel tray and install an interconnect switch tray:

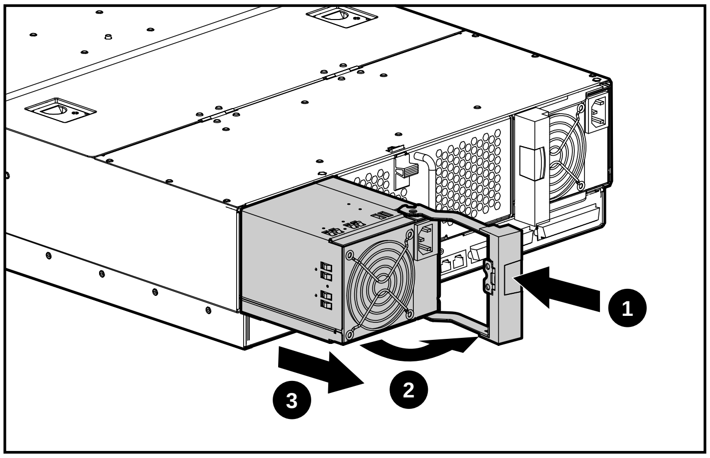


Figure 2-9: Removing a hot-plug power supply

1. Press the port-colored latch to release one hot-plug power supply (1).

   NOTE: Port-color indicates hot-plug components.

2. Pull the handle to its open position (2).
3. Slide the hot-plug power supply out of the server blade enclosure (3).

4. Repeat steps 1 through 3 to remove the other hot-plug power supply.

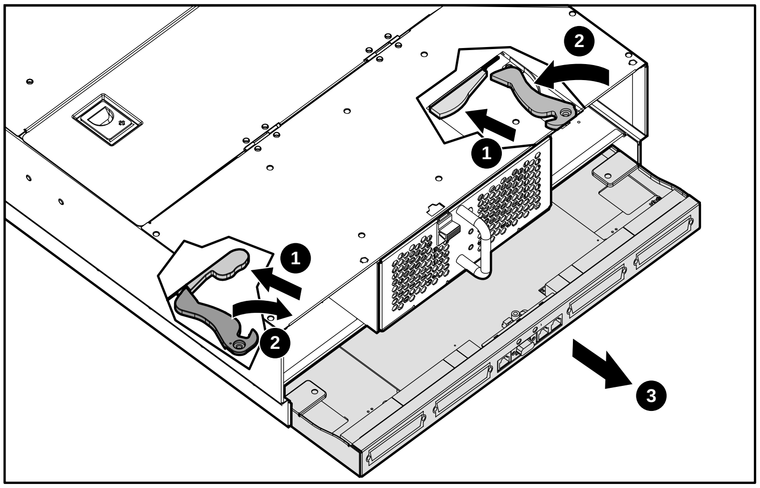


Figure 2-10: Removing the patch panel tray

5. Press both interconnect tray release buttons (1).
6. Simultaneously pull both slate blue ejector levers toward the rear of the server blade enclosure (2).

   NOTE: Slate blue indicates internal touch point components.

7. Pull the patch panel tray out of the server blade enclosure (3).

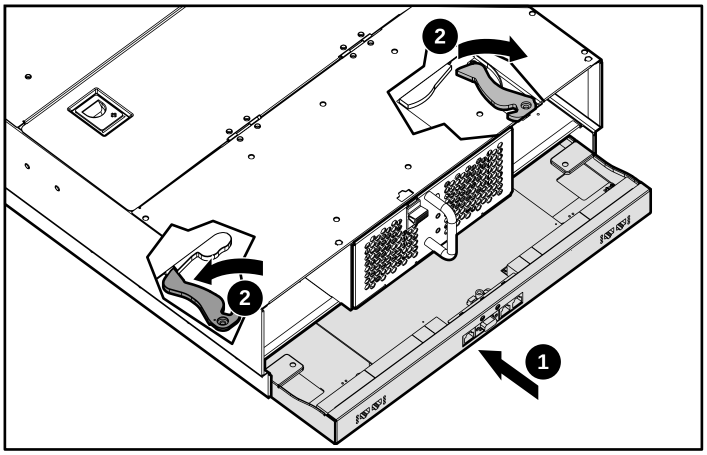


Figure 2-11: Inserting the interconnect switch tray and engaging the interconnect tray levers

8. Insert the interconnect switch tray into the server blade enclosure (1).
9. Simultaneously rotate both ejector levers to the locked position (2).

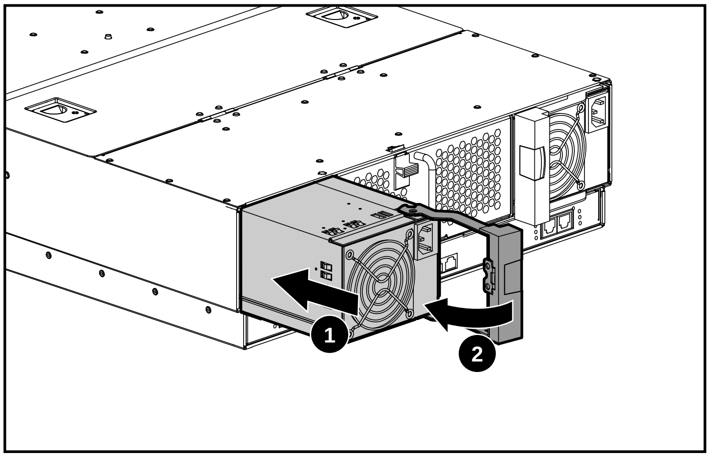


Figure 2-12: Installing a hot-plug power supply

10. Install the hot-plug power supplies (1).
11. Push the power supply handles to the closed position (2).

Planning the Interconnect Switch Configuration

Before you configure the switch modules, Compaq recommends that you plan the configuration. As you plan, keep in mind the default settings, security issues and privileges, and whether you want to configure each switch module manually or configure multiple switch modules at the same time.

Default Settings

IMPORTANT: See Appendix C for detailed default configuration settings.

The interconnect switch ships with a default configuration with all ports (of both Switch A and Switch B) enabled and assigned the same virtual LAN (VLAN). In addition, the Integrated Administrator management connector (connected to internal port 23 of Switch A) is assigned to the same default VLAN.

This default configuration simplifies your initial setup by allowing you to use a single uplink cable (from any external Ethernet connector) to connect the server blade enclosure and its server blades to your network. Keep in mind that your environment may require other configurations.

When planning the configuration, consider the defaults for the following parameters:

- Switch module IP settings
- VLAN and GVRP settings
- STP settings
- Port names and types
- Multilink trunk settings

- CoS settings
- Interswitch cross-connect settings
- SNMP/RMON settings
- User name and password settings
- Default access to various management interfaces
- IGMP Snooping settings

Security Issues

When planning the configuration for a switch module, secure access to the management interface by:

- Creating users with various access levels to the local console, remote Telnet, and Web interface. See Table 2-1 for the three levels of user access privileges.
- Enabling or disabling access to various management interfaces to fit the security policy.
- Changing default SNMP/RMON community strings for read-only and read-write access.

Root, User+, and User Privileges

There are three levels of user privileges: Root, User+, and User. Some menu selections available to users with Root privileges may not be available to those with User+ and User privileges.

The following table summarizes the user privileges.

Table 2-1: User Privileges

Privilege	Root	User+	User
Configuration	Yes	Read-only	Read-only
Network Monitoring	Yes	Read-only	Read-only
Community Strings and Trap Stations	Yes	Read-only	Read-only
Update Firmware and Configuration Files	Yes	No	No
System Utilities	Yes	Ping-only	Ping-only
Factory Reset	Yes	No	No
Reboot Switch	Yes	Yes	No
Add/Update/Delete User Accounts	Yes	No	No
View User Accounts	Yes	No	No

Manually Configuring a Switch Module

A switch module can be configured manually using a local console interface, a remote Telnet console interface, a Web interface, or an SNMP/RMON interface. See Chapters 3 and 4 for information on how to use these interfaces to configure the switch modules.

After a switch module is configured, you can back up the configuration as a binary file to a TFTP server. The backup configuration file can then be downloaded from the TFTP server to restore the switch module back to the original configuration, under one of the following conditions:

- The switch module configuration gets corrupted during operation.
- The switch module needs to be replaced due to hardware failure.

Configuring Multiple Switch Modules

You can configure multiple switch modules using the SNMP script utility or a TFTP server.

Using the SNMP Script Utility

The SNMP script utility, provided with the interconnect switch, allows you to execute customized configuration templates on multiple switch modules. Each configuration template can be tailored to one of the multiple switch modules, and then that first configuration can be deployed to other switch modules from a central deployment workstation.

Using a TFTP Server

If the basic configuration of multiple switch modules in your network is the same, you can manually configure one switch module, upload the configuration to a TFTP server, and use the configuration as a basic configuration template file. This basic configuration template can then be downloaded to multiple switch modules. Switch module IP addresses are acquired by default using DHCP, therefore, each module has a unique IP address. Each switch module can then be remotely accessed from a central deployment workstation and an individual switch module configuration can be entered to meet specific network requirements. See the “Saving Setting to TFTP Server” and “Downloading Configuration File on TFTP Server” sections in Chapter 3 (console management interface) and Chapter 4 (Web-based management interface).

Cabling the Interconnect Switch Tray

After installing the interconnect switch hardware and planning the configuration, cable the interconnect switch tray to your network.

CAUTION: In order to avoid damaging the server blade enclosure, observe the following guidelines when cabling:

- Connect the AC power cords last.
- Be sure to connect both AC power cords for redundancy and proper cooling.
- Bundle all cables and route them to the edge of the rack for proper cooling and airflow.

To cable the interconnect switch tray:

1. Connect the Integrated Administrator module to your network by using the management connector (10/100 Ethernet).

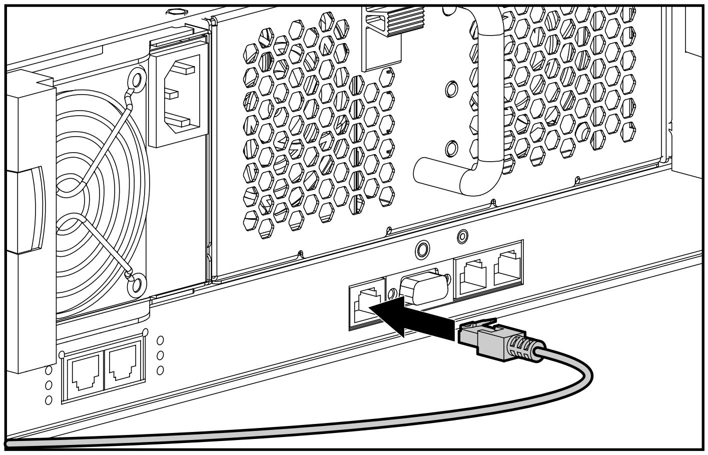


Figure 2-13: Connecting the Integrated Administrator module

2. Install the network cables. By default, each server blade has PXE enabled on Ethernet Port 1. Since the Ethernet Port 1 of every server blade physically routes through Switch A, Compaq recommends that either Port 25 or 26 of Switch A be used for PXE functions.

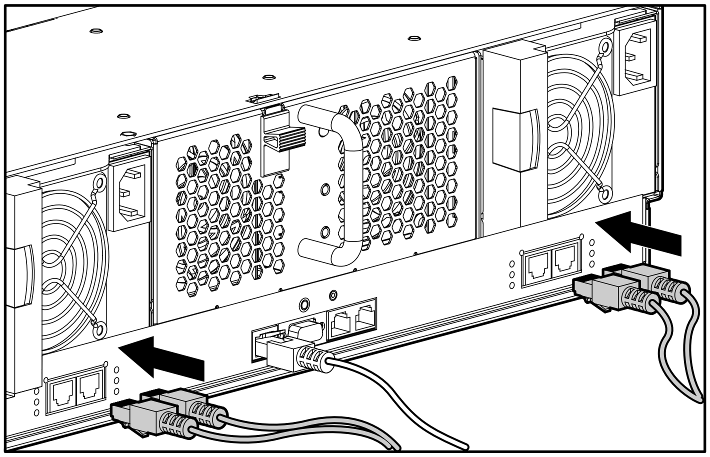


Figure 2-14: Connecting the network cables

3. Install the power cords. The server blade enclosure and interconnect switch power up as soon as power is applied to the enclosure.

> ⚠ **CAUTION:** Because the server blade enclosure uses both power supplies for power redundancy and proper cooling, be sure that both power cords are connected at all times.

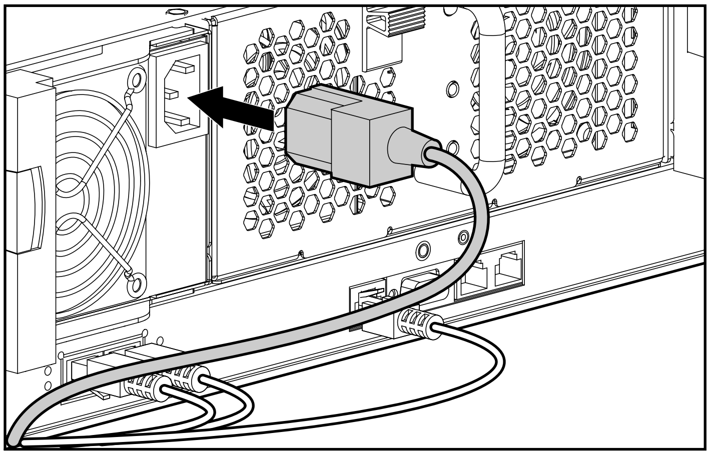


Figure 2-15: Connecting the power cables

4. Bundle the network and power cables together and route them to the outer edge of the rack.

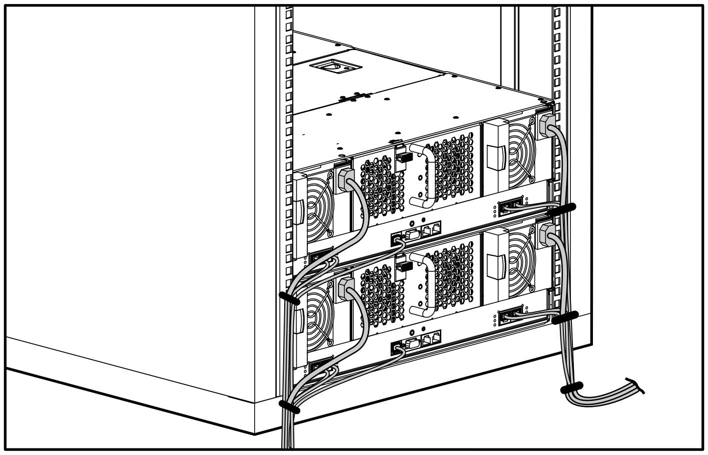


Figure 2-16: Routing the cables

Configuring the Integrated Administrator

After cabling the interconnect switch to your network, the next step is to configure the Integrated Administrator module. The Integrated Administrator module enables monitoring and managing of all functions within a server blade enclosure, as well as the ability to configure the switch modules. After the switch modules are configured, the Integrated Administrator module provides these features through both a Web-based user interface and a command line interface.

You can connect to the Integrated Administrator module command-line interface locally or remotely.

- For local, out-of-band access, connect a null-modem cable into the serial port on the back of the enclosure, and then use VT100 terminal emulation software to connect.
- For remote access, you can use a Telnet or Secure Shell session to connect to the built-in network controller.

NOTE: For complete instructions, refer to the *Compaq ProLiant BL e-Class Integrated Administrator User Guide* on the Documentation CD provided with your server blade enclosure.

To configure the Integrated Administrator module:

1. Using the null-modem serial cable (provided with your server blade enclosure), connect the Integrated Administrator (serial) console connector to a local client device such as a laptop computer with VT100 terminal emulation software.

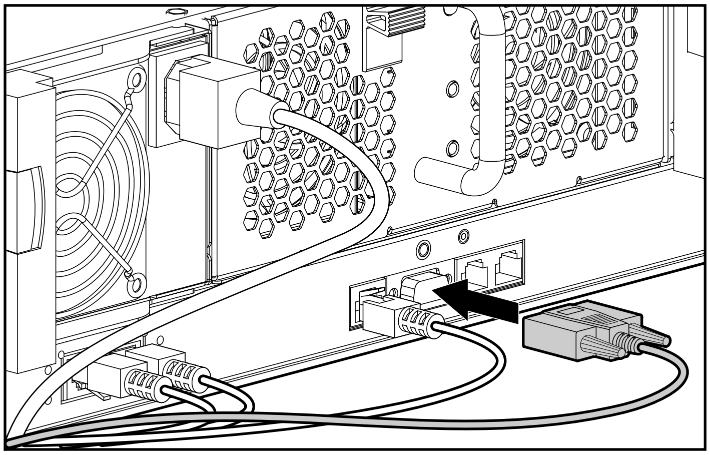


Figure 2-17: Connecting the Integrated Administrator (serial) console connector

2. Open a VT100 terminal emulation session with the following settings: 9600 baud rate, eight data bits, no parity, one stop bit, and hardware flow control disabled.
3. Log on to the Integrated Administrator using the user name and password provided on the tag attached to the interconnect switch tray. The tag contains a unique default password that should be changed during your first logon session.

IMPORTANT: User name and password are case-sensitive.

4. Determine the Integrated Administrator IP address using one of the following methods:

   NOTE: For more information, such as determining the Integrated Administrator IP address using the Web-based user interface, refer to the *Compaq ProLiant BL e-Class Integrated Administrator User Guide* on the Documentation CD provided with your server blade enclosure.

   a. If a DHCP server is attached to the network, type the following at the command line to determine the Integrated Administrator IP address:

   ```
   show network
   ```

   b. If a DHCP server is **not** attached to the network, then type the following commands to assign a static IP address to the Integrated Administrator:

   ```
   set ipconfig static <IP address> <subnet mask>
   set gateway <IP address>
   set DNS <primary DNS server address> {<secondary DNS server
   address>}
   restart
   ```

   You may now access the Integrated Administrator module through a Web browser, Secure Shell, Telnet, or SNMP connection.

5. Perform the following tasks as soon as the Integrated Administrator IP address is assigned:

   a. Reset the administrator password

   b. Set the day, date, and time

   c. Name the server blade enclosure and rack

   d. Set up groups, users, and access privileges

Accessing the Switch Modules

After your ProLiant e-Class C-GbE Interconnect Switch is installed and cabled, you can access and configure the switch modules through the Integrated Administrator software.

1. Access the switch modules from the Integrated Administrator command line interface using one of the following methods:

   a. If you have already logged into the Integrated Administrator as the “Administrator,” you can connect to either switch module console using one of the following commands:

   `connect switch a` to access Switch A

   or

   `connect switch b` to access Switch B

b. If you have **not** logged on to the Integrated Administrator, you can use one of two special logon accounts to access the switch module consoles directly, depending on whether you want to access Switch A or Switch B. At the login prompt type in both the user name and password as either:

```
switcha
```

or

```
switchb
```

The logon screen for Switch A or Switch B will now be displayed.

2. Perform the following tasks for each switch module:
   a. Configure the IP address
   b. Set up users, passwords, and access privileges
   c. Change default SNMP community strings for read/write and read-only

NOTE: After you configure the IP address on the switch module, the switch module can be accessed using Telnet, SNMP, or a Web browser. See the “Configuring IP Address,” section in Chapter 3.

See Chapter 3 for information on how to use the console management interface to change configuration settings and monitor its operation using one of the following:

- Local Serial RS-232 Console Management Interface through Integrated Administrator
- Remote Telnet Console Management Interface

See Chapter 4 for information on how to use the embedded Web-based (HTML) interface to manage the interconnect switch from anywhere on the network using a standard browser, such as Netscape Navigator or Microsoft Internet Explorer.

Appendix E provides information regarding the SNMP and RMON Agents along with the MIBs supported. This appendix also discusses how to use these MIBs to configure and monitor the switch modules using a generic SNMP manager.

Additional Information

For additional information refer to the Compaq website at

www.compaq.com/support/servers

3

Configuring the Switch Modules Using the Console Management Interface

Introduction

Your ProLiant BL e-Class C-GbE Interconnect Switch supports a console management interface that allows you to set up and control your switch modules, either with an ordinary terminal (or terminal emulator), or over the network using the TCP/IP Telnet protocol. You can use this facility to perform many basic network management functions. In addition, the console program allows you to configure the switch modules for management using an SNMP-based network management system. This chapter describes how to use the console interface to log on the switch modules, change their settings, and monitor their operation.

Before You Begin

The ProLiant BL e-Class C-GbE Interconnect Switch supports a wide array of functions and provides flexibility and increased network performance. These capabilities require some planning to arrive at a deployment strategy that maximizes the potential of the interconnect switch. See the “Planning the Interconnect Switch Configuration” section in Chapter 2 for items to keep in mind as you configure your switch modules.

Accessing the Console Management Interface

You can access the console management interface by connecting through the Integrated Administrator, as discussed in Chapter 2, or remotely using a Telnet program. All of the screens are identical, whether they are accessed through the Integrated Administrator or through a Telnet interface.

Before you can access the console management interface through a Telnet program (in VT-100-compatible terminal mode), you must first access the console management interface through the Integrated Administrator and set an IP address for the switch module. See the section, “Configuring IP Address,” in this chapter for information on how to set up the IP address.

Using the Console Management Interface

The console management interface provides many features that make configuring the switch module and navigating through the system easy.

Navigation Features

Use the features in Table 3-1 to navigate through the screens.

Table 3-1: Console Management Interface Navigation

To	Action
Toggle between the field options	Highlight items in **<**angle brackets>, and then press the spacebar.
Enter data in a field	Highlight the item in [square brackets], and then type in the new data.
Execute a command	Highlight the command displayed in UPPERCASE letters, and then press the **Enter** key.
Move between fields on a screen	Press the **Page Up** and **Page Down** keys, the left and right arrow keys, the **Tab** key, or the **Backspace** key.
Display the previous screen	Press the **Esc** key.
Display the main menu	Press **Ctrl+T.**
Refresh the screen display	Press **Ctrl+R.**
Display the next page of information	Press the **N** key.
Display the previous page of information	Press the **P** key.

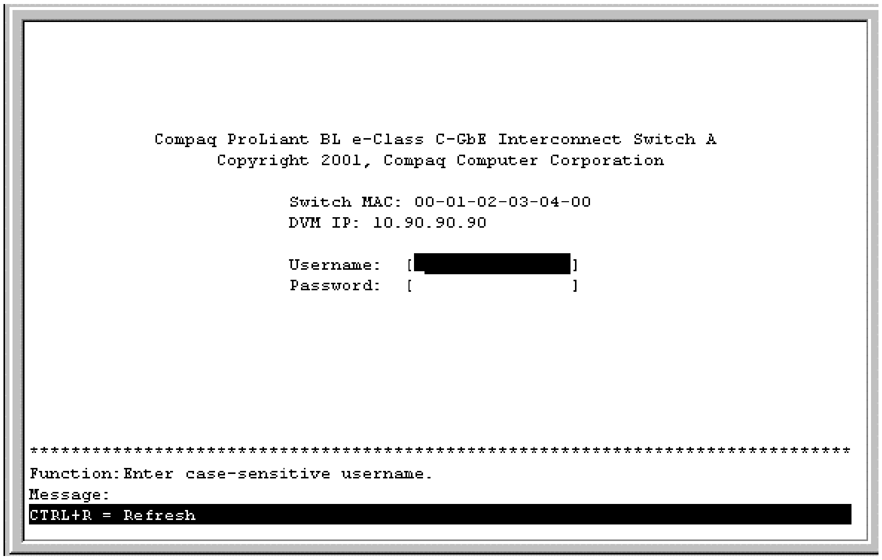
Field-level Help and System Messages

The bottom section of each screen displays field-level help and system messages.

- **Function**—Displays field-level help.
- **Message**—Displays system messages.

Logging on to the Switch Module

When you log on to a switch module, the following logon screen is displayed. Notice that the name of the switch module (Switch A or Switch B) is also displayed on the screen.



```
           Compaq ProLiant BL e-Class C-GbE Interconnect Switch A
                  Copyright 2001, Compaq Computer Corporation

                          Switch MAC: 00-01-02-03-04-00
                          DVM IP: 10.90.90.90

                          Username:  [                ]
                          Password:  [                ]

*******************************************************************************
Function: Enter case-sensitive username.
Message:
CTRL+R = Refresh
```

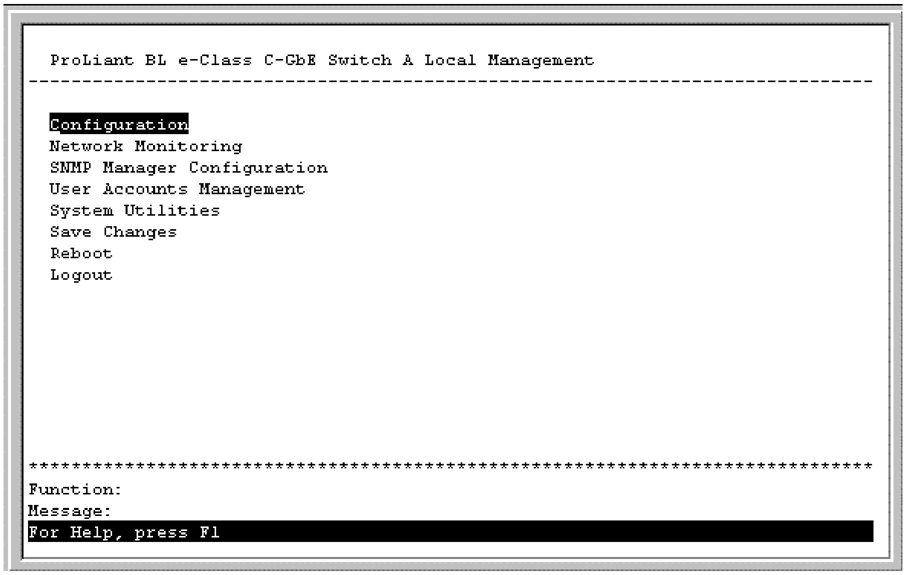
IMPORTANT: The switch module does not have any initial user names or passwords set. Compaq recommends that after logging on, you create at least one Root-level user as the switch administrator. (See Table 2-1 in Chapter 2, “Setting up and Installing the Interconnect Switch,” for an explanation of user privileges.) If you forget your password after it has been set up, call Compaq Customer Support for assistance.

To log on for the first time:

1. Leave the **Username** field blank and press the **Tab** key.

2. Leave the **Password** field blank and press the **Enter** key. The main menu for the switch module is displayed.

NOTE: Subsequent users will enter their user name and password, then press the **Enter** key.



```
  ProLiant BL e-Class C-GbE Switch A Local Management
--------------------------------------------------------------------------------

  Configuration
  Network Monitoring
  SNMP Manager Configuration
  User Accounts Management
  System Utilities
  Save Changes
  Reboot
  Logout








********************************************************************************
Function:
Message:
For Help, press F1
```

The main menu displays the major categories for switch management.

Setting up New Users

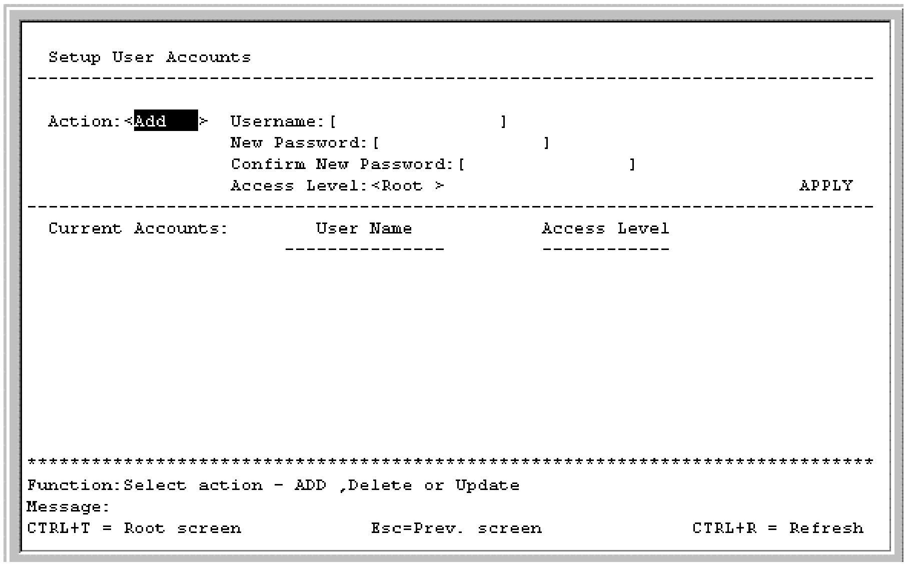
You can set up a maximum of eight users on a switch module.

NOTE: After logging on to the switch module for the first time, you need to set up at least one user account with Root privileges.

To create a new user account:

1. Highlight **User Accounts Management** on the main menu.

2. Press the **Enter** key. The **Setup User Accounts** screen is displayed.



```
  Setup User Accounts
-------------------------------------------------------------------------------

  Action:<Add    >  Username:[                ]
                    New Password:[                ]
                    Confirm New Password:[                ]
                    Access Level:<Root >                                APPLY
-------------------------------------------------------------------------------
  Current Accounts:       User Name          Access Level
                       ---------------       ------------









*******************************************************************************
Function:Select action - ADD ,Delete or Update
Message:
CTRL+T = Root screen           Esc=Prev. screen            CTRL+R = Refresh
```

3. Using the spacebar, toggle the **Action** field to display **ADD.**

   NOTE: The other options are **Delete,** which allows the deletion of a user entry, and **Update,** which allows for changes to be made to an existing user entry.

4. Type the user's name in the **Username** field.
5. Type an initial password for the user in the **New Password** field.

   NOTE: Passwords used to access the switch module are case-sensitive.

6. Type the new password a second time in the **Confirm New Password** field.
7. Using the spacebar, toggle the **Access Level** field to select the user's access privilege.
8. Highlight **APPLY.**
9. Press the **Enter** key to make the user addition effective. A listing of all current user accounts and access levels is displayed.

   IMPORTANT: **APPLY** makes changes to the switch configuration for the current session only. You must enter all permanent changes, including user additions or updates, into non-volatile RAM (NVRAM) using the **Save Changes** option on the main menu. See the "Saving Changes" section.

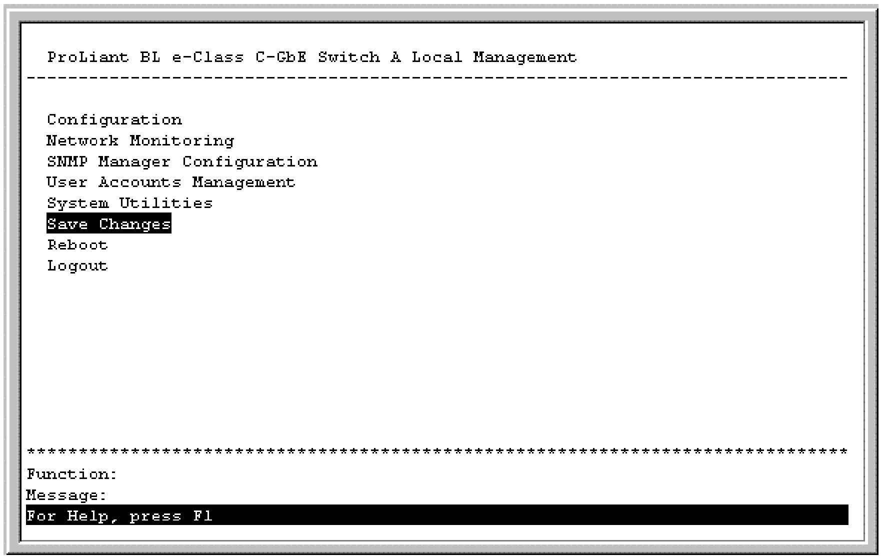
10. Press the **Esc** key to return to the main menu. Use the **Save Changes** option to save the changes into non-volatile RAM.

Saving Changes

The switch module has two levels of memory, normal RAM and non-volatile RAM (NVRAM). Configuration changes are made effective on a screen by highlighting **APPLY,** then pressing **Enter.** When this is done, the settings are immediately applied to the switching software in RAM.

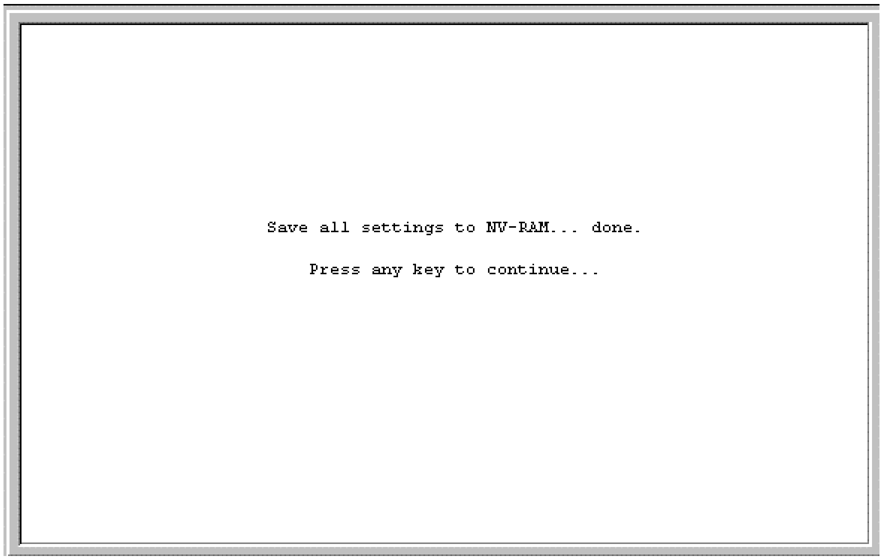
Some settings require you to restart the switch module before they will take effect. Restarting the switch module erases all settings in RAM and reloads the stored settings from the NVRAM. Thus, it is necessary to save all setting changes to NVRAM before rebooting the switch module.

To retain any configuration changes permanently:



```
  ProLiant BL e-Class C-GbE Switch A Local Management
-------------------------------------------------------------------------------

  Configuration
  Network Monitoring
  SNMP Manager Configuration
  User Accounts Management
  System Utilities
  Save Changes
  Reboot
  Logout

*******************************************************************************
Function:
Message:
For Help, press F1
```

1. Highlight **Save Changes** on the main menu.
2. Press the **Enter** key. The following screen is displayed to verify that your new settings have been saved to NVRAM.



```
Save all settings to NV-RAM... done.

    Press any key to continue...
```

After the configuration settings have been saved to NVRAM, they become the default settings for the switch module. These settings are then used every time the switch module is rebooted.

IMPORTANT: After saving your final configuration, Compaq highly recommends that you save the configuration image to TFTP server storage. See the “Saving Settings to TFTP Server” section in Chapter 3 for more information.

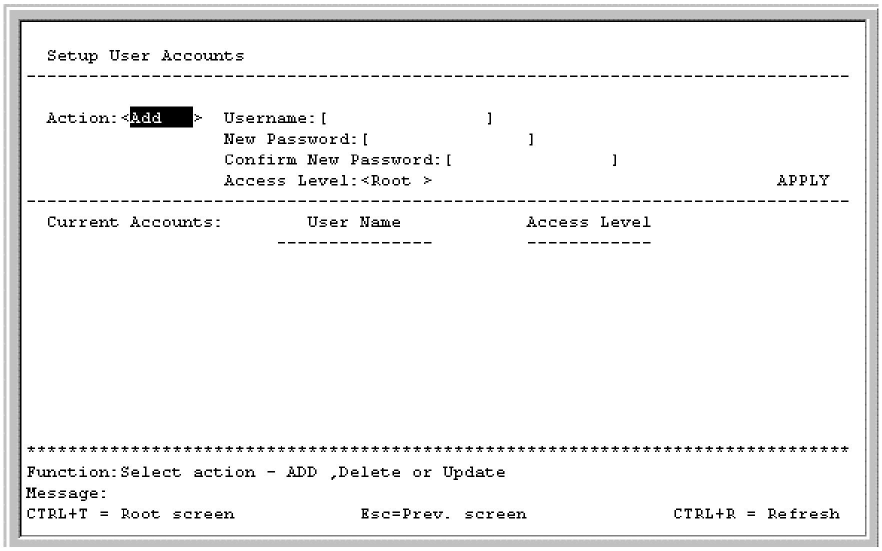
Managing User Accounts

Changes to user accounts are made through the **User Account Management** option on the main menu. Only a user with Root privileges can make changes to user accounts.

Updating a User Account

To update a user password or privilege level:

1. Highlight **User Accounts Management** on the main menu.
2. Press the **Enter** key. The **Setup User Accounts** screen is displayed.



```
  Setup User Accounts
-------------------------------------------------------------------------------

  Action:<Add     >  Username:[                ]
                     New Password:[                ]
                     Confirm New Password:[                ]
                     Access Level:<Root >                                 APPLY
-------------------------------------------------------------------------------
  Current Accounts:        User Name          Access Level
                        ---------------      ------------








*******************************************************************************
Function:Select action - ADD ,Delete or Update
Message:
CTRL+T = Root screen            Esc=Prev. screen             CTRL+R = Refresh
```

3. Toggle the **Action** field to select **Update.**
4. Type the user name for the account you want to change in the **Username** field.
5. If the password is to be changed, type the new password in the **New Password** field.
6. Type the new password again in the **Confirm New Password** field.
7. If the privilege level is to be changed, toggle the **Access Level** field until the appropriate level is displayed—**Root, User+,** or **User.**

8. Highlight **APPLY.**
9. Press the **Enter** key to make the change effective.

NOTE: To save the configuration settings permanently, you must enter them into NVRAM using the **Save Changes** option on the main menu. See the “Saving Changes” section earlier in this chapter.

Viewing Current User Accounts

To view the current user accounts:

1. Highlight **User Accounts Management** on the main menu.
2. Press the **Enter** key. The **Setup User Accounts** screen displays a list of all current user accounts.

Deleting a User Account

To prevent accidental deletion of all of the users with Root privilege, the console interface does not allow you delete the current logged-on user.

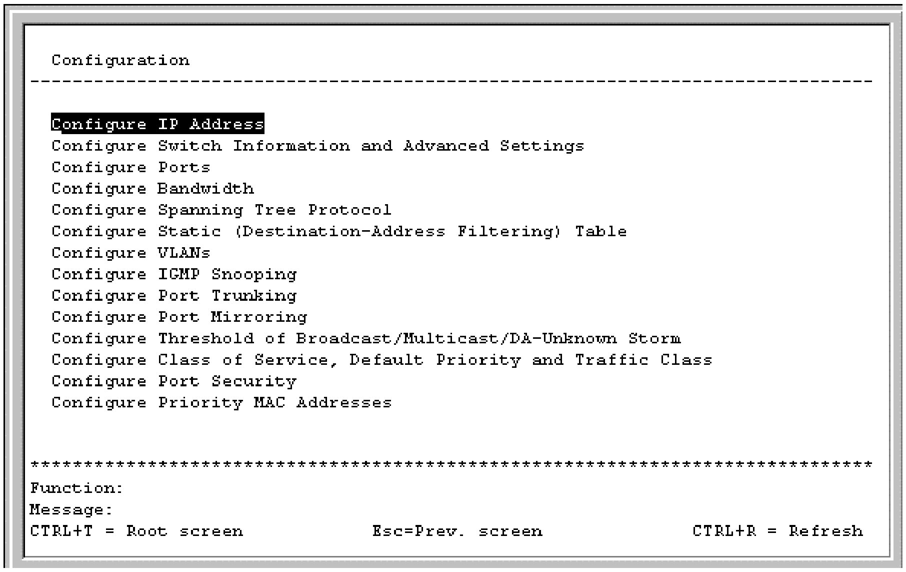
To delete a user account:

1. Highlight **User Accounts Management** on the main menu.
2. Press the **Enter** key. The **Setup User Accounts** screen displays a list of all current user accounts.
3. Toggle the **Action** field to **Delete.**
4. Type the user name in the **Username** field.
5. Type the user’s password for the account you want to delete in the **New Password** field.
6. Highlight **APPLY.**
7. Press the **Enter** key.

NOTE: To save the configuration settings permanently, you must enter them into NVRAM using the **Save Changes** option on the main menu. See the “Saving Changes” section earlier in this chapter.

Configuring the Switch Module

This section describes options found under the **Configuration** menu.



```
  Configuration
-------------------------------------------------------------------------------

  Configure IP Address
  Configure Switch Information and Advanced Settings
  Configure Ports
  Configure Bandwidth
  Configure Spanning Tree Protocol
  Configure Static (Destination-Address Filtering) Table
  Configure VLANs
  Configure IGMP Snooping
  Configure Port Trunking
  Configure Port Mirroring
  Configure Threshold of Broadcast/Multicast/DA-Unknown Storm
  Configure Class of Service, Default Priority and Traffic Class
  Configure Port Security
  Configure Priority MAC Addresses


*******************************************************************************
Function:
Message:
CTRL+T = Root screen           Esc=Prev. screen             CTRL+R = Refresh
```

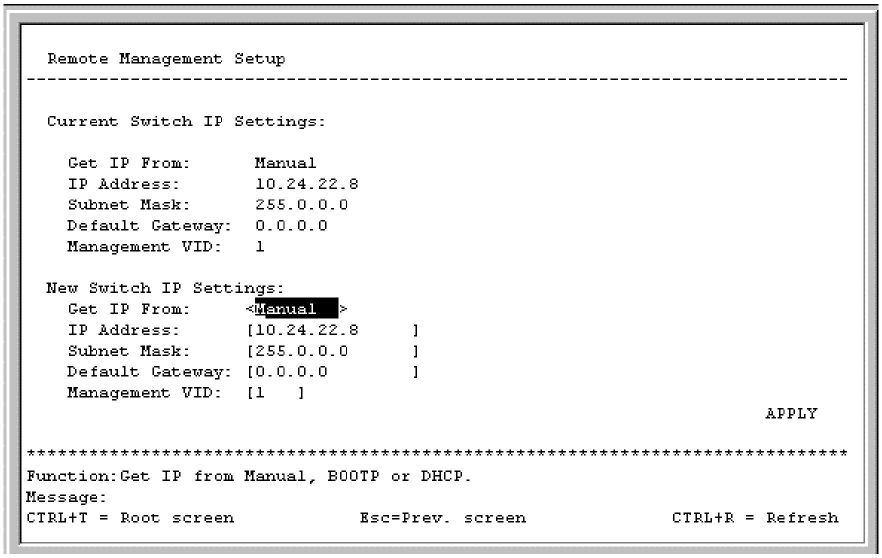
Configuring the IP Address

Some settings must be entered to allow the switch module to be managed from an SNMP-based Network Management System, such as SNMP v1, or to be able to access the switch module using the Telnet protocol.

To set up the switch module for remote management:

1. Highlight **Configure IP Address** from the **Configuration** menu.

2. Press the **Enter** key. The following screen is displayed.



```
  Remote Management Setup
-------------------------------------------------------------------------------

  Current Switch IP Settings:

    Get IP From:      Manual
    IP Address:       10.24.22.8
    Subnet Mask:      255.0.0.0
    Default Gateway:  0.0.0.0
    Management VID:   1

  New Switch IP Settings:
    Get IP From:     <Manual  >
    IP Address:      [10.24.22.8     ]
    Subnet Mask:     [255.0.0.0      ]
    Default Gateway: [0.0.0.0        ]
    Management VID:  [1   ]
                                                                     APPLY

*******************************************************************************
Function:Get IP from Manual, BOOTP or DHCP.
Message:
CTRL+T = Root screen           Esc=Prev. screen            CTRL+R = Refresh
```

The **Remote Management Setup** screen lets you specify how the switch module will be assigned an IP address, which allows an in-band network management system (for example, Telnet) client to find it on the network.

The fields listed under the **Current Switch IP Settings** heading are those that are currently being used by the switch module. Those fields listed under the **New Switch IP Settings** heading are those which will be used after the switch module has been rebooted.

To reset the switch module IP settings:

1. Toggle the **Get IP From** field to choose from **Manual, BOOTP,** or **DCHP.** This action selects how the switch module will be assigned an IP address on the next reboot or startup.
    - **BOOTP**—The switch module sends out a BOOTP broadcast request when it is powered up. The BOOTP protocol allows IP addresses, network masks, and default gateways to be assigned by a central BOOTP server. If this option is set, the switch module first looks for a BOOTP server to provide it with this information before using the default or previously entered settings.
    - **DCHP**—The switch module sends out a DCHP broadcast request when it is powered up. The DCHP protocol allows IP addresses, network masks, and default gateways to be assigned by a DCHP server. If this option is set, the switch module first looks for a DCHP server to provide it with this information before using the default or previously entered settings.

— **Manual**—This option allows the entry of an IP address, subnet mask, and default gateway for the switch module. The data in these fields should be of the form *xxx.xxx.xxx.xxx*, where each *xxx* is a number between 0 and 255. This address should be a unique address on the network assigned for use by the Network Administrator. The fields that require entries under this option include:

  — **Subnet Mask**—A Bitmask that determines the extent of the subnet that the switch module is on. The value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network, but custom subnet masks are allowed.

  — **Default Gateway**—An IP address that determines where packets with a destination address outside the current subnet should be sent. This is usually the address of a router or a host acting as an IP gateway. If your network is not part of an intranet, or you do not want the switch module to be accessible outside your local network, you can leave this field unchanged.

If you select Manual, type the appropriate data into the **IP Address, Subnet Mask,** and **Default Gateway** fields.

2. Type the VLAN ID (VID) of a VLAN that will have access to the Telnet manager in the **Management VID** field. This ID will be the VID of the VLAN on which a management station is located.
3. Highlight **APPLY.**
4. Press the **Enter** key to make the change effective.

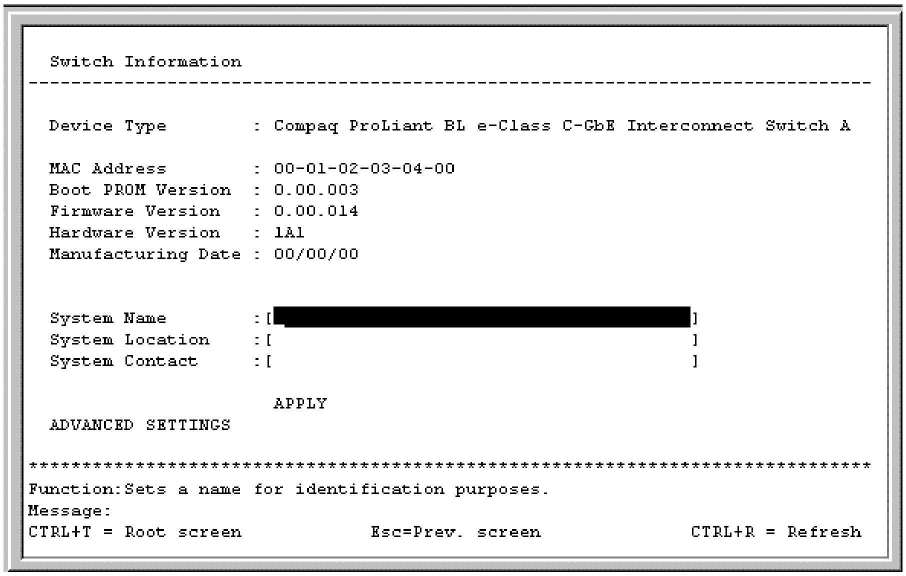
NOTE: To save the configuration settings permanently, you must enter them into NVRAM using the **Save Changes** option on the main menu. See the “Saving Changes” section earlier in this chapter.

Configuring the Switch Module Information and Advanced Settings

To configure the switch module information and advanced settings:

1. Highlight **Configure Switch Information and Advanced Settings** from the **Configuration** menu.

2. Press the **Enter** key. The following screen is displayed.



```
  Switch Information
-------------------------------------------------------------------------------

  Device Type        : Compaq ProLiant BL e-Class C-GbE Interconnect Switch A

  MAC Address        : 00-01-02-03-04-00
  Boot PROM Version  : 0.00.003
  Firmware Version   : 0.00.014
  Hardware Version   : 1A1
  Manufacturing Date : 00/00/00


  System Name        :[                                      ]
  System Location    :[                                      ]
  System Contact     :[                                      ]

                      APPLY
  ADVANCED SETTINGS

*******************************************************************************
Function:Sets a name for identification purposes.
Message:
CTRL+T = Root screen            Esc=Prev. screen             CTRL+R = Refresh
```

Configuring Switch Module Information

The **Switch Information** menu shows the type of switch, any external modules that are installed, and the **MAC address** (assigned by the factory and unchangeable) for that switch module. In addition, the **Boot PROM** and **Firmware Version** numbers are shown. This information is helpful in monitoring PROM and firmware updates and to obtain the MAC address for entry into another network device's address table.

To complete the switch module information:

1. Type the name of the system in the **System Name** field.
2. Type the location of the system in the **System Location** field.
3. Type the name and telephone number of the System Administrator in the **System Contact** field. Compaq recommends that the person who is responsible for the maintenance of the network system on which this switch module is installed be listed here.
4. Highlight **APPLY.**
5. Press the **Enter** key to make the change effective.

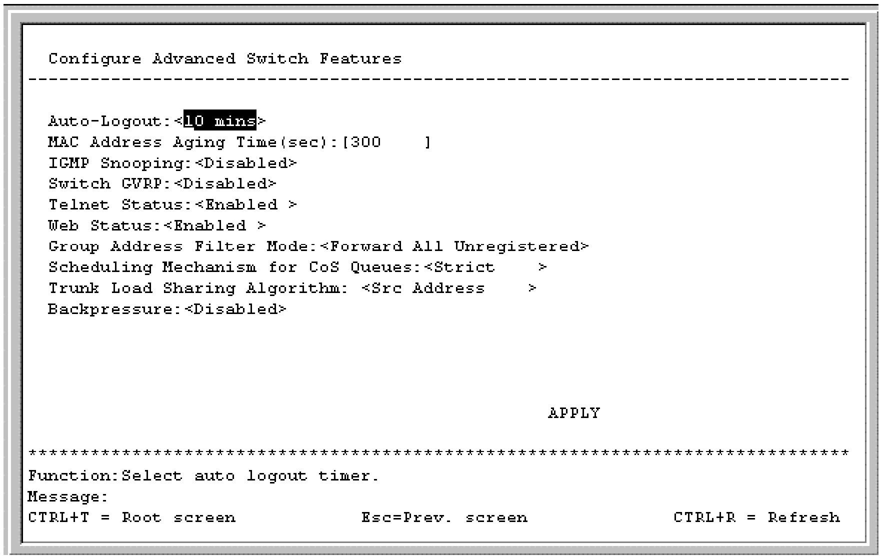
NOTE: To save the configuration settings permanently, you must enter them into NVRAM using the **Save Changes** option on the main menu. See the "Saving Changes" section earlier in this chapter.

Configuring Advanced Switch Module Features

To configure advanced switch module features:

1. Highlight **ADVANCED SETTINGS** at the bottom of the **Switch Information** menu.

2. Press the **Enter** key. The following screen is displayed.



```
  Configure Advanced Switch Features
-------------------------------------------------------------------------------

  Auto-Logout:<10 mins>
  MAC Address Aging Time(sec):[300    ]
  IGMP Snooping:<Disabled>
  Switch GVRP:<Disabled>
  Telnet Status:<Enabled >
  Web Status:<Enabled >
  Group Address Filter Mode:<Forward All Unregistered>
  Scheduling Mechanism for CoS Queues:<Strict    >
  Trunk Load Sharing Algorithm: <Src Address    >
  Backpressure:<Disabled>




                                                  APPLY

*******************************************************************************
Function:Select auto logout timer.
Message:
CTRL+T = Root screen            Esc=Prev. screen             CTRL+R = Refresh
```

This screen allows you to set the following features:

- **Auto-Logout**—Sets the time the interface can be idle before the switch module automatically logs out the user. The options are **2 mins, 5 mins, 10 mins, 15 mins,** and **Never.**
- **MAC Address Aging Time (sec)**—Specifies the length of time a learned MAC address remains in the forwarding table without being accessed (that is, how long a learned MAC address is allowed to remain idle). The **Aging Time** can be set to any value between 10 and 1,000,000 seconds.

NOTE: A very long aging time can result in out-of-date Dynamic Entries that may cause incorrect packet filtering/forwarding decisions. A very short aging time may cause entries to be aged out too soon, resulting in a high percentage of received packets whose source addresses cannot be found in the address table, in which case the switch module will broadcast the packet to all ports, negating many of the benefits of having a switch.

- **IGMP** Snooping—Enables Internet Group Management Protocol (IGMP) Snooping, which enables the switch module to read IGMP packets being forwarded through the switch module in order to obtain forwarding information from them and learn which ports contain multicast members.
- **Switch GVRP**—Allows members to dynamically join VLANs. This feature is used to enable or disable Group VLAN Registration Protocol (GVRP) on the switch module.
- **Telnet Status**—Allows access to the switch module over the network using the TCP/IP Telnet protocol by toggling to **Enabled.**
- **Web Status**—Allows use of a Web-based browser to manage the switch module by toggling to **Enabled.**

- **Group Address Filter Mode**—Sets the IGMP filter mode for processing multicast packets. The options are **Forward All, Forward All Unregistered,** and **Filtered All Unregistered.**
- **Scheduling Mechanism for CoS Queues**—Provides two possibilities for setting Class of Service queue options, **RoundRobin** and **Strict.** If you select **Strict,** when the highest priority queue is full, those packets are the first to be forwarded. If you select **RoundRobin,** the forwarding is based on the settings made on the **Class of Service Configuration** screen.
- **Trunk Load Sharing Algorithm**—Sets options for trunk load sharing. The trunk load sharing options are **Dst Address, Src&Dst Address,** and **Src Address.**
- **Backpressure**—Select Enabled or Disabled to initiate or terminate traffic flow control in and out of the interconnect switch.

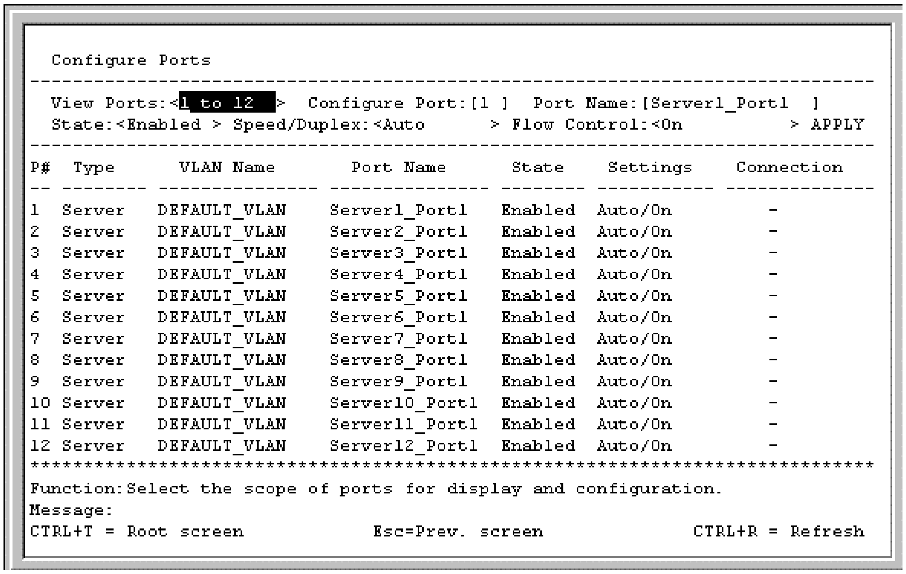
3. After making your changes, highlight **APPLY,** then press the **Enter** key.

NOTE: To save the configuration settings permanently, you must enter them into NVRAM using the **Save Changes** option on the main menu. See the “Saving Changes” section earlier in this chapter.

Configuring Port Settings

To configure ports:

1. Highlight **Configure Ports** from the **Configuration** menu.
2. Press the **Enter** key. The following screen is displayed.



```
  Configure Ports
-------------------------------------------------------------------------------
  View Ports:<1 to 12  >  Configure Port:[1 ]  Port Name:[Server1_Port1  ]
  State:<Enabled > Speed/Duplex:<Auto      > Flow Control:<On          > APPLY
-------------------------------------------------------------------------------
P#  Type      VLAN Name       Port Name       State    Settings    Connection
-- -------- --------------- --------------- -------- ----------- --------------
1  Server   DEFAULT_VLAN    Server1_Port1   Enabled  Auto/On         -
2  Server   DEFAULT_VLAN    Server2_Port1   Enabled  Auto/On         -
3  Server   DEFAULT_VLAN    Server3_Port1   Enabled  Auto/On         -
4  Server   DEFAULT_VLAN    Server4_Port1   Enabled  Auto/On         -
5  Server   DEFAULT_VLAN    Server5_Port1   Enabled  Auto/On         -
6  Server   DEFAULT_VLAN    Server6_Port1   Enabled  Auto/On         -
7  Server   DEFAULT_VLAN    Server7_Port1   Enabled  Auto/On         -
8  Server   DEFAULT_VLAN    Server8_Port1   Enabled  Auto/On         -
9  Server   DEFAULT_VLAN    Server9_Port1   Enabled  Auto/On         -
10 Server   DEFAULT_VLAN    Server10_Port1  Enabled  Auto/On         -
11 Server   DEFAULT_VLAN    Server11_Port1  Enabled  Auto/On         -
12 Server   DEFAULT_VLAN    Server12_Port1  Enabled  Auto/On         -
*******************************************************************************
Function:Select the scope of ports for display and configuration.
Message:
CTRL+T = Root screen           Esc=Prev. screen            CTRL+R = Refresh
```

3. Toggle the **View Ports** field, using the space bar, to view the configuration of either Ports 1 through 12 or Ports 13 through 24.
4. Type the port number in the **Configure Port** field.
5. Toggle the **State** field to either enable or disable a given port.

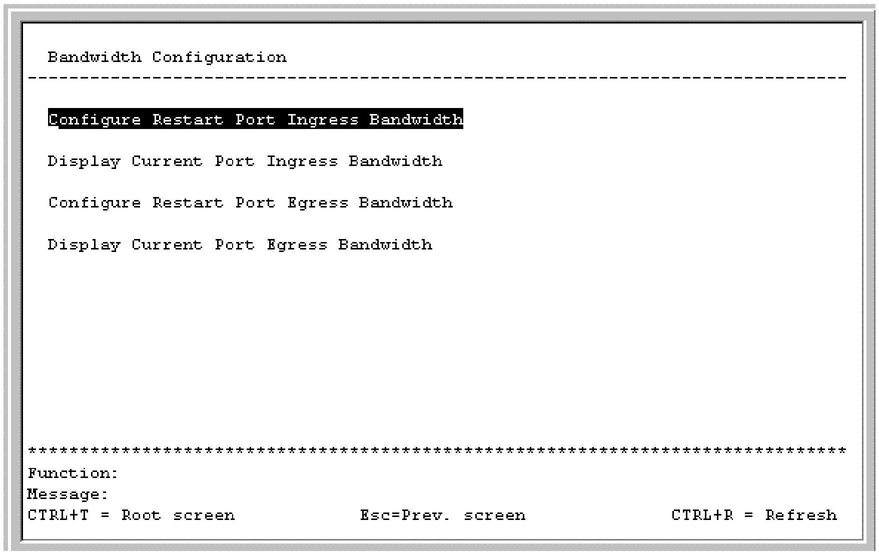
6. Toggle the **Speed/Duplex** field to select the speed and duplex/half-duplex state of the port. **Auto** means auto-negotiation between 10 and 100 Mb/s devices, in full- or half-duplex mode. The **Auto** setting allows the port to automatically determine the fastest settings the device the port is connected to can handle. The other options are **100M/Full, 100M/Half, 10M/Full,** or **10M/Half.** There is no automatic adjustment of port settings with any option other than **Auto.**
7. Toggle **Flow Control** to **On** or **Off** when either **100M/Full** or **10M/Full** is selected.
8. Highlight **APPLY.**
9. Press the **Enter** key to make the change effective.

NOTE: To save the configuration settings permanently, you must enter them into NVRAM using the **Save Changes** option on the main menu. See the "Saving Changes" section earlier in this chapter.

Configuring Bandwidth

To configure bandwidth:

1. Highlight **Configure Bandwidth** on the **Configuration** menu.
2. Press the **Enter** key. The following screen is displayed.



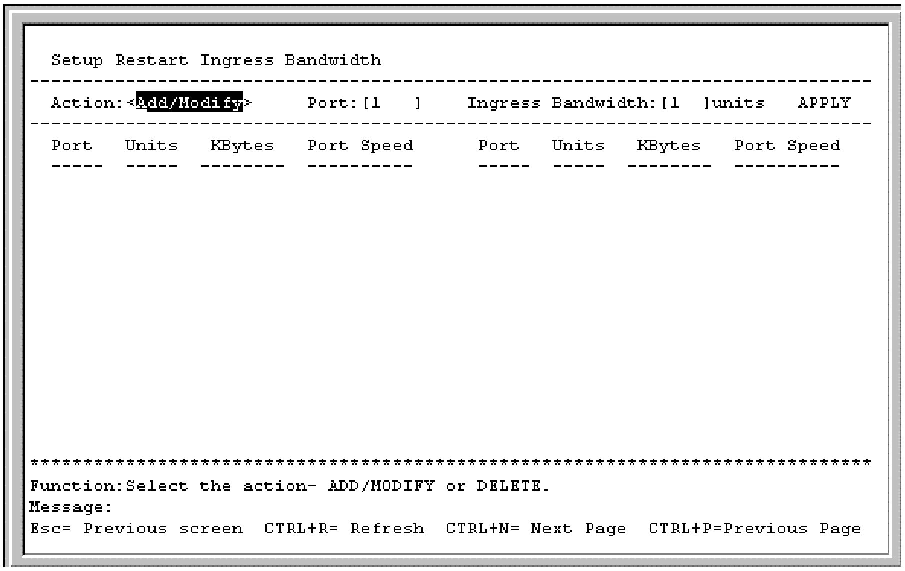
```
  Bandwidth Configuration
-------------------------------------------------------------------------------

  Configure Restart Port Ingress Bandwidth

  Display Current Port Ingress Bandwidth

  Configure Restart Port Egress Bandwidth

  Display Current Port Egress Bandwidth









*******************************************************************************
Function:
Message:
CTRL+T = Root screen           Esc=Prev. screen            CTRL+R = Refresh
```

The **Bandwidth Configuration** menu allows you to access screens that set and display the ingress bandwidth and egress bandwidth of specified ports on the switch module.

Configuring Restart Port Ingress Bandwidth

To configure restart port ingress bandwidth:

1. Highlight **Configure Restart Port Ingress Bandwidth** on the **Bandwidth Configuration** menu.
2. Press **Enter.** The following screen is displayed.



```
  Setup Restart Ingress Bandwidth
-------------------------------------------------------------------------------
  Action:<Add/Modify>     Port:[1   ]    Ingress Bandwidth:[1  ]units   APPLY
-------------------------------------------------------------------------------
  Port   Units   KBytes   Port Speed      Port   Units   KBytes   Port Speed
  -----  -----  --------  ----------      -----  -----  --------  ----------









*******************************************************************************
Function:Select the action- ADD/MODIFY or DELETE.
Message:
Esc= Previous screen  CTRL+R= Refresh  CTRL+N= Next Page  CTRL+P=Previous Page
```

To configure ingress bandwidth for a specific port:

1. Toggle the **Action** field to **Add/Modify.**

   NOTE: To delete an entry, toggle the **Action** field to **Delete.**

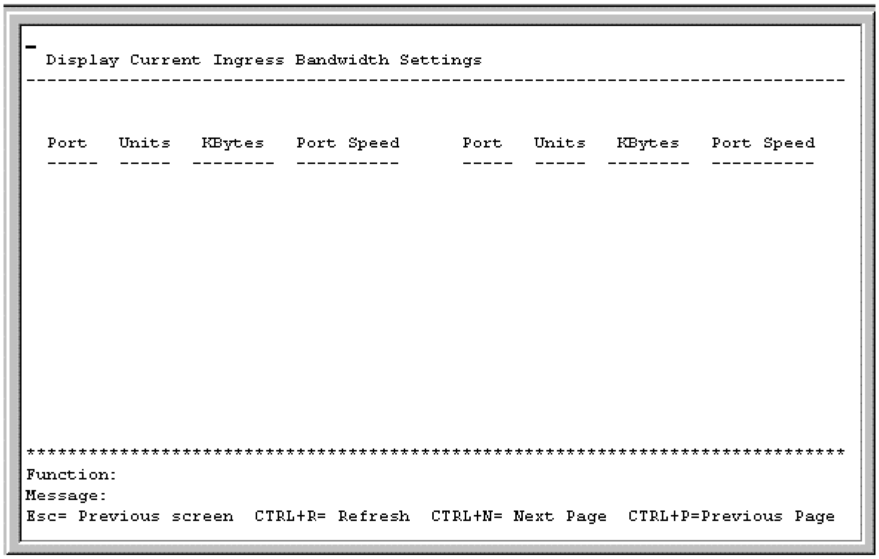
2. Type a port number in the **Port** field.
3. Type a number between 1 and 127 in the **Ingress Bandwidth** field.
4. Highlight **APPLY.**
5. Press the **Enter** key.
6. Save the changes using **Save Changes** on the main menu.
7. Reboot the switch module to allow your changes to take effect.

Displaying Current Port Ingress Bandwidth

To view the current port ingress bandwidth settings:

1. Highlight **Display Current Port Ingress Bandwidth** on the **Bandwidth Configuration** menu.

2. Press the **Enter** key. The following screen is displayed.



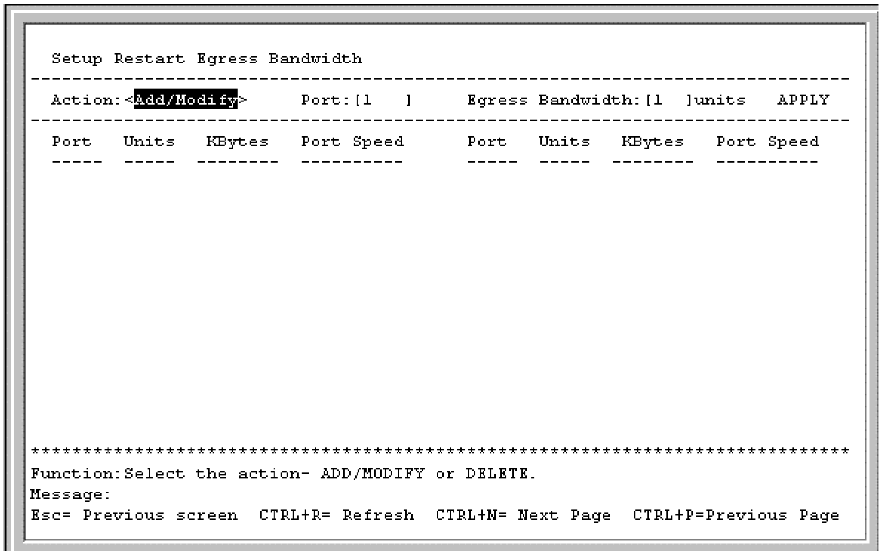
```
_
  Display Current Ingress Bandwidth Settings
-------------------------------------------------------------------------------


  Port   Units   KBytes   Port Speed      Port   Units   KBytes   Port Speed
  -----  -----  --------  ----------      -----  -----  --------  ----------











*******************************************************************************
Function:
Message:
Esc= Previous screen  CTRL+R= Refresh  CTRL+N= Next Page  CTRL+P=Previous Page
```

This read-only screen displays current ingress bandwidth information.

Configuring Restart Port Egress Bandwidth

To configure port egress bandwidth:

1. Highlight **Configure Restart Port Egress Bandwidth** on the **Bandwidth Configuration** screen.
2. Press the **Enter** key. The following screen is displayed.



```
  Setup Restart Egress Bandwidth
-------------------------------------------------------------------------------
  Action:<Add/Modify>     Port:[1   ]     Egress Bandwidth:[1  ]units   APPLY
-------------------------------------------------------------------------------
  Port   Units   KBytes   Port Speed      Port   Units   KBytes   Port Speed
  -----  -----  --------  ----------      -----  -----  --------  ----------











*******************************************************************************
Function:Select the action- ADD/MODIFY or DELETE.
Message:
Esc= Previous screen  CTRL+R= Refresh  CTRL+N= Next Page  CTRL+P=Previous Page
```

3. Toggle to **Add/Modify** in the **Action** field.

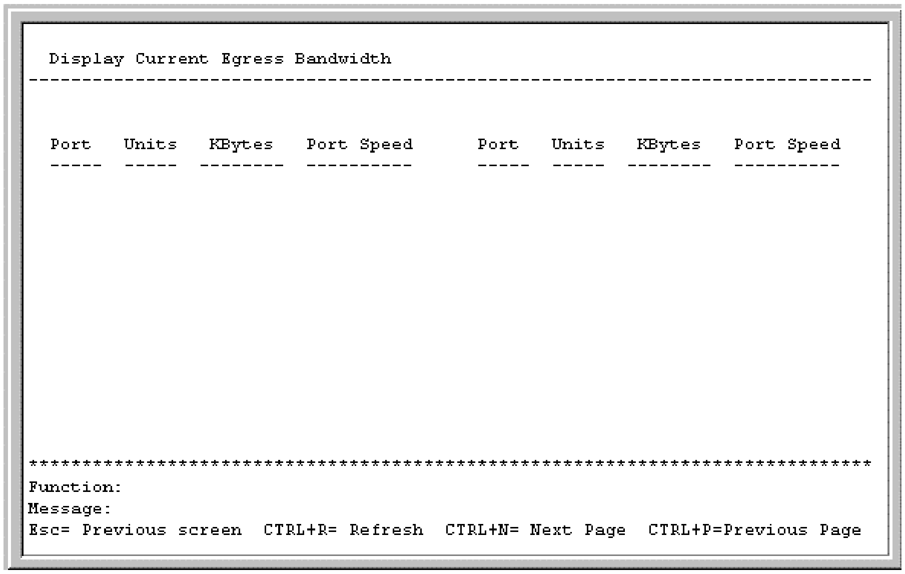
NOTE: To delete an entry, toggle the **Action** field to **Delete.**

4. Type a destination port in the **Port** field.
5. Type a number between 1 and 127 in the **Egress Bandwidth** field.
6. Highlight **APPLY.**
7. Press the **Enter** key.
8. Save the changes using **Save Changes** on the main menu.
9. Reboot the switch module to allow your changes take effect.

Displaying Current Port Egress Bandwidth Settings

To view port egress bandwidth settings:

1. Highlight **Display Current Port Egress Bandwidth** on the **Bandwidth Configuration** menu.
2. Press the **Enter** key. The following screen is displayed.



```
  Display Current Egress Bandwidth
--------------------------------------------------------------------------------


  Port   Units   KBytes   Port Speed      Port   Units   KBytes   Port Speed
  -----  -----  --------  ----------      -----  -----  --------  ----------














********************************************************************************
Function:
Message:
Esc= Previous screen  CTRL+R= Refresh  CTRL+N= Next Page  CTRL+P=Previous Page
```

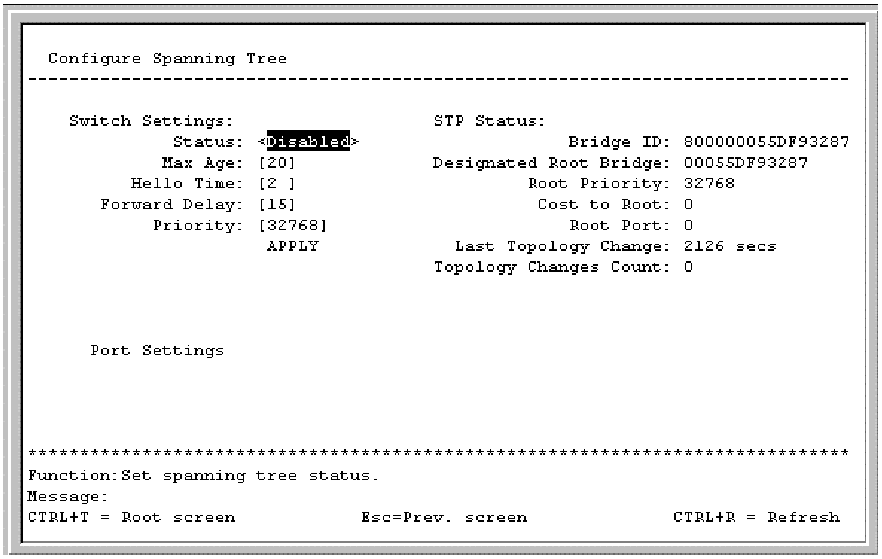
This read-only screen displays current egress bandwidth information.

Configuring Spanning Tree Protocol

To globally configure Spanning Tree Protocol (STP) on the switch module:

1. Highlight **Configure Spanning Tree Protocol** on the **Configuration** menu.

2. Press the **Enter** key. The following screen is displayed.



```
  Configure Spanning Tree
-------------------------------------------------------------------------------

    Switch Settings:                     STP Status:
              Status: <Disabled>                      Bridge ID: 800000055DF93287
             Max Age: [20]               Designated Root Bridge: 00055DF93287
          Hello Time: [2 ]                        Root Priority: 32768
       Forward Delay: [15]                         Cost to Root: 0
            Priority: [32768]                         Root Port: 0
                       APPLY               Last Topology Change: 2126 secs
                                         Topology Changes Count: 0



      Port Settings




*******************************************************************************
Function:Set spanning tree status.
Message:
CTRL+T = Root screen            Esc=Prev. screen              CTRL+R = Refresh
```

STP operates on two levels: the switch module level and the port level. On the switch module level, the settings are globally implemented. On the port level, the settings are implemented on a per user-defined group basis.

NOTE: The factory default settings should cover the majority of installations. Compaq recommends that you keep the default settings as set at the factory unless it is absolutely necessary to change them.

The user-changeable parameters in the switch module are:

— **Status**—Toggle to **Enabled** to implement STP on the switch module.

— **Max Age**—The maximum age can be set from 6 to 40 seconds. At the end of the maximum age, if a Bridge Protocol Data Unit (BPDU) has still not been received from the Root Bridge, your switch module will start sending its own BPDU to all other switches for permission to become the Root Bridge. If your switch module has the lowest Bridge Identifier, it will become the Root Bridge.

— **Hello Time**—The hello time can be set from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge. If you set a hello time for your switch module, and it is not the Root Bridge, the set hello time will be used if and when your switch module becomes the Root Bridge.

NOTE: The hello time cannot be longer than the maximum age, otherwise, a configuration error will occur.

— **Forward Delay**—The forward delay can be from 4 to 30 seconds. This is the time any port on the switch module spends in the listening state while moving from the blocking state to the forwarding state.

— **Priority**—A priority for the switch module can be set from 0 to 65535. 0 is equal to the highest priority. This number is used in the voting process between switches on the network to determine which switch module will be the Root switch module. A low number indicates a high priority, and a high probability that this switch module will be elected as the Root switch module.

NOTE: Observe the following formulas when setting the previously-mentioned parameters:

- Max. Age ≤ 2 x (Forward Delay - 1 second)
- Max. Age ≥ 2 x (Hello Time + 1 second)

3. After making your changes, highlight **APPLY,** then press the **Enter** key.

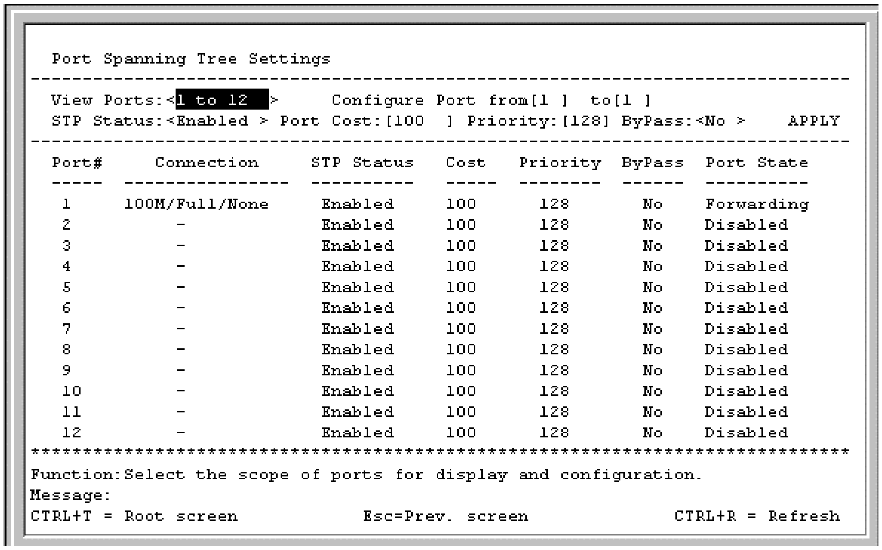
NOTE: To save the configuration settings permanently, you must enter them into NVRAM using the **Save Changes** option on the main menu. See the “Saving Changes” section earlier in this chapter.

Configuring Port Spanning Tree Settings

In addition to setting Spanning Tree parameters for use on the switch module level, the switch module allows for the configuration of STP on individual ports.

To define individual ports:

1. Highlight **Port Settings** on the **Configure Spanning Tree** menu.
2. Press the **Enter** key. The following screen is displayed.



```
  Port Spanning Tree Settings
------------------------------------------------------------------------------
  View Ports:<1 to 12  >     Configure Port from[1 ]  to[1 ]
  STP Status:<Enabled > Port Cost:[100  ] Priority:[128] ByPass:<No >    APPLY
------------------------------------------------------------------------------
  Port#     Connection      STP Status   Cost   Priority  ByPass  Port State
  -----  ----------------  ----------   -----  --------  ------  ----------
   1     100M/Full/None     Enabled     100      128       No    Forwarding
   2           -            Enabled     100      128       No    Disabled
   3           -            Enabled     100      128       No    Disabled
   4           -            Enabled     100      128       No    Disabled
   5           -            Enabled     100      128       No    Disabled
   6           -            Enabled     100      128       No    Disabled
   7           -            Enabled     100      128       No    Disabled
   8           -            Enabled     100      128       No    Disabled
   9           -            Enabled     100      128       No    Disabled
   10          -            Enabled     100      128       No    Disabled
   11          -            Enabled     100      128       No    Disabled
   12          -            Enabled     100      128       No    Disabled
******************************************************************************
Function:Select the scope of ports for display and configuration.
Message:
CTRL+T = Root screen           Esc=Prev. screen            CTRL+R = Refresh
```

3. Toggle the **View Ports** field to the range of ports to be configured. The Fast Ethernet ports displayed for configuration in groups of 12 and the optional 100Base-TX ports are displayed together—if a 2-port rather than a 1-port extension module is installed.

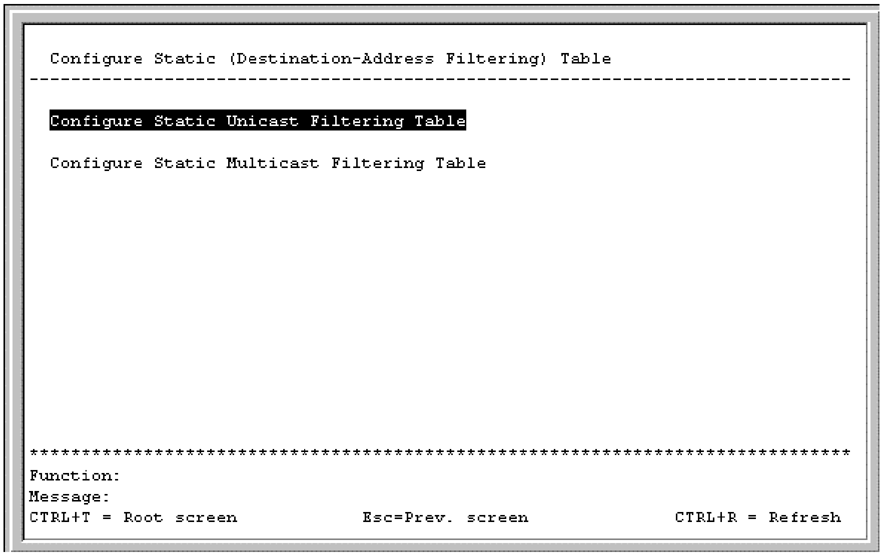
4. Type the port number or port range in the **Configure Port** field.
5. Toggle the **STP Status** field to **Enable** or **Disable.**
6. Type the Spanning Tree port cost in the **Port Cost** field.
7. Type the Spanning Tree priority in the **Priority** field.
8. Toggle the **Bypass** field to **Yes** if you want to enable the switch module to skip the usual waiting time associated with the listening state. (This is also known as fast forward.)
9. Highlight **APPLY.**
10. Press the **Enter** key.

NOTE: To save the configuration settings permanently, you must enter them into NVRAM using the **Save Changes** option on the main menu. See the “Saving Changes” section earlier in this chapter.

Configuring the Static (Destination-Address Filtering) Table

To configure the Static (Destination-Address Filtering) Table:

1. Highlight **Configure Static (Destination-Address Filtering) Table** on the **Configuration** menu.
2. Press the **Enter** key. The following screen is displayed.



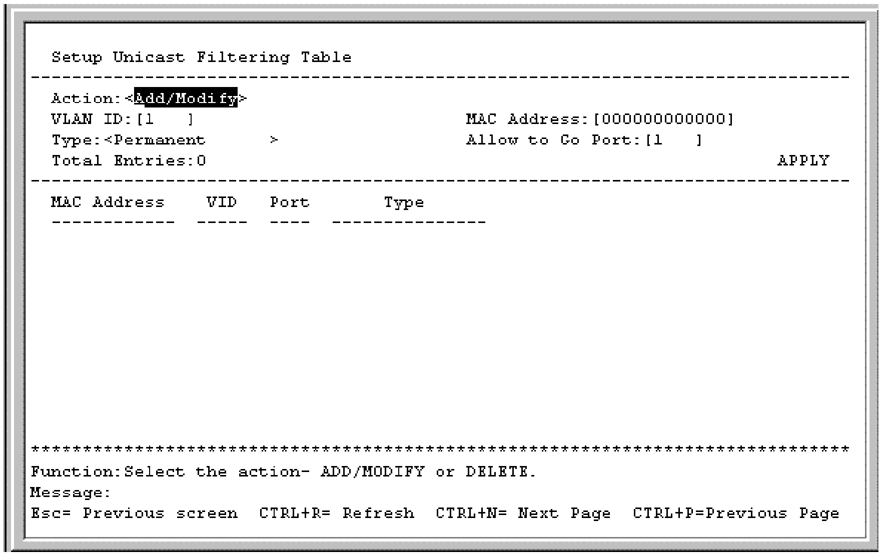
```
  Configure Static (Destination-Address Filtering) Table
-------------------------------------------------------------------------------

  Configure Static Unicast Filtering Table

  Configure Static Multicast Filtering Table













*******************************************************************************
Function:
Message:
CTRL+T = Root screen           Esc=Prev. screen              CTRL+R = Refresh
```

The **Configure Static (Destination-Address Filtering) Table** menu allows you to access screens to create, modify, and delete both the Static Unicast Filtering Table and the Static Multicast Filtering Table.

Configuring Static Unicast Filtering Table

To configure the **Static Unicast Table:**

1. Highlight **Configure Static Unicast Table** on the **Configure Static (Destination-Address Filtering) Table** menu.
2. Press the **Enter** key. The following screen is displayed.



```
  Setup Unicast Filtering Table
-------------------------------------------------------------------------------
  Action:<Add/Modify>
  VLAN ID:[1   ]                        MAC Address:[000000000000]
  Type:<Permanent      >                Allow to Go Port:[1   ]
  Total Entries:0                                                     APPLY
-------------------------------------------------------------------------------
  MAC Address    VID   Port       Type
  ------------  -----  ----  ---------------









*******************************************************************************
Function:Select the action- ADD/MODIFY or DELETE.
Message:
Esc= Previous screen  CTRL+R= Refresh  CTRL+N= Next Page  CTRL+P=Previous Page
```

3. Toggle the **Action** field between **Add/Modify** and **Delete.**
4. Type the VID in the **VLAN ID** field.
5. Type the MAC address to be statically entered in the forwarding table in the **MAC Address** field.
6. Toggle the **Type** field to **Permanent** or **DeleteOnReset,** to set the unicast filter type.
7. Type the port number in the **Port** field.
8. Highlight **APPLY.**
9. Press the **Enter** key.

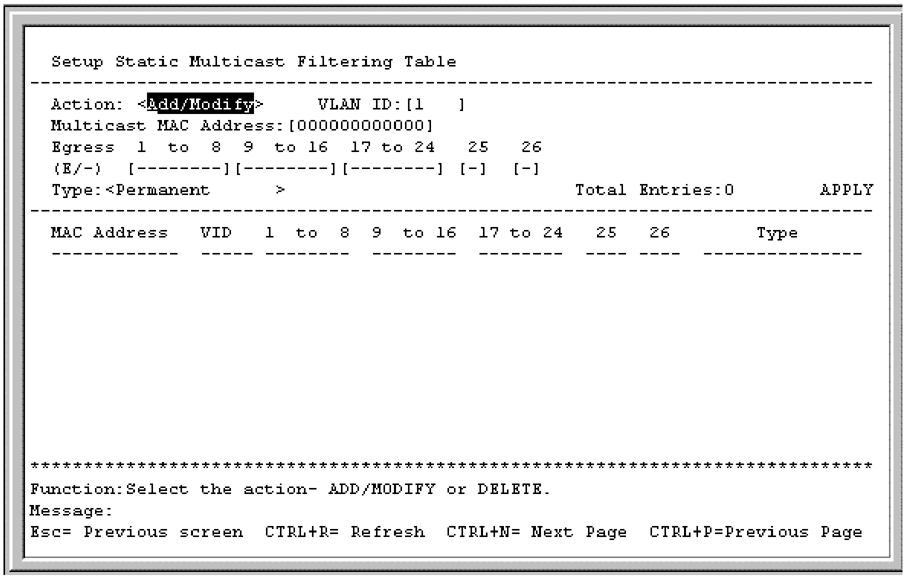
NOTE: To save the configuration settings permanently, you must enter them into NVRAM using the **Save Changes** option on the main menu. See the “Saving Changes” section earlier in this chapter.

Configuring Static Multicast Filtering Table

To edit the IEEE 802.1q Multicast Filtering settings:

1. Highlight **Configure Static Multicast Filtering Table** on the **Configure Static (Destination-Address Filtering) Table.**

2. Press the **Enter** key. The following screen is displayed.



```
  Setup Static Multicast Filtering Table
-------------------------------------------------------------------------------
  Action: <Add/Modify>     VLAN ID:[1   ]
  Multicast MAC Address:[000000000000]
  Egress  1  to  8  9  to 16  17 to 24   25   26
  (E/-)  [--------][--------][--------] [-]  [-]
  Type:<Permanent      >                          Total Entries:0       APPLY
-------------------------------------------------------------------------------
  MAC Address   VID   1  to  8  9  to 16  17 to 24   25   26        Type
  ------------  ----- --------  --------  --------  ---- ----  ---------------










*******************************************************************************
Function:Select the action- ADD/MODIFY or DELETE.
Message:
Esc= Previous screen  CTRL+R= Refresh  CTRL+N= Next Page  CTRL+P=Previous Page
```

3. Toggle to **Add/Modify** in the **Action** field.
4. Type the VLAN ID number of the VLAN that will be receiving the multicast packets in the **VLAN ID** field.
5. Type the MAC address of the multicast source in the **Multicast MAC Address** field.
6. Set the multicast group membership of each port by highlighting **(E/-)** field using the arrow keys, and then toggling between **E, F,** or — using the space bar.
    a. **E** (Egress Member)—Specifies the port as being a static member of the multicast group. Egress Member Ports are ports that transmit traffic for the multicast group.
    b. **F** (Forbidden Nonmember)—Specifies the port as not being a member of the multicast group and that the port is forbidden from becoming a member of the multicast group dynamically.
    c. **—** (Nonmember)—Specifies the port as not being a member of the multicast group, but the port can become a member of the multicast group dynamically.
7. Toggle to the static multicast filter type **Permanent** or **DeleteOnReset** in the **Type** field.
8. Highlight **APPLY.**
9. Press the **Enter** key.

NOTE: To save the configuration settings permanently, you must enter them into NVRAM using the **Save Changes** option on the main menu. See the “Saving Changes” section earlier in this chapter.

Configuring VLANs

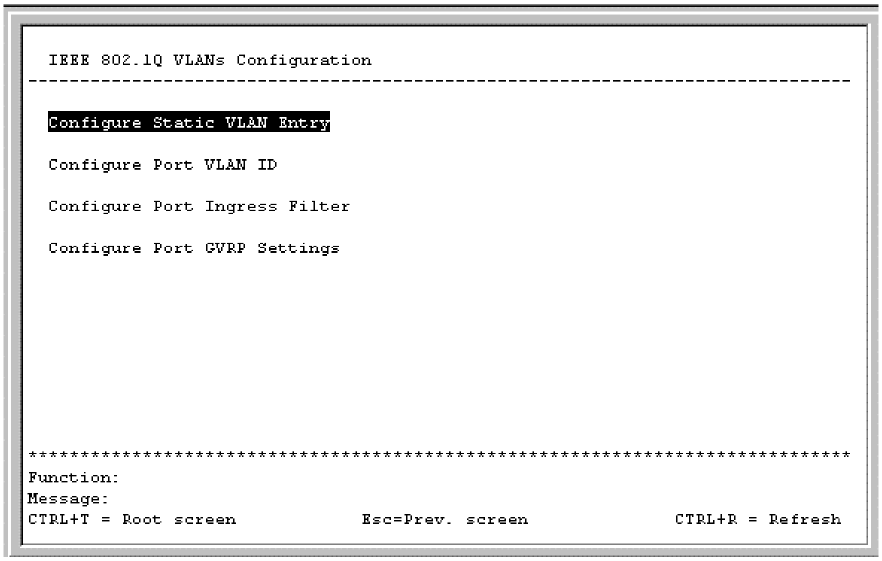
The switch module reserves one VLAN, VID = 1, called the DEFAULT_VLAN for internal use. The factory default setting assigns all ports on the switch module to the DEFAULT_VLAN. As new VLANs are configured, their respective member ports are removed from the DEFAULT_VLAN. If the DEFAULT_VLAN is reconfigured, all ports are again assigned to it. Ports that are not wanted as part of the DEFAULT_VLAN are removed during the configuration.

Packets cannot cross VLANs. If a member of one VLAN wants to connect to another VLAN, it must be through a router.

NOTE: The DEFAULT_VLAN has a VID = 1. An IP interface called System in the IP interface entry menu also has a VID = 1, and therefore corresponds to the DEFAULT_VLAN

To edit VLAN definitions and to configure port settings for IEEE 802.1Q VLAN support:

1. Highlight **Configure VLANs** on the **Configuration** menu.
2. Press the **Enter** key. The following screen is displayed.



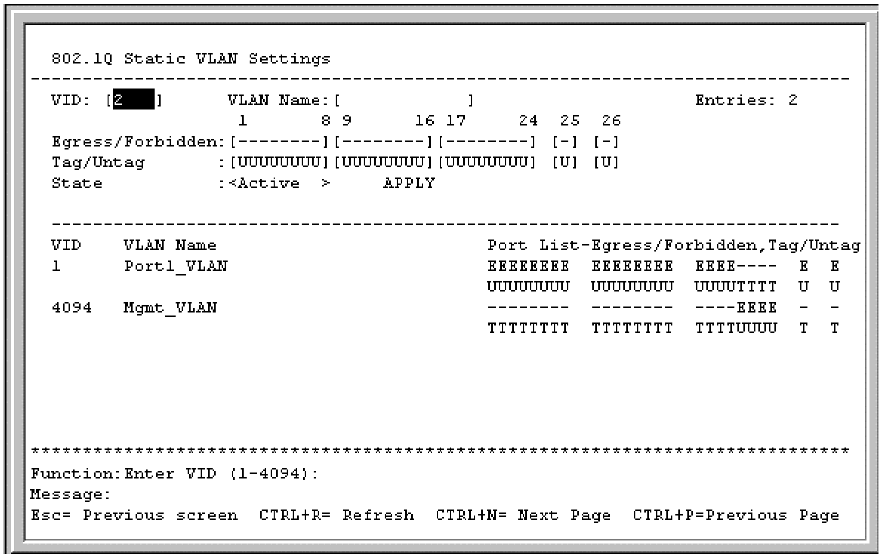
```
  IEEE 802.1Q VLANs Configuration
-------------------------------------------------------------------------------

  Configure Static VLAN Entry

  Configure Port VLAN ID

  Configure Port Ingress Filter

  Configure Port GVRP Settings









*******************************************************************************
Function:
Message:
CTRL+T = Root screen           Esc=Prev. screen             CTRL+R = Refresh
```

Configuring Static VLA N Entry

To create an 802.1Q VLAN:

1. Highlight **Configure Static VLAN Entry** on the **IEEE 802.1Q VLANs Configuration** menu.

2. Press the **Enter** key. The following screen is displayed.



```
  802.1Q Static VLAN Settings
-------------------------------------------------------------------------------
  VID: [2   ]      VLAN Name:[              ]                   Entries: 2
                    1       8 9      16 17     24  25  26
  Egress/Forbidden:[--------][--------][--------] [-] [-]
  Tag/Untag       :[UUUUUUUU][UUUUUUUU][UUUUUUUU] [U] [U]
  State           :<Active  >     APPLY

  ----------------------------------------------------------------------------
  VID    VLAN Name                          Port List-Egress/Forbidden,Tag/Untag
  1      Port1_VLAN                         EEEEEEEE  EEEEEEEE  EEEE----  E  E
                                            UUUUUUUU  UUUUUUUU  UUUUTTTT  U  U
  4094   Mgmt_VLAN                          --------  --------  ----EEEE  -  -
                                            TTTTTTTT  TTTTTTTT  TTTTUUUU  T  T






*******************************************************************************
Function:Enter VID (1-4094):
Message:
Esc= Previous screen  CTRL+R= Refresh  CTRL+N= Next Page  CTRL+P=Previous Page
```

3. Type a VLAN ID number in the **VID** field.

4. Type a name for the new VLAN in the **VLAN Name** field.

5. Set the 802.1Q VLAN membership for each port by highlighting the **Egress/Forbidden** field using the arrow keys, and then toggling between **E, F,** and — using the space bar.

    — **E** (Egress Member)—Specifies the port as being a static member of the VLAN. Egress Member Ports are ports that will be transmitting traffic for the VLAN. These ports can be either tagged or untagged.

    — **F** (Forbidden Nonmember)—Defines the port as not being a member and also forbids the port from joining a VLAN dynamically.

    — **—** (Nonmember)—Specifies the port as not being a member of the VLAN, but the port can become a member of the VLAN dynamically.

6. Set the state of each port by highlighting the **Tag/Untag** field using the arrow keys and then toggling between **U** or **T** using the space bar.

    — **U**—Specifies the port as an untagged member of the VLAN. When the port transmits an untagged packet, the packet header remains unchanged. When a tagged packet exits the port, the tag is stripped and the packet is changed to an untagged packet.

    — **T**—Specifies the port as a tagged member of the VLAN. When the port transmits an untagged packet, the packet header is changed to include the 32-bit tag associated with the PVID (Port VLAN Identifier—see the following section). When a tagged packet exits the port, the packet header is unchanged.

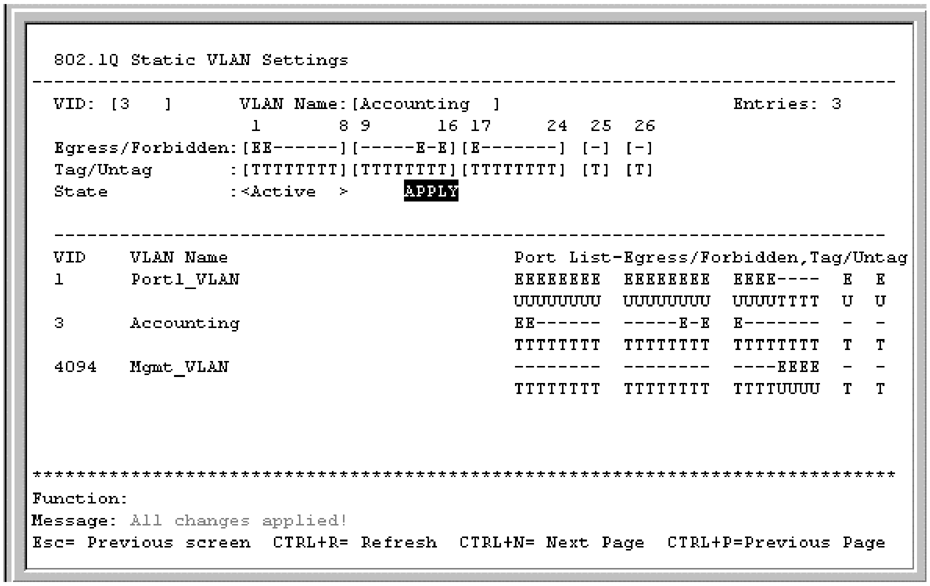
NOTE: If the port is attached to a device that is not IEEE 802.1Q VLAN compliant (VLAN-tag unaware), then set the port to U—Untagged. If the port is attached to a device that is IEEE 802.1Q VLAN compliant, (VLAN-tag aware), then set the port to T—Tagged.

7. Toggle the **State** field between **Active** and **Inactive.**
8. Highlight **APPLY.**
9. Press the **Enter** key.

NOTE: To save the configuration settings permanently, you must enter them into NVRAM using the **Save Changes** option on the main menu. See the "Saving Changes" section earlier in this chapter.

Example of 802.1Q VLAN

In the following example, the VLAN "Accounting"—VID # 3—has been added. Ports 1, 2, 14, 16, and 17 are Egress ports (static members of "Accounting").



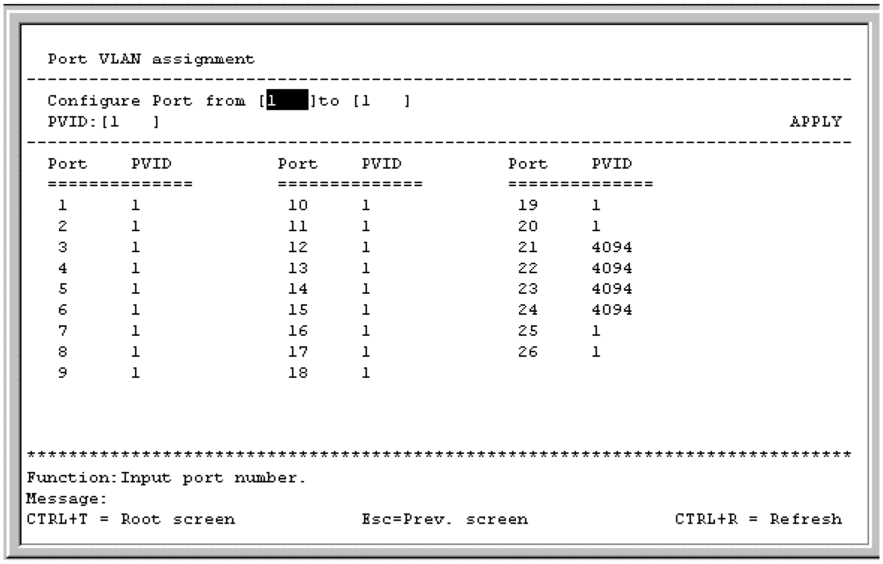
```
  802.1Q Static VLAN Settings
-------------------------------------------------------------------------------
  VID: [3   ]      VLAN Name:[Accounting  ]                     Entries: 3
                    1       8 9      16 17     24  25  26
  Egress/Forbidden:[EE------][-----E-E][E-------] [-] [-]
  Tag/Untag       :[TTTTTTTT][TTTTTTTT][TTTTTTTT] [T] [T]
  State           :<Active  >     APPLY

  ----------------------------------------------------------------------------
  VID    VLAN Name                          Port List-Egress/Forbidden,Tag/Untag
  1      Port1_VLAN                         EEEEEEEE  EEEEEEEE  EEEE----  E  E
                                            UUUUUUUU  UUUUUUUU  UUUUTTTT  U  U
  3      Accounting                         EE------  -----E-E  E-------  -  -
                                            TTTTTTTT  TTTTTTTT  TTTTTTTT  T  T
  4094   Mgmt_VLAN                          --------  --------  ----EEEE  -  -
                                            TTTTTTTT  TTTTTTTT  TTTTUUUU  T  T



*******************************************************************************
Function:
Message: All changes applied!
Esc= Previous screen  CTRL+R= Refresh  CTRL+N= Next Page  CTRL+P=Previous Page
```

Configuring a Port VLAN

To assign a port a PVID:

1. Highlight **Configure Port VLAN ID** on the **IEEE 802.1Q VLANs Configuration** menu.

2. Press the **Enter** key. The following screen is displayed.



```
  Port VLAN assignment
-------------------------------------------------------------------------------
  Configure Port from [1   ]to [1   ]
  PVID:[1   ]                                                            APPLY
-------------------------------------------------------------------------------
  Port     PVID           Port     PVID           Port     PVID
  ==============          ==============          ==============
   1       1               10      1               19      1
   2       1               11      1               20      1
   3       1               12      1               21      4094
   4       1               13      1               22      4094
   5       1               14      1               23      4094
   6       1               15      1               24      4094
   7       1               16      1               25      1
   8       1               17      1               26      1
   9       1               18      1



*******************************************************************************
Function:Input port number.
Message:
CTRL+T = Root screen            Esc=Prev. screen              CTRL+R = Refresh
```

3. Type the range of port numbers you want to configure in the **Configure Port** field.
4. Type the PVID for the VLAN member ports you want to configure in the **PVID** field.

   Port VLAN Identifier (PVID) is a classification mechanism that associates a port with a specific VLAN and is used to make forwarding decisions for untagged packets received by the port. For example, if Port 2 is assigned a PVID of 3, then all untagged packets received on Port 2 will be assigned to VLAN 3. This number is generally the same as the VID# number assigned to the port in the **802.1Q Static VLAN Settings** screen.
5. Highlight **APPLY.**
6. Press the **Enter** key.

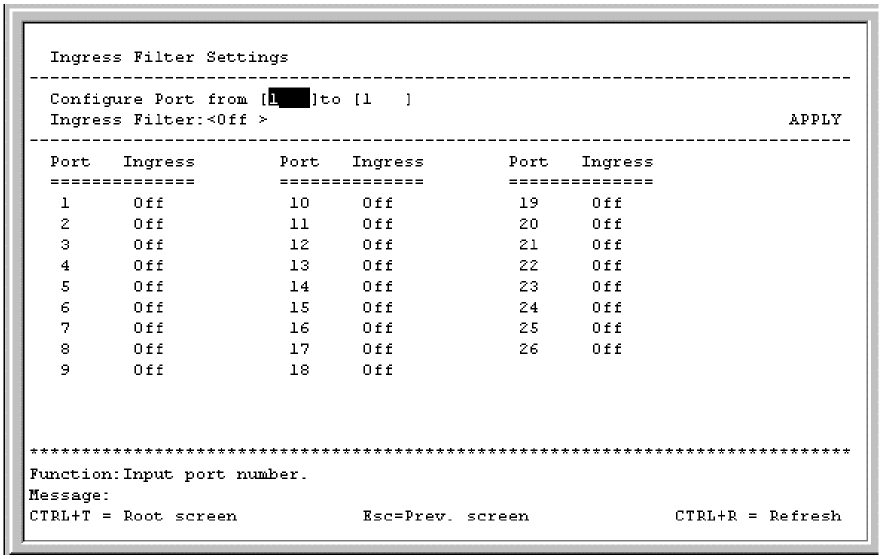
NOTE: To save the configuration settings permanently, you must enter them into NVRAM using the **Save Changes** option on the main menu. See the “Saving Changes” section earlier in this chapter.

Configuring Port Ingress Filtering

To set ingress filtering on a port:

1. Highlight **Configure Port Ingress Filter** on the **IEEE 802.1Q VLANs Configuration** menu.

2. Press the **Enter** key. The following screen is displayed.



```
  Ingress Filter Settings
-------------------------------------------------------------------------------
  Configure Port from [1   ]to [1   ]
  Ingress Filter:<Off >                                                   APPLY
-------------------------------------------------------------------------------
  Port   Ingress        Port   Ingress        Port   Ingress
  ==============        ==============        ==============
   1      Off            10     Off            19     Off
   2      Off            11     Off            20     Off
   3      Off            12     Off            21     Off
   4      Off            13     Off            22     Off
   5      Off            14     Off            23     Off
   6      Off            15     Off            24     Off
   7      Off            16     Off            25     Off
   8      Off            17     Off            26     Off
   9      Off            18     Off



*******************************************************************************
Function:Input port number.
Message:
CTRL+T = Root screen            Esc=Prev. screen             CTRL+R = Refresh
```

3. Type the range of port numbers you want to configure in the **Configure Port** field.
4. Toggle between **On** and **Off** in the **Ingress Filter** field.

   An ingress filter enables the port to compare the VID tag of an incoming packet with the PVID number assigned to the port. If the two are different, the port filters (drops) the packet.
5. Highlight **APPLY.**
6. Press the **Enter** key.

NOTE: To save the configuration settings permanently, you must enter them into NVRAM using the **Save Changes** option on the main menu. See the “Saving Changes” section earlier in this chapter.

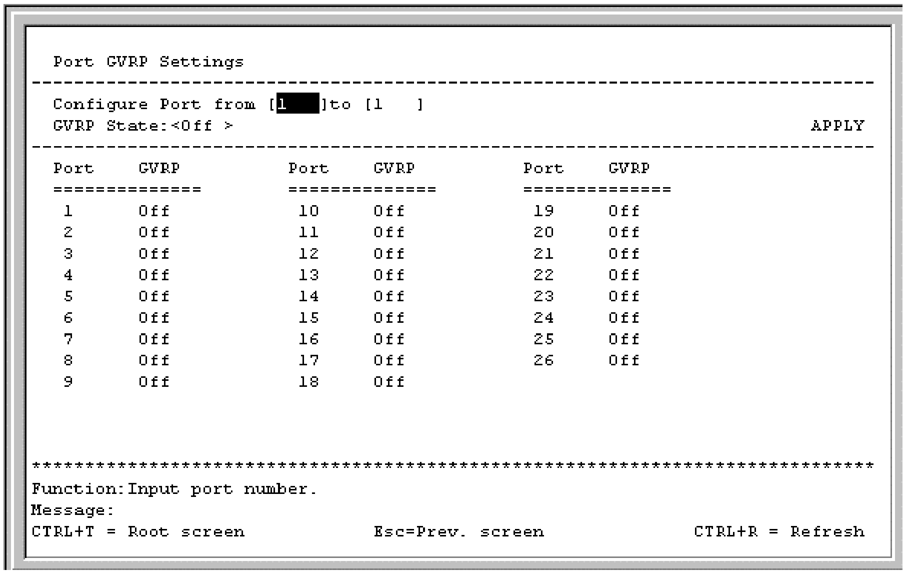
Configuring Port GVRP Settings

GARP VLAN Registration Protocol (GVRP) is a Generic Attribute Registration Protocol (GARP) application that provides 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports. With GVRP, the switch module can exchange VLAN configuration information with other GVRP switches, prune unnecessary broadcast and unknown unicast traffic, and dynamically create and manage VLANs on switches connected through 802.1Q trunk ports.

To enable a port to dynamically become a member of a VLAN:

1. Highlight **Configure Port GVRP Settings** on the **IEEE 802.1Q VLANs Configuration** menu.

2. Press the **Enter** key. The following screen is displayed.



```
  Port GVRP Settings
-------------------------------------------------------------------------------
  Configure Port from [1   ]to [1   ]
  GVRP State:<Off >                                                      APPLY
-------------------------------------------------------------------------------
  Port    GVRP          Port    GVRP          Port    GVRP
  =============         =============         =============
   1      Off            10     Off            19     Off
   2      Off            11     Off            20     Off
   3      Off            12     Off            21     Off
   4      Off            13     Off            22     Off
   5      Off            14     Off            23     Off
   6      Off            15     Off            24     Off
   7      Off            16     Off            25     Off
   8      Off            17     Off            26     Off
   9      Off            18     Off



*******************************************************************************
Function:Input port number.
Message:
CTRL+T = Root screen            Esc=Prev. screen              CTRL+R = Refresh
```

This screen allows you to enable or disable GARP VLAN Registration Protocol (GVRP).

1. Type the range of ports to be configured in the **Configure Port** fields.
2. Toggle the **GVRP State** to **On.**
3. Highlight **APPLY.**
4. Press the **Enter** key.

NOTE: To save the configuration settings permanently, you must enter them into NVRAM using the **Save Changes** option on the main menu. See the “Saving Changes” section earlier in this chapter.

GVRP updates dynamic VLAN registration entries and communicates the new VLAN information across the network. This feature allows stations to physically move to other switch module ports and keep their original VLAN settings, without having to reconfigure.

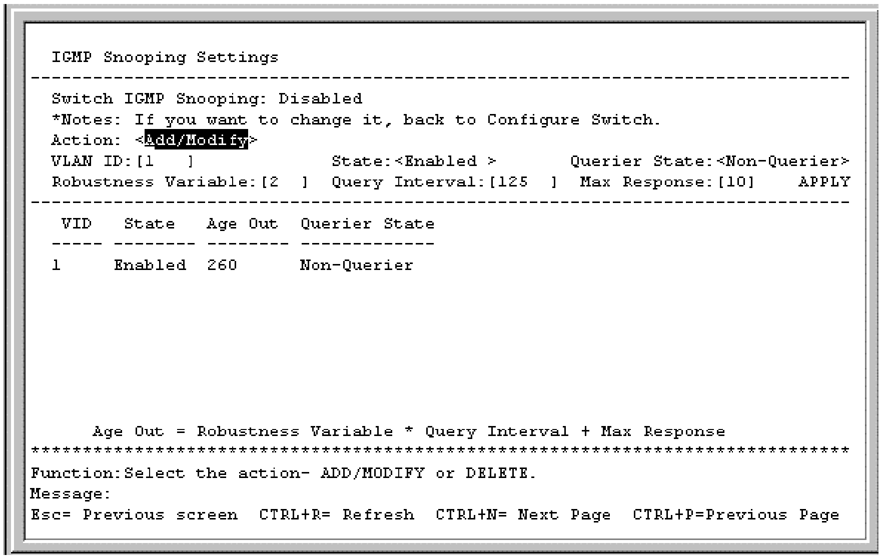
Configuring IGMP Snooping

Internet Group Management Protocol (IGMP) Snooping allows the switch module to recognize IGMP queries and reports sent between network stations or devices and an IGMP host. When enabled for IGMP Snooping, the switch module can open or close a port to a specific device based on IGMP messages passing through the switch module.

To configure IGMP Snooping:

1. Highlight **Configure IGMP Snooping** on the **Configuration** menu.

2. Press the **Enter** key. The following screen is displayed.



```
  IGMP Snooping Settings
-------------------------------------------------------------------------------
  Switch IGMP Snooping: Disabled
  *Notes: If you want to change it, back to Configure Switch.
  Action: <Add/Modify>
  VLAN ID:[1   ]            State:<Enabled >       Querier State:<Non-Querier>
  Robustness Variable:[2  ]  Query Interval:[125  ]  Max Response:[10]    APPLY
-------------------------------------------------------------------------------
   VID   State    Age Out  Querier State
  ----- -------- -------- -------------
  1     Enabled  260      Non-Querier







      Age Out = Robustness Variable * Query Interval + Max Response
*******************************************************************************
Function:Select the action- ADD/MODIFY or DELETE.
Message:
Esc= Previous screen  CTRL+R= Refresh  CTRL+N= Next Page  CTRL+P=Previous Page
```

The user-changeable parameters in the switch module are:

— **Switch IGMP Snooping**—Toggle using the space bar between **Disabled** and **Enabled.** This setting is used to enable or disable IGMP Snooping globally on the switch module.

— **Action**—Toggle to the option you want, **Add/Modify** or **Delete.**

— **Querier State**—Toggle between **Non-Querier, V1-Querier,** and **V2-Querier.** This setting is used to specify the IGMP version (1 or 2) that is used by the IGMP interface when making queries.

— **Robustness Variable**—This option is a tuning variable to allow for subnetworks that are expected to lose a large number of packets. A value between 2 and 255 can be entered, with larger values being specified for subnetworks that are expected to lose larger numbers of packets.

— **Query Interval**—You can enter a value between 1 and 65,500 seconds, with a default of 125 seconds. This setting specifies the length of time between sending IGMP queries.

— **Max Response**—Set the maximum amount of time allowed before sending an IGMP response report. A value between 1 and 25 seconds can be entered; the default is 10 seconds.

3. After making your changes, highlight **APPLY**, then press the **Enter** key.

NOTE: To save the configuration settings permanently, you must enter them into NVRAM using the **Save Changes** option on the main menu. See the “Saving Changes” section earlier in this chapter.

Configuring Port Trunking

Port trunking allows several ports to be grouped together to act as a single link. This setting provides a bandwidth that is a multiple of a single link bandwidth. Port trunking is most commonly used to link a bandwidth-intensive network device or devices—such as a server—to the backbone of a network.

The switch module allows the creation of up to six port trunking groups, each group consisting of up to eight links (ports). The trunked ports must be contiguous (they must have sequential port numbers). All of the ports in the group must be members of the same VLAN. Further, the trunked ports must all be of the same speed and should be configured as full-duplex.

The configuration of the lowest numbered port in the group becomes the configuration for all of the ports in the aggregation group. This port is called the Master Port of the group, and all configuration options, including the VLAN configuration, that can be applied to the Master Port are applied to the entire port trunking group.

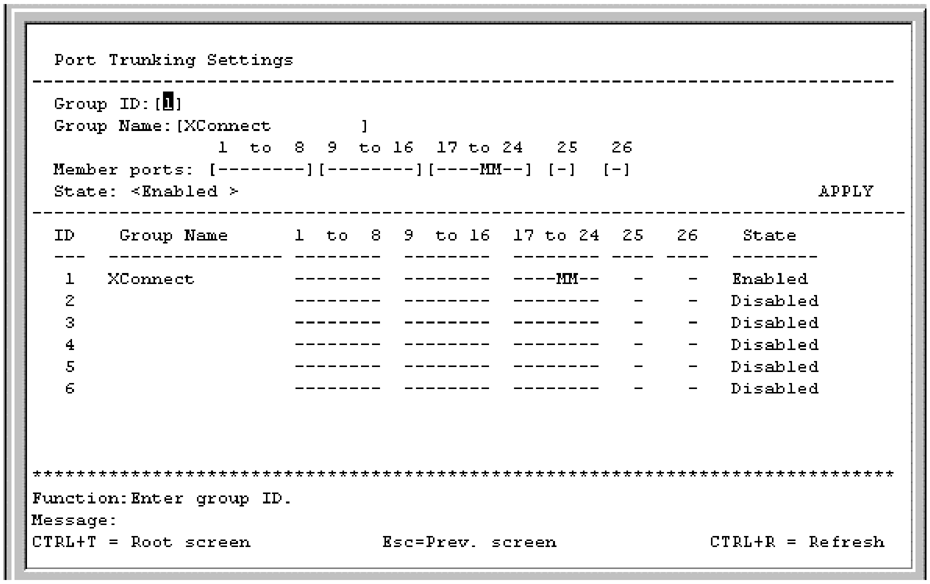
Load balancing is automatically applied to the ports in the trunked group, and a link failure within the group causes the network traffic to be directed to the remaining links in the group.

The Spanning Tree Protocol treats a port trunking group as a single link on the switch module level. On the port level, the STP uses the port parameters of the Master Port in the calculation of port cost and in determining the state of the port trunking group. If two redundant port trunking groups are configured on the switch module, STP blocks one entire group—in the same way STP blocks a single port that has a redundant link.

To configure a port trunking group:

1. Highlight **Configure Port Trunking** on the **Configuration** menu.

2. Press the **Enter** key. The following screen is displayed.



```
  Port Trunking Settings
-------------------------------------------------------------------------------
  Group ID:[1]
  Group Name:[XConnect        ]
                1  to  8  9  to 16  17 to 24   25   26
  Member ports: [--------][--------][----MM--] [-]  [-]
  State: <Enabled >                                                   APPLY
--------------------------------------------------------------------------------
  ID    Group Name      1  to  8  9  to 16  17 to 24  25   26    State
  ---  ---------------- --------  --------  -------- ---- ----  --------
   1   XConnect         --------  --------  ----MM--   -    -   Enabled
   2                    --------  --------  --------   -    -   Disabled
   3                    --------  --------  --------   -    -   Disabled
   4                    --------  --------  --------   -    -   Disabled
   5                    --------  --------  --------   -    -   Disabled
   6                    --------  --------  --------   -    -   Disabled



*******************************************************************************
Function:Enter group ID.
Message:
CTRL+T = Root screen          Esc=Prev. screen            CTRL+R = Refresh
```

The user-changeable parameters in the switch module are as follows:

- **Group ID**—This field is for a group ID number for the port trunking group.
- **Group Name**—Enter a name for the port trunking group.
- **Member ports**—Toggle between **M** to indicate membership of the port trunking group, or a dash (**—**) to indicate nonmembership.
- **State**—Toggle between **Enabled** and **Disabled.** This setting is used to turn a port trunking group on or off. It is useful for diagnostics, to quickly isolate a bandwidth intensive network device or to have an absolute backup aggregation group that is not under automatic control.

3. After making your changes, highlight **APPLY,** then press the **Enter** key.

NOTE: To save the configuration settings permanently, you must enter them into NVRAM using the **Save Changes** option on the main menu. See the “Saving Changes” section earlier in this chapter.

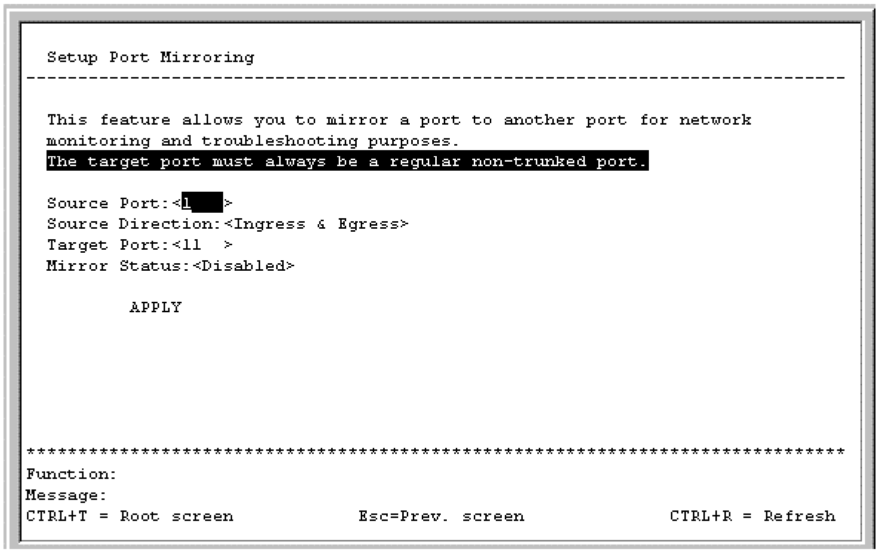
Configuring Port Mirroring

The switch module allows you to copy frames transmitted and received on a port and redirect the copies to another port. You can attach a monitoring device to the mirrored port, such as a sniffer or an RMON probe, to view details about the packets passing through the first port. This setting is useful for network monitoring and troubleshooting purposes.

NOTE: You cannot mirror a fast port onto a slower port. For example, if you try to mirror the traffic from a 100-Mb/s port onto a 10-Mb/s port, you can cause throughput problems. The port from which you are copying frames should always support an equal or lower speed than the port to which you are sending the copies. Also, the target port cannot be a member of a trunk group.

To configure port mirroring:

1. Highlight **Configure Port Mirroring** on the **Configuration** menu.
2. Press the **Enter** key. The following screen is displayed.



```
  Setup Port Mirroring
--------------------------------------------------------------------------------

  This feature allows you to mirror a port to another port for network
  monitoring and troubleshooting purposes.
  The target port must always be a regular non-trunked port.

  Source Port:<1    >
  Source Direction:<Ingress & Egress>
  Target Port:<11  >
  Mirror Status:<Disabled>

          APPLY







********************************************************************************
Function:
Message:
CTRL+T = Root screen            Esc=Prev. screen             CTRL+R = Refresh
```

3. Toggle to the number of the port from which you want to copy frames in the **Source Port** field.
4. Toggle to the desired source direction in the **Source Direction** field.
5. Toggle to the port that receives the copies from the source port in the **Target Port** field. The target port is where you connect a monitoring/troubleshooting device, such as a sniffer or an RMON probe.
6. Toggle the **Mirror Status** field to **Enabled.**
7. Highlight **APPLY.**
8. Press the **Enter** key.

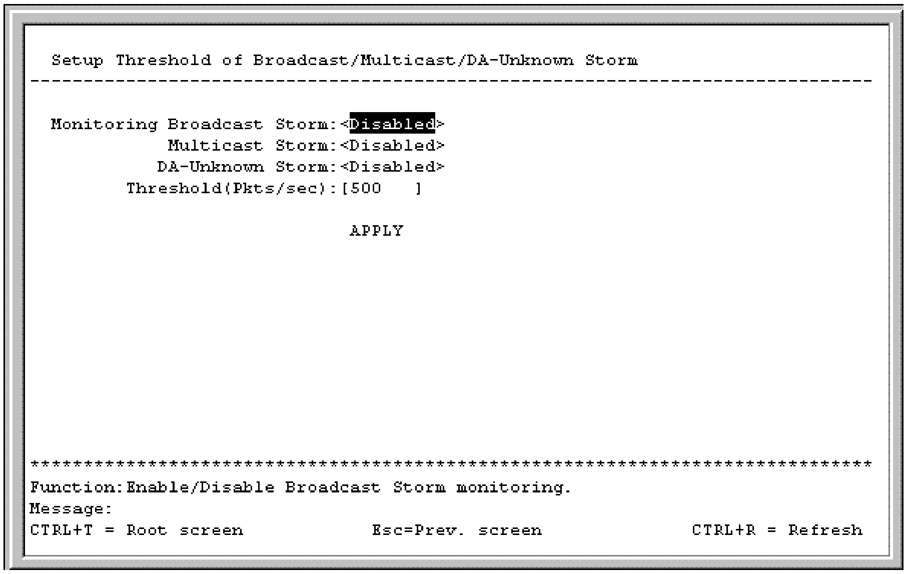
NOTE: To save the configuration settings permanently, you must enter them into NVRAM using the **Save Changes** option on the main menu. See the “Saving Changes” section earlier in this chapter.

Configuring the Threshold of Broadcast/Multicast/DA-Unknown Storm

To configure the threshold of a broadcast, multicast, or DA-Unknown Storm:

1. Highlight **Configure Threshold of Broadcast/Multicast/DA-Unknown Storm** on the **Configuration** menu.

2. Press the **Enter** key. The following screen is displayed.



```
  Setup Threshold of Broadcast/Multicast/DA-Unknown Storm
-------------------------------------------------------------------------------

  Monitoring Broadcast Storm:<Disabled>
             Multicast Storm:<Disabled>
            DA-Unknown Storm:<Disabled>
         Threshold(Pkts/sec):[500   ]

                              APPLY

*******************************************************************************
Function:Enable/Disable Broadcast Storm monitoring.
Message:
CTRL+T = Root screen            Esc=Prev. screen             CTRL+R = Refresh
```

3. Toggle the option to **Enabled.**
4. Type a threshold in the **Threshold (Pkts/sec)** field.
5. Highlight **APPLY.**
6. Press the **Enter** key.

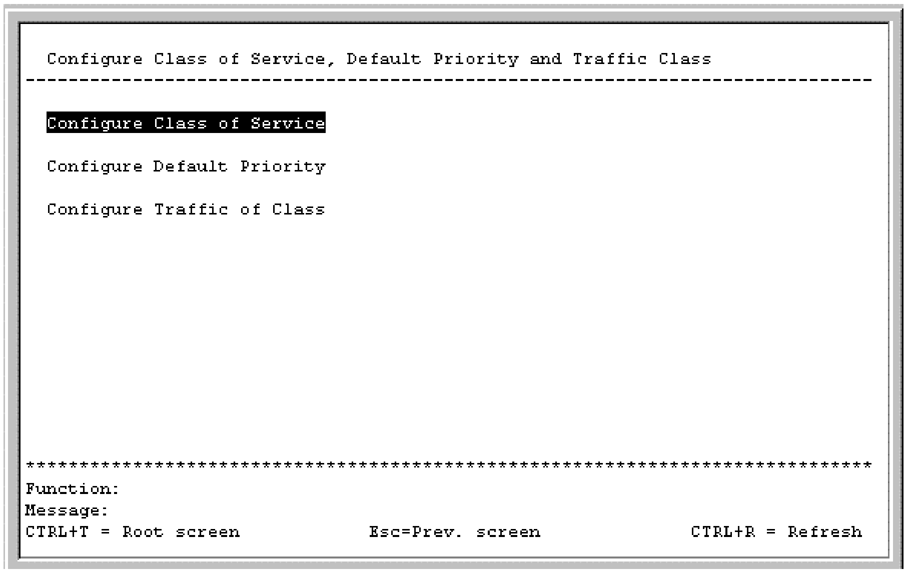
NOTE: To save the configuration settings permanently, you must enter them into NVRAM using the **Save Changes** option on the main menu. See the “Saving Changes” section earlier in this chapter.

Configuring Class of Service, Default Priority, and Traffic Class

To configure Class of Service, default priority, and traffic class:

1. Highlight **Configure Class of Service, Default Priority,** and **Traffic Class** on the **Configuration** menu.

2. Press the **Enter** key. The following screen is displayed.

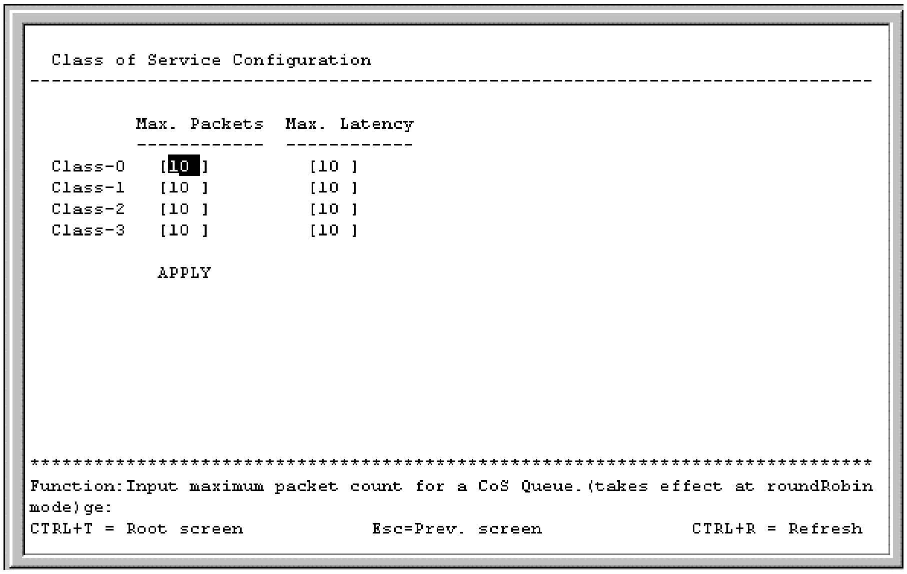


```
  Configure Class of Service, Default Priority and Traffic Class
-------------------------------------------------------------------------------

  Configure Class of Service

  Configure Default Priority

  Configure Traffic of Class











*******************************************************************************
Function:
Message:
CTRL+T = Root screen            Esc=Prev. screen             CTRL+R = Refresh
```

Configuring Class of Service

To configure Class of Service:

1. Highlight **Configure Class of Service** on the **Configure Class of Service, Default Priority,** and **Traffic Class** menu.
2. Press the **Enter** key. The following screen is displayed.



```
  Class of Service Configuration
-------------------------------------------------------------------------------


          Max. Packets  Max. Latency
          ------------  ------------
  Class-0   [10 ]         [10 ]
  Class-1   [10 ]         [10 ]
  Class-2   [10 ]         [10 ]
  Class-3   [10 ]         [10 ]

            APPLY









*******************************************************************************
Function:Input maximum packet count for a CoS Queue.(takes effect at roundRobin
mode)ge:
CTRL+T = Root screen            Esc=Prev. screen             CTRL+R = Refresh
```

This screen allows you to set the following features:

- **Max. Packets**—The Class of Service scheduling algorithm starts from the highest CoS for a given port, sends the maximum number of packets, then moves on to the next lower CoS. Values from 0 to 255 can be entered in this field. Entering zero instructs the switch module to continue processing packets until there are no more packets in the CoS transaction queue.
- **Max. Latency**—The maximum latency is the maximum allowable time a packet stays in the CoS queue. The packets in this queue are not delayed more than the amount entered in this field. The timer is disabled when this field is set to zero. Each unit of this timer is equal to 16µ.

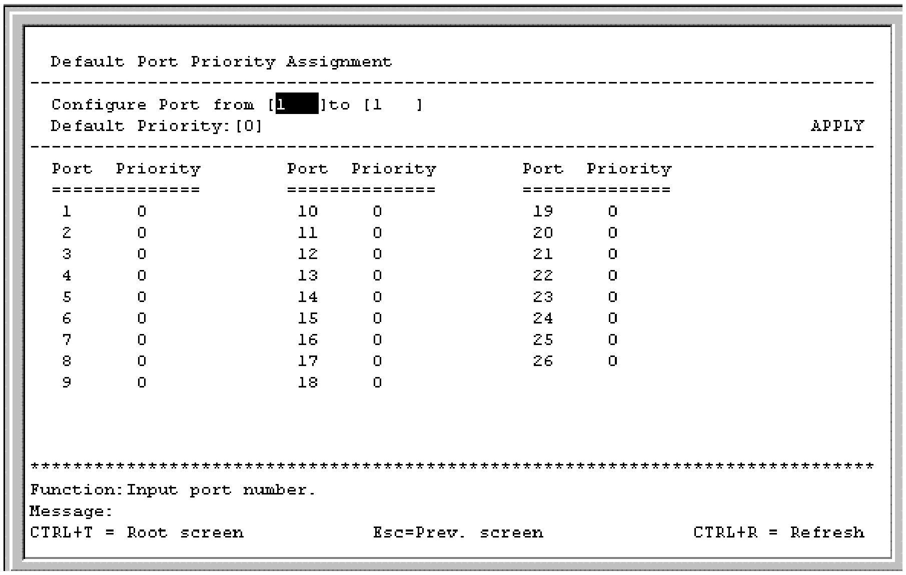
3. After making your changes, highlight **APPLY** and then press the **Enter** key.

NOTE: To save the configuration settings permanently, you must enter them into NVRAM using the **Save Changes** option on the main menu. See the “Saving Changes” section earlier in this chapter.

Assigning Port Default Priority

To assign port default priority:

1. Highlight **Configure Default Priority** on the **Configure Class of Service, Default Priority,** and **Traffic Class** menu.
2. Press the **Enter** key. The following screen is displayed.



```
  Default Port Priority Assignment
-------------------------------------------------------------------------------
  Configure Port from [1   ]to [1   ]
  Default Priority:[0]                                                   APPLY
-------------------------------------------------------------------------------
  Port  Priority          Port  Priority          Port  Priority
  ==============          ==============          ==============
   1      0                10     0                19     0
   2      0                11     0                20     0
   3      0                12     0                21     0
   4      0                13     0                22     0
   5      0                14     0                23     0
   6      0                15     0                24     0
   7      0                16     0                25     0
   8      0                17     0                26     0
   9      0                18     0



*******************************************************************************
Function:Input port number.
Message:
CTRL+T = Root screen            Esc=Prev. screen              CTRL+R = Refresh
```

3. Type the port range in **Configure Port** field.

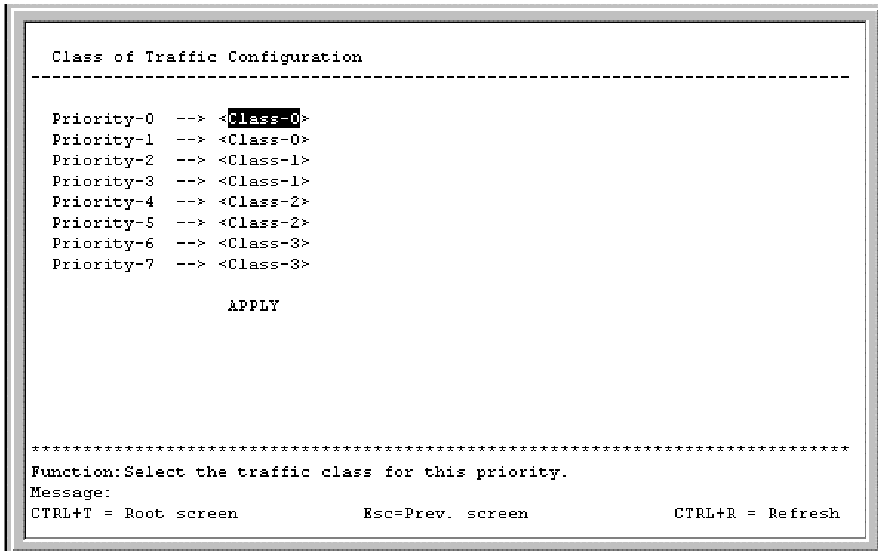
4. Highlight **APPLY.**
5. Press the **Enter** key.

NOTE: To save the configuration settings permanently, you must enter them into NVRAM using the **Save Changes** option on the main menu. See the "Saving Changes" section earlier in this chapter.

Configuring Class of Traffic

To configure traffic class:

1. Highlight **Configure Traffic of Class** on the **Configure Class of Service, Default Priority,** and **Traffic Class** menu.
2. Press the **Enter** key. The following screen is displayed.



```
  Class of Traffic Configuration
------------------------------------------------------------------------------

  Priority-0  --> <Class-0>
  Priority-1  --> <Class-0>
  Priority-2  --> <Class-1>
  Priority-3  --> <Class-1>
  Priority-4  --> <Class-2>
  Priority-5  --> <Class-2>
  Priority-6  --> <Class-3>
  Priority-7  --> <Class-3>

                 APPLY

******************************************************************************
Function:Select the traffic class for this priority.
Message:
CTRL+T = Root screen           Esc=Prev. screen            CTRL+R = Refresh
```

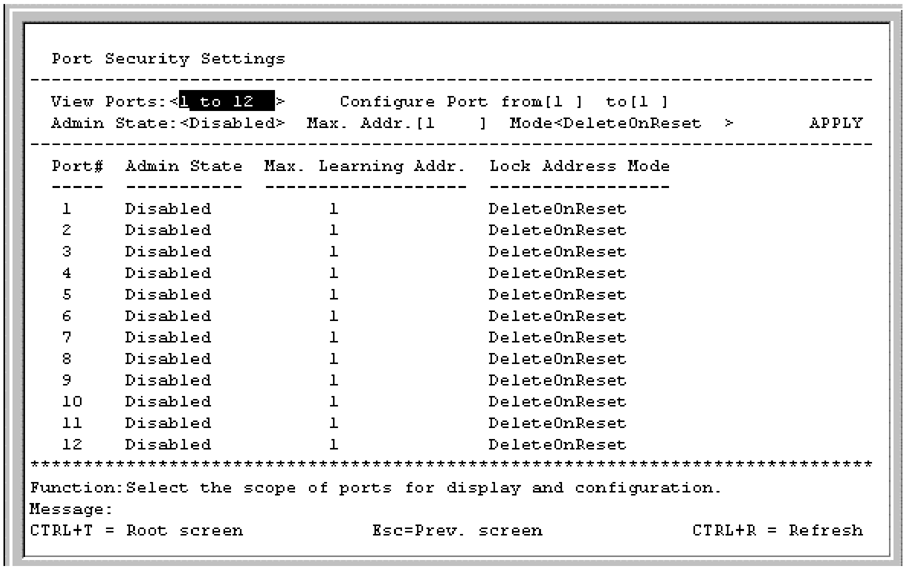
3. Toggle the **Priority** fields to set the traffic class for the eight levels of priority for the switch module. Class values are from 0 to 3.
4. Highlight **APPLY.**
5. Press the **Enter** key.

NOTE: To save the configuration settings permanently, you must enter them into NVRAM using the **Save Changes** option on the main menu. See the "Saving Changes" section earlier in this chapter.

Configuring Port Security

To configure security for a specified port or range of ports on the switch module:

1. Highlight **Configure Port Security** on the **Configuration** menu.
2. Press the **Enter** key. The following screen is displayed.



```
  Port Security Settings
--------------------------------------------------------------------------------
  View Ports:<1 to 12  >     Configure Port from[1 ]  to[1 ]
  Admin State:<Disabled>  Max. Addr.[1    ]  Mode<DeleteOnReset  >       APPLY
--------------------------------------------------------------------------------
  Port#  Admin State  Max. Learning Addr.  Lock Address Mode
  -----  -----------  -------------------  -----------------
   1     Disabled          1               DeleteOnReset
   2     Disabled          1               DeleteOnReset
   3     Disabled          1               DeleteOnReset
   4     Disabled          1               DeleteOnReset
   5     Disabled          1               DeleteOnReset
   6     Disabled          1               DeleteOnReset
   7     Disabled          1               DeleteOnReset
   8     Disabled          1               DeleteOnReset
   9     Disabled          1               DeleteOnReset
   10    Disabled          1               DeleteOnReset
   11    Disabled          1               DeleteOnReset
   12    Disabled          1               DeleteOnReset
********************************************************************************
Function:Select the scope of ports for display and configuration.
Message:
CTRL+T = Root screen           Esc=Prev. screen             CTRL+R = Refresh
```

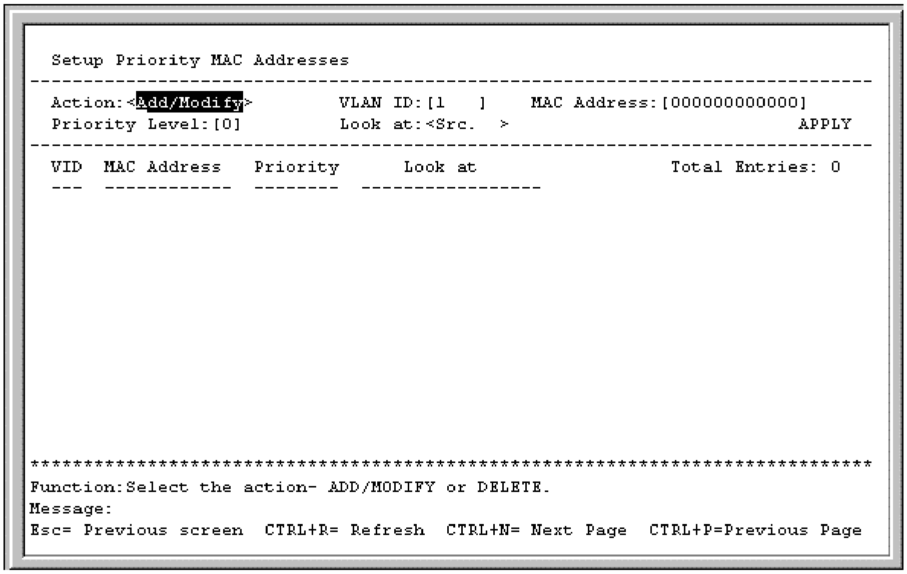
3. Toggle the **View Ports** field to the range that you want.
4. Type the port range in the **Configure Port** fields.
5. Toggle **Admin State** to **Enabled.**
6. Type the maximum number of addresses in the **Max. Addr.** field.
7. Toggle to the mode that you want in the **Mode** field.
8. Highlight **APPLY.**
9. Press the **Enter** key.

NOTE: To save the configuration settings permanently, you must enter them into NVRAM using the **Save Changes** option on the main menu. See the “Saving Changes” section earlier in this chapter.

Configuring Priority MAC Addresses

To configure priority MAC address for a specified port or range of ports on the switch module:

1. Highlight **Configure Priority MAC Addresses** on the **Configuration** menu.
2. Press the **Enter** key. The following screen is displayed.



```
  Setup Priority MAC Addresses
-------------------------------------------------------------------------------
  Action:<Add/Modify>        VLAN ID:[1   ]    MAC Address:[000000000000]
  Priority Level:[0]         Look at:<Src.  >                          APPLY
-------------------------------------------------------------------------------
  VID  MAC Address   Priority      Look at                   Total Entries: 0
  ---  ------------  --------  -----------------

*******************************************************************************
Function:Select the action- ADD/MODIFY or DELETE.
Message:
Esc= Previous screen  CTRL+R= Refresh  CTRL+N= Next Page  CTRL+P=Previous Page
```

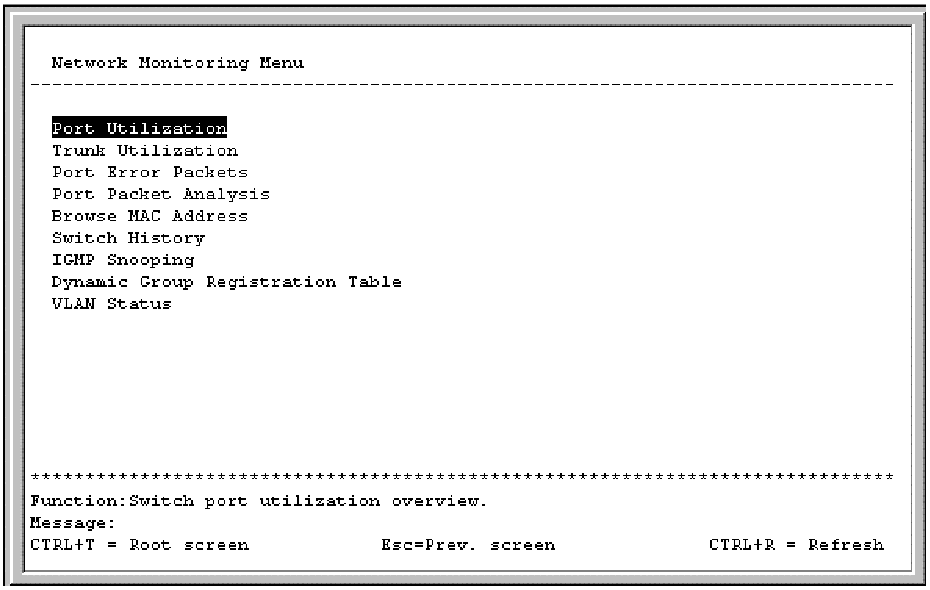
The **Setup Priority MAC Address** window allows you to set up the priority MAC address for each VLAN ID.

Monitoring Switch Module Functions

The switch module provides extensive network monitoring capabilities.

To display the network data compiled by the switch module:

1. Highlight **Network Monitoring** on the main menu.
2. Press the **Enter** key. The following screen is displayed.

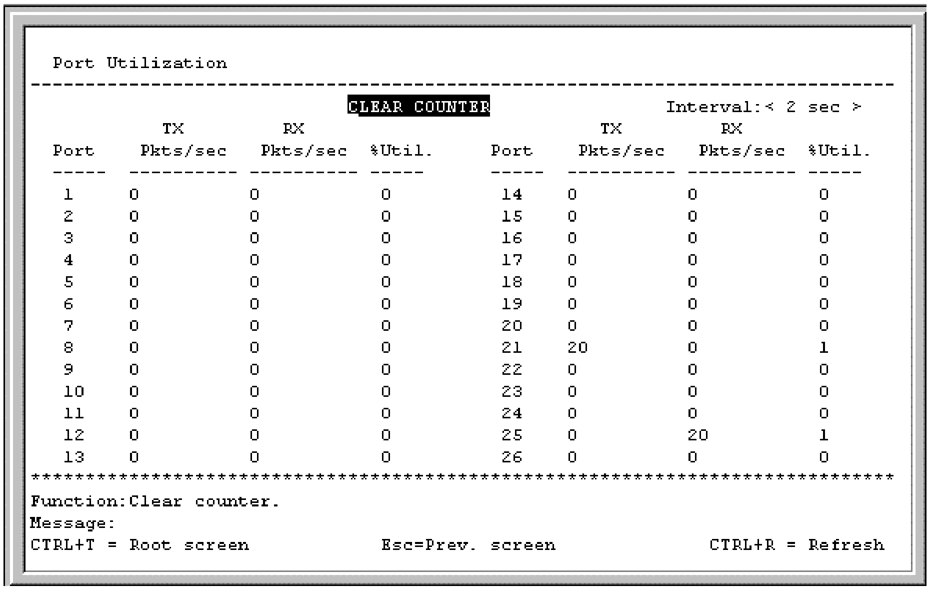


```
  Network Monitoring Menu
--------------------------------------------------------------------------------

  Port Utilization
  Trunk Utilization
  Port Error Packets
  Port Packet Analysis
  Browse MAC Address
  Switch History
  IGMP Snooping
  Dynamic Group Registration Table
  VLAN Status







********************************************************************************
Function:Switch port utilization overview.
Message:
CTRL+T = Root screen           Esc=Prev. screen             CTRL+R = Refresh
```

Monitoring Port Utilization

To view the port utilization of all the ports on the switch module:

1. Highlight **Port Utilization** on the **Network Monitoring** menu.
2. Press the **Enter** key. The following screen is displayed.



```
  Port Utilization
--------------------------------------------------------------------------------
                             CLEAR COUNTER                  Interval:< 2 sec >
            TX         RX                            TX         RX
  Port    Pkts/sec   Pkts/sec  %Util.      Port    Pkts/sec   Pkts/sec  %Util.
  -----  ---------- ---------- -----       -----  ---------- ---------- -----
   1     0          0           0           14    0          0           0
   2     0          0           0           15    0          0           0
   3     0          0           0           16    0          0           0
   4     0          0           0           17    0          0           0
   5     0          0           0           18    0          0           0
   6     0          0           0           19    0          0           0
   7     0          0           0           20    0          0           0
   8     0          0           0           21    20         0           1
   9     0          0           0           22    0          0           0
   10    0          0           0           23    0          0           0
   11    0          0           0           24    0          0           0
   12    0          0           0           25    0          20          1
   13    0          0           0           26    0          0           0
********************************************************************************
Function:Clear counter.
Message:
CTRL+T = Root screen            Esc=Prev. screen               CTRL+R = Refresh
```

The **Port Utilization** screen shows the number of packets transmitted and received per second and calculates the percentage of the total available bandwidth being used on the port (displayed under **%Util.**).

To reset the counters:

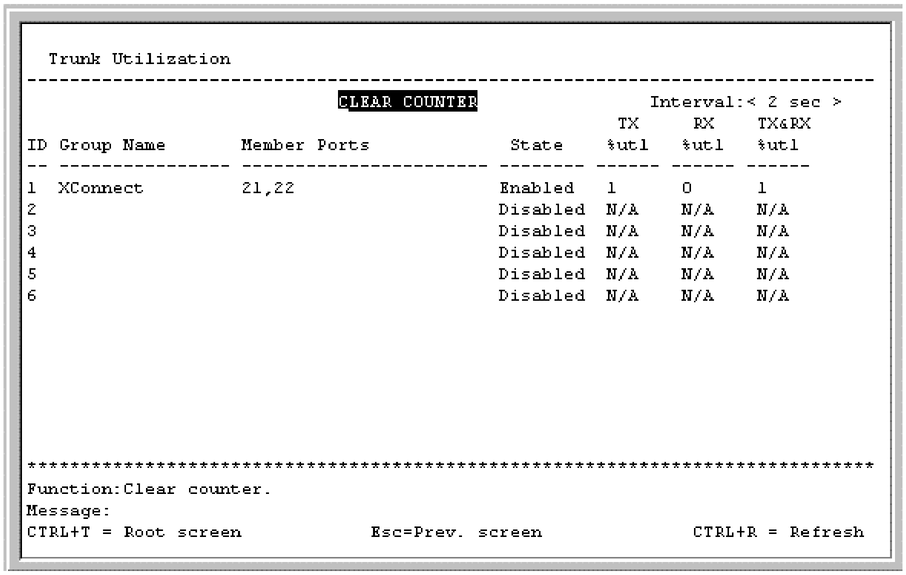
1. Highlight **CLEAR COUNTER.**
2. Press the **Enter** key.

Monitoring Trunk Utilization

To view the trunk utilization of all the ports on the switch module:

1. Highlight **Trunk Utilization** on the **Network Monitoring** menu.

2. Press the **Enter** key. The following screen is displayed.



```
  Trunk Utilization
-------------------------------------------------------------------------------
                             CLEAR COUNTER              Interval:< 2 sec >
                                                    TX     RX     TX&RX
ID Group Name       Member Ports             State    %utl   %utl   %utl
-- ---------------- ----------------------- -------- ------ ------ ------
1  XConnect         21,22                   Enabled  1      0      1
2                                           Disabled N/A    N/A    N/A
3                                           Disabled N/A    N/A    N/A
4                                           Disabled N/A    N/A    N/A
5                                           Disabled N/A    N/A    N/A
6                                           Disabled N/A    N/A    N/A









*******************************************************************************
Function:Clear counter.
Message:
CTRL+T = Root screen          Esc=Prev. screen             CTRL+R = Refresh
```

The **Trunk Utilization** window allows you to view three items for an individual port trunking group: the percentage of total available bandwidth being utilized by the group, the percentage of packets transmitted, and the percentage of packets being received per second.

To reset the counters:

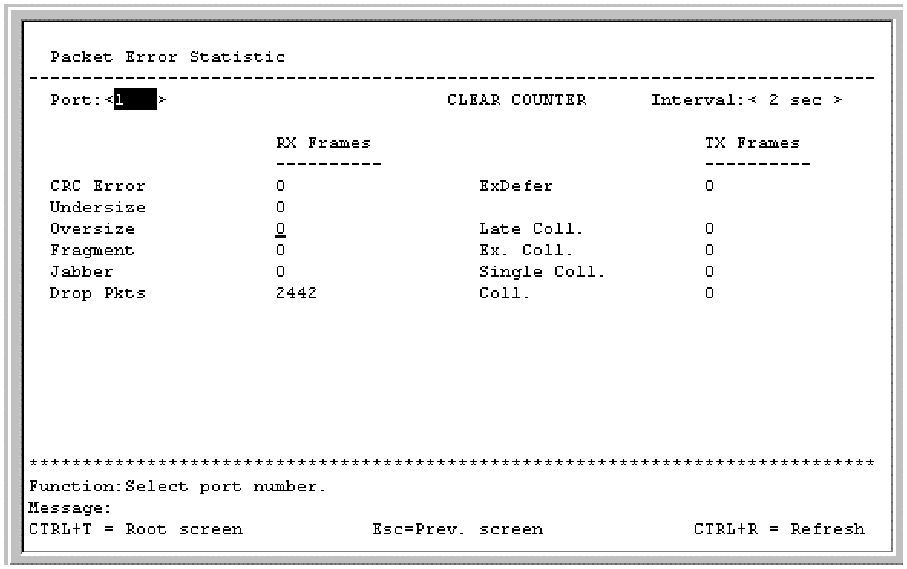
1. Highlight **CLEAR COUNTER.**
2. Press the **Enter** key.

Monitoring Port Error Packets

To view the error statistics for a port:

1. Highlight **Port Error Packets** on the **Network Monitoring** menu.

2. Press the **Enter** key. The following screen is displayed.



```
  Packet Error Statistic
--------------------------------------------------------------------------------
  Port:<1   >                          CLEAR COUNTER      Interval:< 2 sec >

                       RX Frames                               TX Frames
                       ----------                              ----------
  CRC Error            0                  ExDefer              0
  Undersize            0
  Oversize             0                  Late Coll.           0
  Fragment             0                  Ex. Coll.            0
  Jabber               0                  Single Coll.         0
  Drop Pkts            2442               Coll.                0







********************************************************************************
Function:Select port number.
Message:
CTRL+T = Root screen            Esc=Prev. screen              CTRL+R = Refresh
```

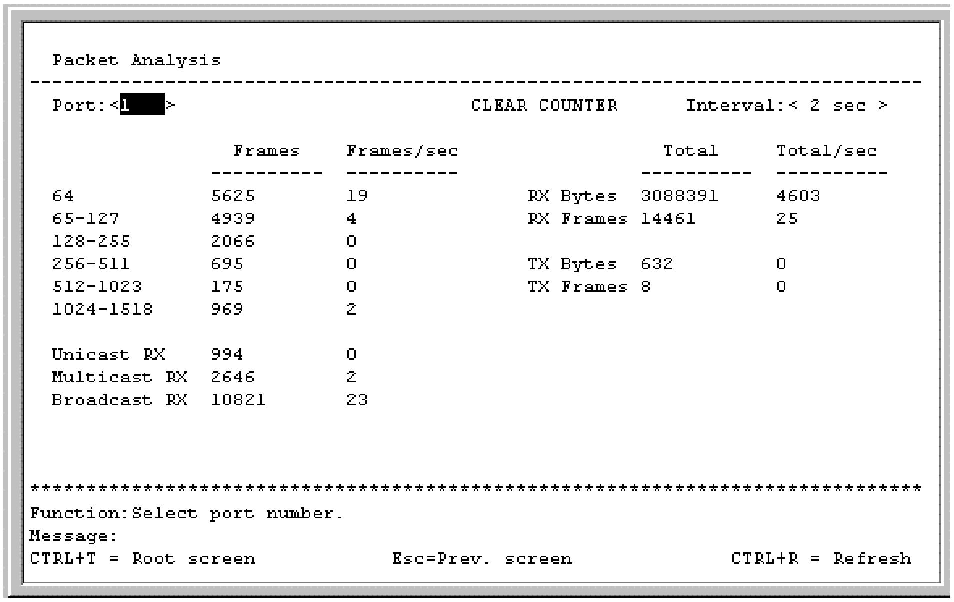
3. Toggle the **Port** field to the number of the port to be viewed.
4. Toggle the **Interval** field from 2 seconds to 1 minute, or select **Suspend,** to set the interval at which the error statistics are updated.
5. Highlight **CLEAR COUNTER.**
6. Press the **Enter** key to reset the counters.

Monitoring Port Packet Analysis

To view an analysis of the size of packets received or transmitted by a port:

1. Highlight **Port Packet Analysis** on the **Network Monitoring** menu.

2. Press the **Enter** key. The following screen is displayed.



```
  Packet Analysis
--------------------------------------------------------------------------------
  Port:<1   >                                CLEAR COUNTER      Interval:< 2 sec >

                  Frames    Frames/sec                 Total      Total/sec
                ----------  ----------              ----------  ----------
  64              5625        19             RX Bytes  3088391     4603
  65-127          4939        4              RX Frames 14461       25
  128-255         2066        0
  256-511         695         0              TX Bytes  632         0
  512-1023        175         0              TX Frames 8           0
  1024-1518       969         2

  Unicast RX      994         0
  Multicast RX    2646        2
  Broadcast RX    10821       23



********************************************************************************
Function:Select port number.
Message:
CTRL+T = Root screen            Esc=Prev. screen             CTRL+R = Refresh
```

In addition to the size of packets received or transmitted by the selected port, statistics on the number of unicast, multicast, and broadcast packets are displayed.

To reset the counters:

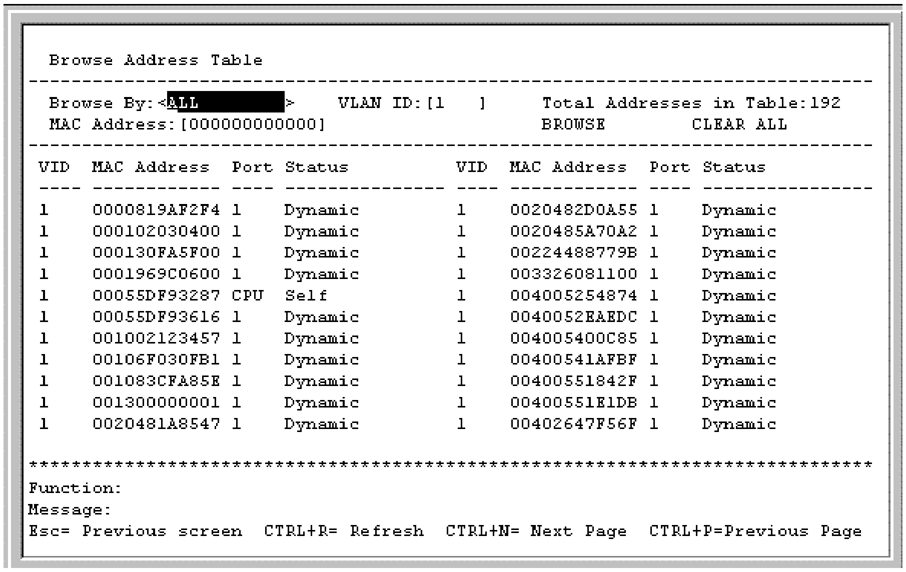
1. Highlight **CLEAR COUNTER.**
2. Press the **Enter** key.

Monitoring MAC Address Forwarding Table

To view the MAC address forwarding table:

1. Highlight **Browse MAC Address** on the **Network Monitoring** menu.

2. Press the **Enter** key. The following screen is displayed.



```
  Browse Address Table
-------------------------------------------------------------------------------
  Browse By:<ALL        >    VLAN ID:[1    ]     Total Addresses in Table:192
  MAC Address:[000000000000]                     BROWSE        CLEAR ALL
-------------------------------------------------------------------------------
 VID  MAC Address  Port Status          VID  MAC Address  Port Status
 ---- ------------ ---- --------------- ---- ------------ ---- ----------------
 1    0000819AF2F4 1    Dynamic         1    0020482D0A55 1    Dynamic
 1    000102030400 1    Dynamic         1    0020485A70A2 1    Dynamic
 1    000130FA5F00 1    Dynamic         1    00224488779B 1    Dynamic
 1    0001969C0600 1    Dynamic         1    003326081100 1    Dynamic
 1    00055DF93287 CPU  Self            1    004005254874 1    Dynamic
 1    00055DF93616 1    Dynamic         1    0040052EAEDC 1    Dynamic
 1    001002123457 1    Dynamic         1    004005400C85 1    Dynamic
 1    00106F030FB1 1    Dynamic         1    00400541AFBF 1    Dynamic
 1    001083CFA85E 1    Dynamic         1    00400551842F 1    Dynamic
 1    001300000001 1    Dynamic         1    00400551E1DB 1    Dynamic
 1    0020481A8547 1    Dynamic         1    00402647F56F 1    Dynamic

*******************************************************************************
Function:
Message:
Esc= Previous screen  CTRL+R= Refresh  CTRL+N= Next Page  CTRL+P=Previous Page
```

3. Toggle the **Browse By** field between **ALL, MAC Address, Port,** and **VLAN.** This option sets a filter to determine which MAC addresses from the forwarding table are displayed. ALL specifies no filter.

Searching for a Particular MAC Address

To search for a particular MAC address:

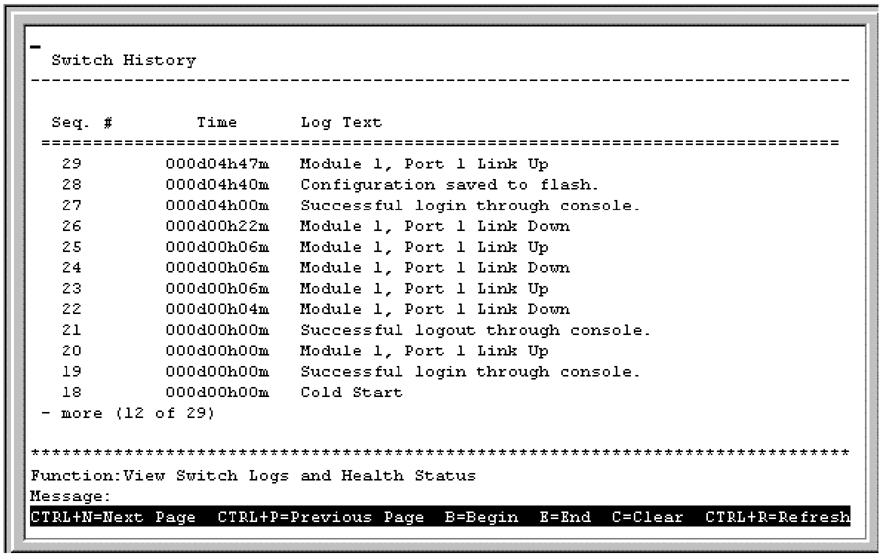
1. Toggle the **Browse By** field to MAC address. A **MAC Address** field is displayed.
2. Type the MAC address in the **MAC Address** field.
3. Press the **Enter** key.
4. Highlight **BROWSE**.
5. Press the **Enter** key to initiate the browsing action.
6. Highlight **CLEAR ALL.**
7. Press the **Enter** key to reset the table counters.

Monitoring Switch Module History

To view the **Switch Module History** log:

1. Highlight **Switch History** from the **Network Monitoring** menu.

2. Press the **Enter** key. The following screen is displayed.



```
  Switch History
--------------------------------------------------------------------------------

  Seq. #        Time      Log Text
 ==============================================================================
   29        000d04h47m   Module 1, Port 1 Link Up
   28        000d04h40m   Configuration saved to flash.
   27        000d04h00m   Successful login through console.
   26        000d00h22m   Module 1, Port 1 Link Down
   25        000d00h06m   Module 1, Port 1 Link Up
   24        000d00h06m   Module 1, Port 1 Link Down
   23        000d00h06m   Module 1, Port 1 Link Up
   22        000d00h04m   Module 1, Port 1 Link Down
   21        000d00h00m   Successful logout through console.
   20        000d00h00m   Module 1, Port 1 Link Up
   19        000d00h00m   Successful login through console.
   18        000d00h00m   Cold Start
 - more (12 of 29)

********************************************************************************
Function:View Switch Logs and Health Status
Message:
CTRL+N=Next Page  CTRL+P=Previous Page  B=Begin  E=End  C=Clear  CTRL+R=Refresh
```

The **Switch History** screen displays the switch module logs and health status.

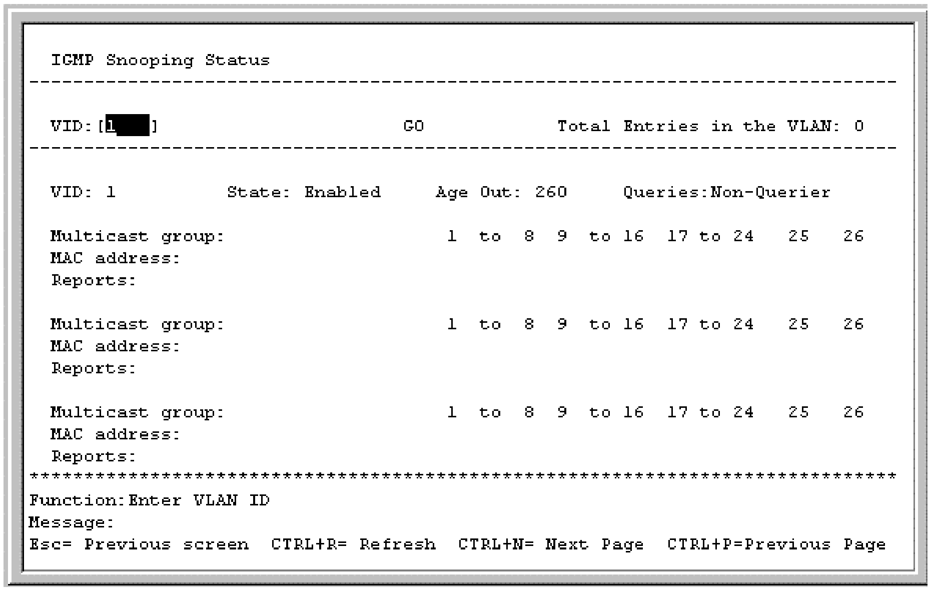
Monitoring IGMP Snooping

IGMP Snooping allows the switch module to read the Multicast Group IP address and the corresponding MAC address from IGMP packets that pass through the switch module. The ports where the IGMP packets were snooped are displayed and signified with an “M.” The number of IGMP reports that were snooped is also displayed in the **Reports** field.

To view the IGMP Snooping table:

1. Highlight **IGMP Snooping** on the **Network Monitoring** menu.

2. Press the **Enter** key. The following screen is displayed.



```
  IGMP Snooping Status
-------------------------------------------------------------------------------

  VID:[1   ]                        GO            Total Entries in the VLAN: 0
-------------------------------------------------------------------------------

  VID: 1          State: Enabled     Age Out: 260     Queries:Non-Querier

  Multicast group:                   1  to  8  9  to 16  17 to 24   25   26
  MAC address:
  Reports:

  Multicast group:                   1  to  8  9  to 16  17 to 24   25   26
  MAC address:
  Reports:

  Multicast group:                   1  to  8  9  to 16  17 to 24   25   26
  MAC address:
  Reports:
*******************************************************************************
Function:Enter VLAN ID
Message:
Esc= Previous screen  CTRL+R= Refresh  CTRL+N= Next Page  CTRL+P=Previous Page
```

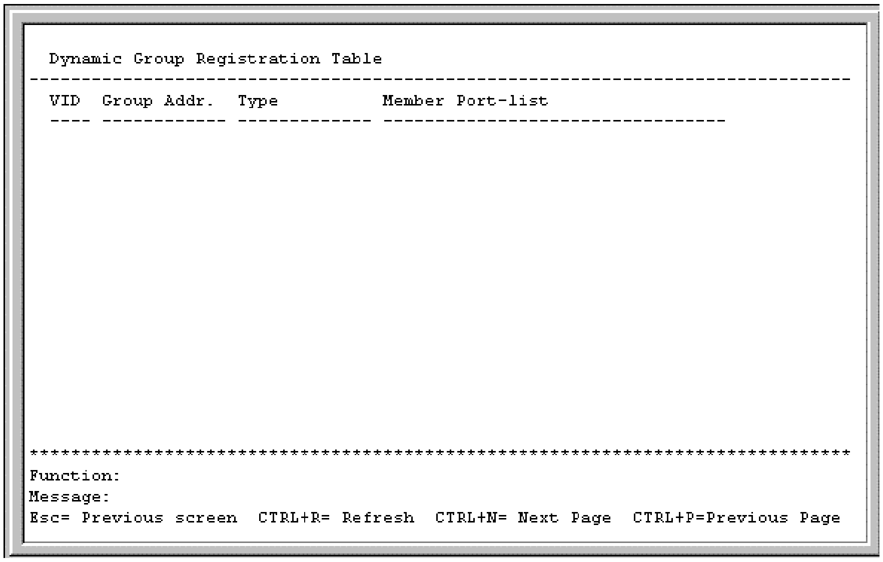
3. Type the VLAN name in the **VID** field.
4. Highlight **GO** to view the IGMP Snooping table.
5. Press the **Enter** key.

Monitoring the Dynamic Group Registration Table

To view the **Dynamic Group Registration Table:**

1. Highlight **Dynamic Group Registration Table** on the **Network Monitoring** menu.

2. Press the **Enter** key. The following screen is displayed.



```
  Dynamic Group Registration Table
--------------------------------------------------------------------------------
  VID  Group Addr.  Type          Member Port-list
  ---- ------------ ------------- ---------------------------------

*******************************************************************************
Function:
Message:
Esc= Previous screen  CTRL+R= Refresh  CTRL+N= Next Page  CTRL+P=Previous Page
```

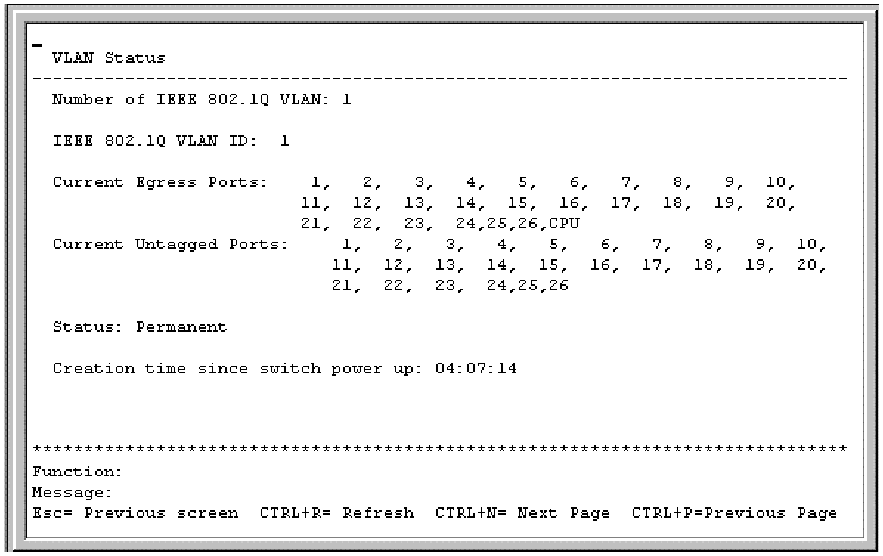
The **Dynamic Group Registration Table** displays filtering information for VLANs configured into the Bridge by local or network management, or learned dynamically. It specifies the set of ports to which frames received on a VLAN for this forwarding database (FDB) and containing a specific group destination address are allowed to be forwarded.

Monitoring VLAN Status

To view the **VLAN Status table:**

1. Highlight **VLAN Status** on the **Network Monitoring** menu.

2. Press the **Enter** key. The following screen is displayed.



```
_
  VLAN Status
-------------------------------------------------------------------------------
  Number of IEEE 802.1Q VLAN: 1

  IEEE 802.1Q VLAN ID:  1

  Current Egress Ports:     1,   2,   3,   4,   5,   6,   7,   8,   9,  10,
                           11,  12,  13,  14,  15,  16,  17,  18,  19,  20,
                           21,  22,  23,  24,25,26,CPU
  Current Untagged Ports:     1,   2,   3,   4,   5,   6,   7,   8,   9,  10,
                             11,  12,  13,  14,  15,  16,  17,  18,  19,  20,
                             21,  22,  23,  24,25,26

  Status: Permanent

  Creation time since switch power up: 04:07:14



*******************************************************************************
Function:
Message:
Esc= Previous screen  CTRL+R= Refresh  CTRL+N= Next Page  CTRL+P=Previous Page
```

The **VLAN Status** window displays which VLAN ports are egress and which ports are untagged.

Configuring SNMP Manager

The switch module sends out SNMP traps (alert messages) to network management stations whenever certain exceptional events occur, such as when the switch module is turned on or when a system reset occurs. The switch module allows traps to be routed to up to four different network management hosts.

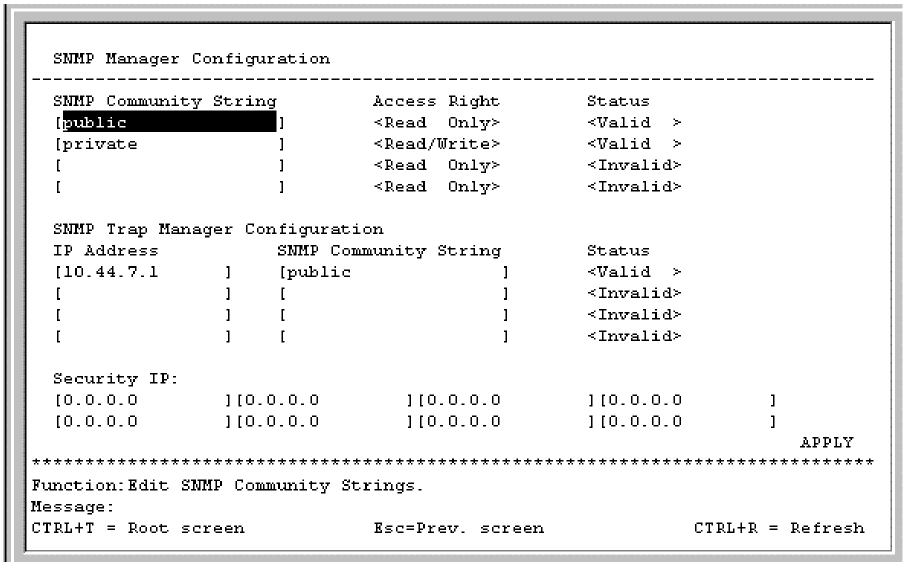
SNMP (version 1) implements a rudimentary form of security by requiring that each request include a “community name.” A community name is an arbitrary string of characters used as a “password” to control access to the switch module. If the switch module receives a request with a community name it does not recognize, it triggers an authentication trap.

The SNMP allows up to four different community names to be defined. The community name “public” is defined by default; you can change this name in addition to adding others. You need to coordinate these names with the community name settings you use in your network management system.

To set the **SNMP Manager Configuration** settings:

1. Highlight **SNMP Manager Configuration** on the main menu.

2. Press the **Enter** key. The following screen is displayed.



```
  SNMP Manager Configuration
-------------------------------------------------------------------------------
  SNMP Community String         Access Right        Status
  [public              ]        <Read  Only>        <Valid  >
  [private             ]        <Read/Write>        <Valid  >
  [                    ]        <Read  Only>        <Invalid>
  [                    ]        <Read  Only>        <Invalid>

  SNMP Trap Manager Configuration
  IP Address           SNMP Community String        Status
  [10.44.7.1      ]    [public              ]       <Valid  >
  [               ]    [                    ]       <Invalid>
  [               ]    [                    ]       <Invalid>
  [               ]    [                    ]       <Invalid>

  Security IP:
  [0.0.0.0        ][0.0.0.0         ][0.0.0.0         ][0.0.0.0          ]
  [0.0.0.0        ][0.0.0.0         ][0.0.0.0         ][0.0.0.0          ]
                                                                        APPLY
*******************************************************************************
Function:Edit SNMP Community Strings.
Message:
CTRL+T = Root screen            Esc=Prev. screen              CTRL+R = Refresh
```

The following SNMP Manager and Trap Manager Configuration parameters can be set:

— **SNMP Community String**—Displays the community string that is included on SNMP packets sent to and from the switch module. Any station not privy to this community does not receive the packet.

— **Access Right**—Allows each community to be separately set to either **Read-Only,** meaning that the community member can only view switch settings, or **Read/Write,** which allows the member to change settings in the switch module.

— **Status**—Determines whether this community name entry is **Valid** or **Invalid.** An entry can be disabled by changing its status to **Invalid.**

— **IP Address**—Designates the IP address of the network management station that receives traps.

The **Security IP** section allows you to create a list of IP addresses that are allowed to access the switch module via SNMP or Telnet.

3. After making your changes, highlight **APPLY**, then press the **Enter** key.

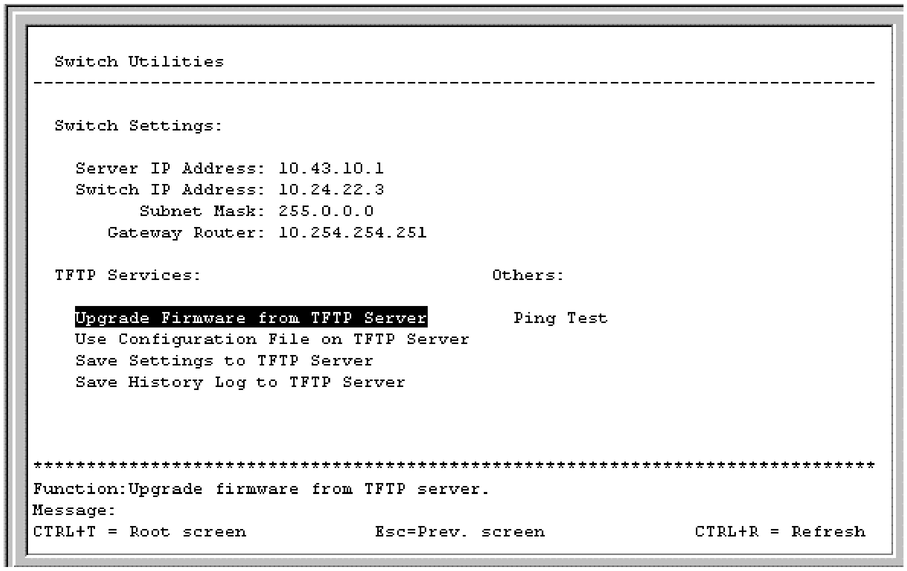
NOTE: To save the configuration settings permanently, you must enter them into NVRAM using the **Save Changes** option on the main menu. See the “Saving Changes” section earlier in this chapter.

Using System Utilities

To set the system utilities settings:

1. Highlight **System Utilities** on the main menu.

2. Press the **Enter** key. The following screen is displayed.



```
  Switch Utilities
--------------------------------------------------------------------------------

  Switch Settings:

    Server IP Address: 10.43.10.1
    Switch IP Address: 10.24.22.3
          Subnet Mask: 255.0.0.0
       Gateway Router: 10.254.254.251

  TFTP Services:                           Others:

    Upgrade Firmware from TFTP Server        Ping Test
    Use Configuration File on TFTP Server
    Save Settings to TFTP Server
    Save History Log to TFTP Server



********************************************************************************
Function:Upgrade firmware from TFTP server.
Message:
CTRL+T = Root screen            Esc=Prev. screen              CTRL+R = Refresh
```

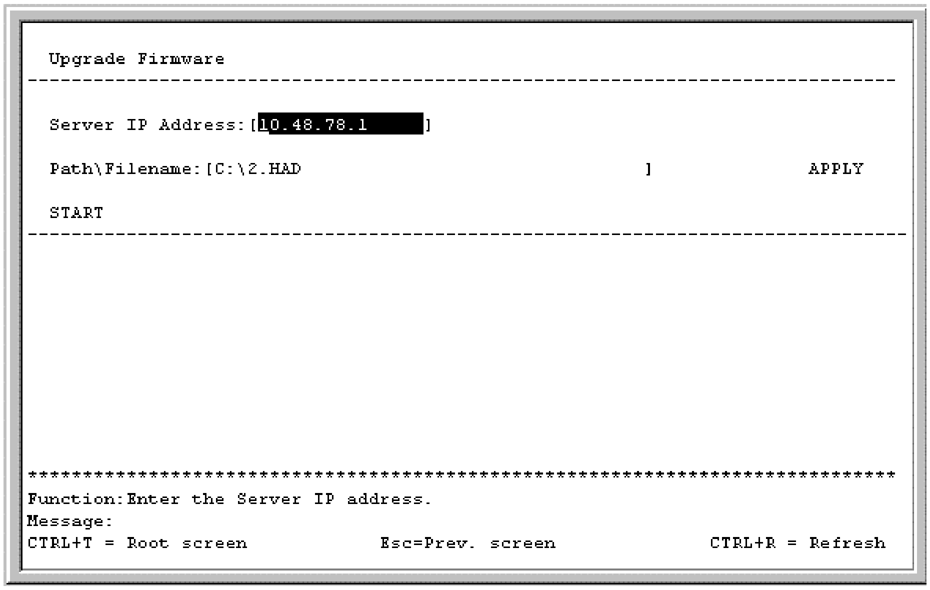
NOTE: Trivial File Transfer Protocol (TFTP) services allow the switch firmware to be upgraded by transferring a new firmware file from a TFTP server to the switch module. A configuration file can also be loaded into the switch module from a TFTP server, switch module settings can be saved to the TFTP server, and a history log can be uploaded from the switch module to the TFTP server.

Upgrading Firmware from a TFTP Server

To upgrade the firmware from a TFTP server:

1. Highlight **Upgrade Firmware from TFTP Server** on the **Switch Utilities** menu.

2. Press the **Enter** key. The following screen is displayed.



```
  Upgrade Firmware
-------------------------------------------------------------------------------

  Server IP Address:[10.48.78.1      ]

  Path\Filename:[C:\2.HAD                                  ]              APPLY

  START
--------------------------------------------------------------------------------










*******************************************************************************
Function:Enter the Server IP address.
Message:
CTRL+T = Root screen           Esc=Prev. screen            CTRL+R = Refresh
```

3. Type the IP address of the TFTP server in the **Server IP Address** field.

   NOTE: The TFTP server must be on the same IP subnet as the switch module.

4. Type the path and the filename to the firmware file on the TFTP server in the **Path\Filename** field.

   NOTE: The TFTP server must be running TFTP server software to perform the file transfer. TFTP server software is a part of many network management software packages, or can be obtained as a separate program.

5. Highlight **APPLY.**
6. Press the **Enter** key to record the IP address of the TFTP server.
7. Highlight **START.**
8. Press the **Enter** key to initiate the file transfer.

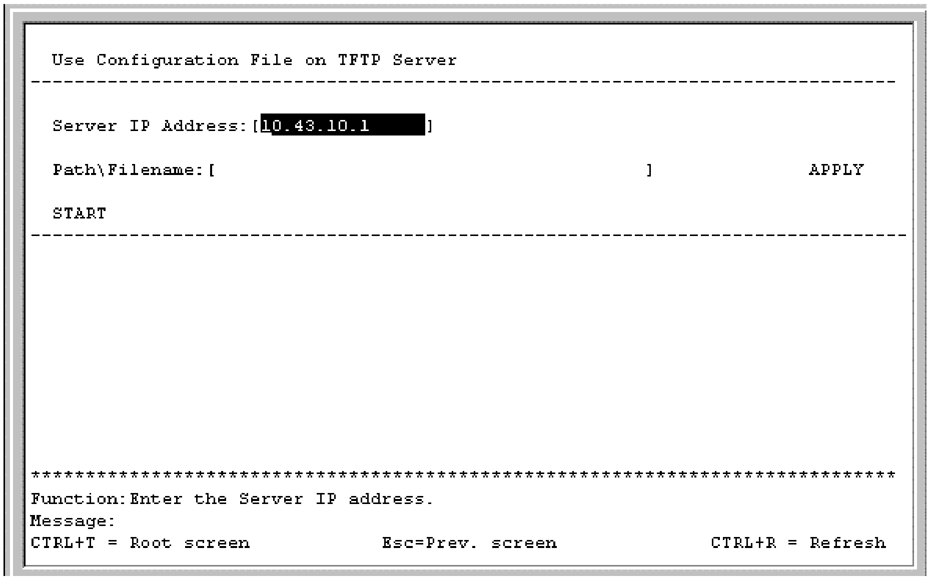
   NOTE: To save the configuration settings permanently, you must enter them into NVRAM using the **Save Changes** option on the main menu. See the “Saving Changes” section earlier in this chapter.

Downloading Configuration File from a TFTP Server

To download a switch module configuration file from a TFTP server:

1. Highlight **Use a Configuration File on TFTP Server** on the **Switch Utilities** menu.

2. Press the **Enter** key. The following screen is displayed.



```
  Use Configuration File on TFTP Server
--------------------------------------------------------------------------------

  Server IP Address:[10.43.10.1     ]

  Path\Filename:[                                        ]              APPLY

  START
--------------------------------------------------------------------------------









********************************************************************************
Function:Enter the Server IP address.
Message:
CTRL+T = Root screen           Esc=Prev. screen             CTRL+R = Refresh
```

3. Type the IP address of the TFTP server in the **Server IP Address** field.
4. Type the location of the switch module configuration file on the TFTP server in the **Path\Filename** field.
5. Highlight **APPLY.**
6. Press the **Enter** key to record the IP address of the TFTP server.
7. Highlight **START.**
8. Press the **Enter** key to initiate the file transfer.

NOTE: To save the configuration settings permanently, you must enter them into NVRAM using the **Save Changes** option on the main menu. See the “Saving Changes” section earlier in this chapter.

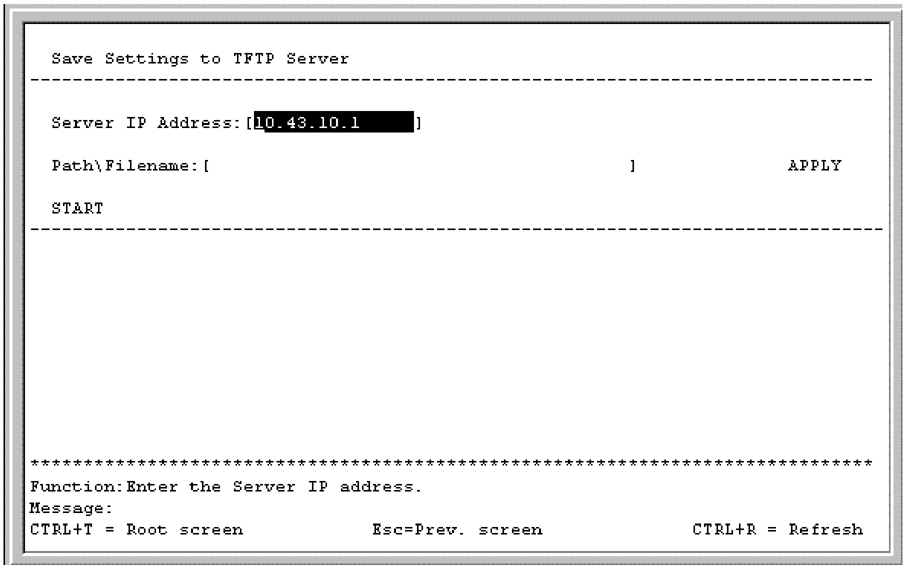
Saving Settings to a TFTP Server

After completing the final configuration for the switch module, Compaq highly recommends that you save the switch module configuration file to TFTP server storage.

To save the switch module configuration file to a TFTP server:

1. Highlight **Save Settings to TFTP Server** on the **Switch Utilities** menu.

2. Press the **Enter** key. The following screen is displayed.



```
  Save Settings to TFTP Server
--------------------------------------------------------------------------------

  Server IP Address:[10.43.10.1      ]

  Path\Filename:[                                       ]              APPLY

  START
---------------------------------------------------------------------------------









********************************************************************************
Function:Enter the Server IP address.
Message:
CTRL+T = Root screen           Esc=Prev. screen             CTRL+R = Refresh
```

3. Type the IP address of the TFTP server in the **Server IP Address** field.
4. Type the location of the switch module configuration file on the TFTP server in the **Path\Filename** field.
5. Highlight **APPLY.**
6. Press the **Enter** key.
7. Highlight **START.**
8. Press the **Enter** key to initiate the file transfer.

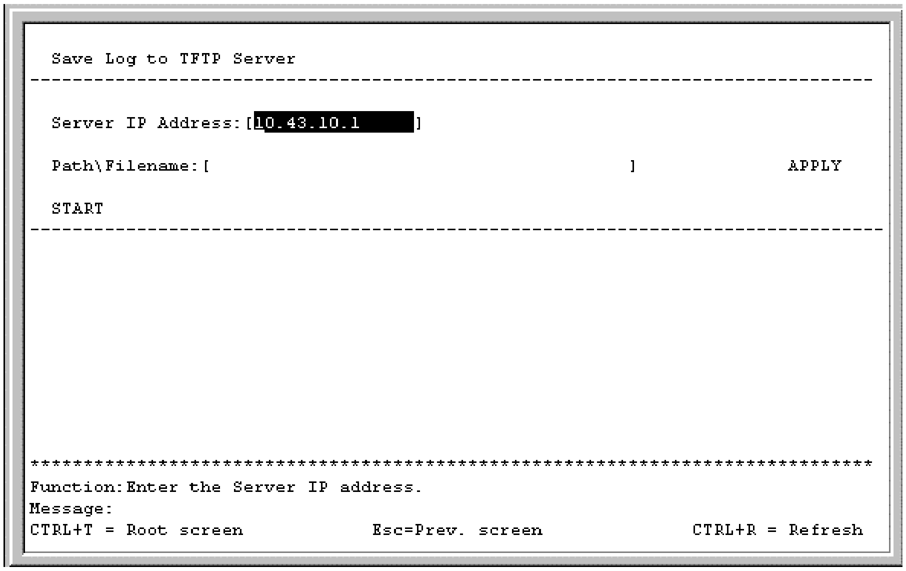
NOTE: To save the configuration settings permanently, you must enter them into NVRAM using the **Save Changes** option on the main menu. See the “Saving Changes” section earlier in this chapter.

Saving the History Log to a TFTP Server

To save the **History Log** on a TFTP server:

1. Highlight **Save History Log to TFTP Server** on the **Switch Utilities** menu.

2. Press the **Enter** key. The following screen is displayed.



```
  Save Log to TFTP Server
--------------------------------------------------------------------------------

  Server IP Address:[10.43.10.1       ]

  Path\Filename:[                                        ]               APPLY

  START
--------------------------------------------------------------------------------









********************************************************************************
Function:Enter the Server IP address.
Message:
CTRL+T = Root screen            Esc=Prev. screen             CTRL+R = Refresh
```

3. Type the IP address of the TFTP server in the **Server IP Address** field.
4. Type the path and filename for the history log on the TFTP server in the **Path\Filename** field.
5. Highlight **APPLY.**
6. Press the **Enter** key to make the changes current.
7. Highlight **START.**
8. Press the **Enter** key to initiate the file transfer.

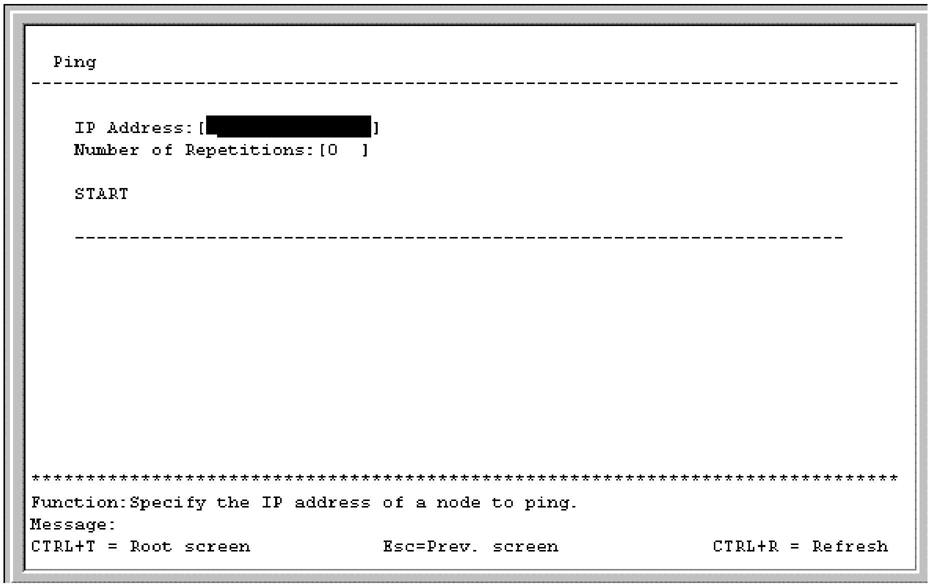
NOTE: To save the configuration settings permanently, you must enter them into NVRAM using the **Save Changes** option on the main menu. See the “Saving Changes” section earlier in this chapter.

Performing a Ping Test

To test the connection with another network device using Ping:

1. Highlight **Ping Test** on the **Switch Utilities** menu.

2. Press the **Enter** key. The following screen is displayed.



```
  Ping
-------------------------------------------------------------------------------

    IP Address:[                ]
    Number of Repetitions:[0  ]

    START

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









*******************************************************************************
Function:Specify the IP address of a node to ping.
Message:
CTRL+T = Root screen           Esc=Prev. screen            CTRL+R = Refresh
```

3. Type the IP address of the network device to be pinged in the **IP Address** field.
4. Type the number of test packets to be sent (three is usually enough) in the **Number of Repetitions** field.
5. Highlight **START.**
6. Press the **Enter** key.

NOTE: To save the configuration settings permanently, you must enter them into NVRAM using the **Save Changes** option on the main menu. See the “Saving Changes” section earlier in this chapter.

Rebooting the Switch Module

The switch module reboot options are:

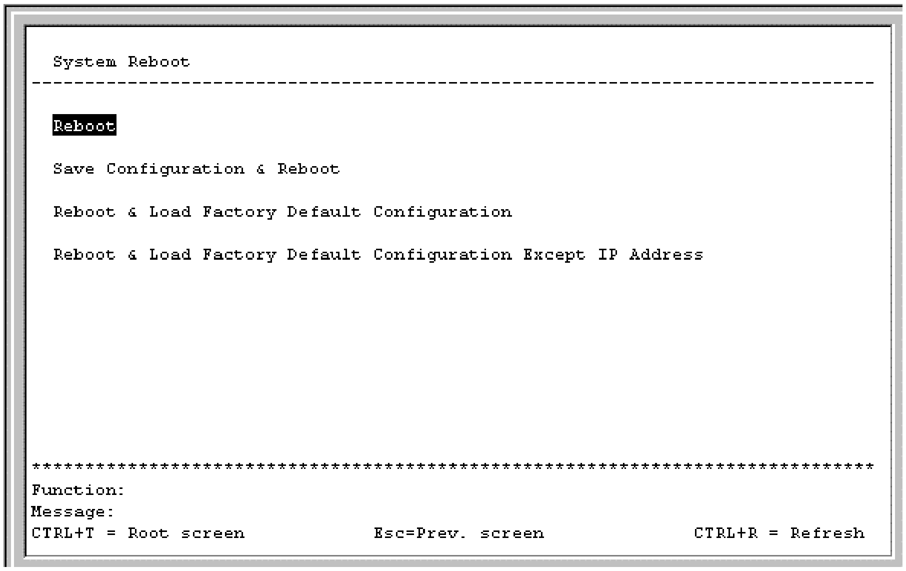
- **Reboot**—Restarts the switch module. Any configuration settings not saved using **Save Changes** from the main menu are lost. The switch module configuration is restored to the last configuration saved in NVRAM.
- **Save Configuration & Reboot**—Saves the configuration to NVRAM (identical to using **Save Changes**) and then restarts the switch module.

- **Reboot & Load Factory Default Configuration**—Restarts the switch module using the default factory configuration. All user-defined configuration data is lost.
- **Reboot & Load Factory Default Configuration Except IP Address**—Restarts the switch module using the default factory configuration, except the user-configured IP address, which is retained. All other configuration data is lost. If you want your IP address to default from DHCP or BOOTP, do not choose this option.

NOTE: See Appendix C for a list of factory default settings.

To reboot the switch module from the console:

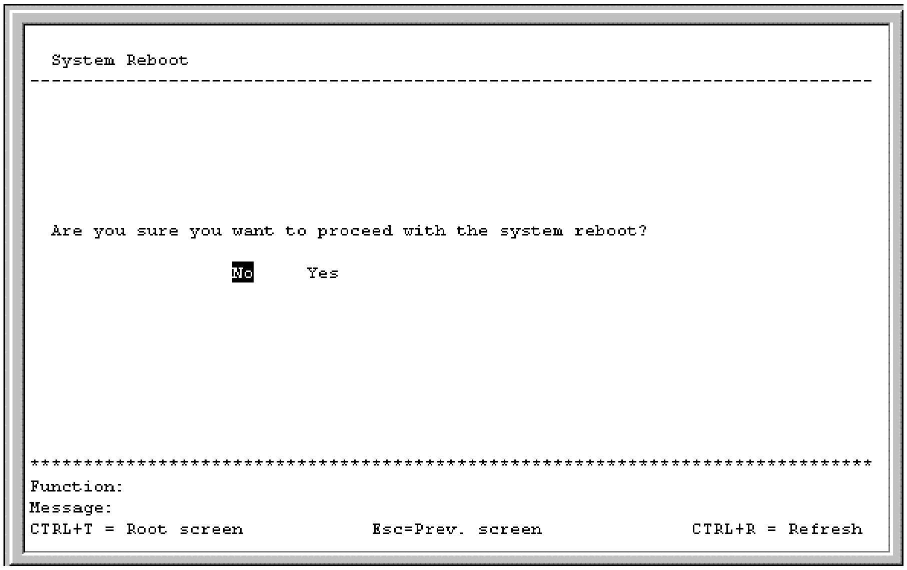
1. Highlight **Reboot** on the main menu.
2. Press the **Enter** key. The following screen is displayed.



```
  System Reboot
--------------------------------------------------------------------------------

  Reboot

  Save Configuration & Reboot

  Reboot & Load Factory Default Configuration

  Reboot & Load Factory Default Configuration Except IP Address








********************************************************************************
Function:
Message:
CTRL+T = Root screen            Esc=Prev. screen              CTRL+R = Refresh
```

3. Highlight the appropriate selection.

4. Press the **Enter** key. The following screen is displayed.



```
  System Reboot
--------------------------------------------------------------------------------




  Are you sure you want to proceed with the system reboot?

                 No     Yes







********************************************************************************
Function:
Message:
CTRL+T = Root screen           Esc=Prev. screen              CTRL+R = Refresh
```

5. Highlight **Yes.**
6. Press the **Enter** key.

Logging Out

To exit the setup pages, select **Logout** on the **Maintenance** menu. The Account Login screen is displayed.

4

Configuring the Switch Modules Using the Web-Based Management Interface

Introduction

The interconnect switch offers an embedded Web-based (HTML) interface that allows users to manage each switch module from anywhere on the network through a standard browser, such as Netscape Navigator or Microsoft Internet Explorer. The Web browser acts as a universal access tool and can communicate directly with the switch modules using the HTTP protocol.

NOTE: Your browser window may differ compared with the screen shots in this guide.

The Web-based management module and the console management program (and Telnet) are different ways to access and configure the same internal switching software. All settings encountered in Web-based management are the same as those found in the console management program.

This chapter describes how to use the Web-based management interface to access the switch modules, change their settings, and monitor their operation.

NOTE: This Web-based management module does not accept Chinese language input (or other languages requiring two bytes per character).

Before You Begin

The ProLiant BL e-Class C-GbE Interconnect Switch supports a wide array of functions and gives great flexibility and increased network performance. This flexibility and rich feature set require some planning to arrive at a deployment strategy that will maximize the potential of the interconnect switch. See the section, “Planning the Interconnect Switch Configuration,” in Chapter 2 for things to keep in mind as you configure your switch modules.

Connecting to the Switch Modules

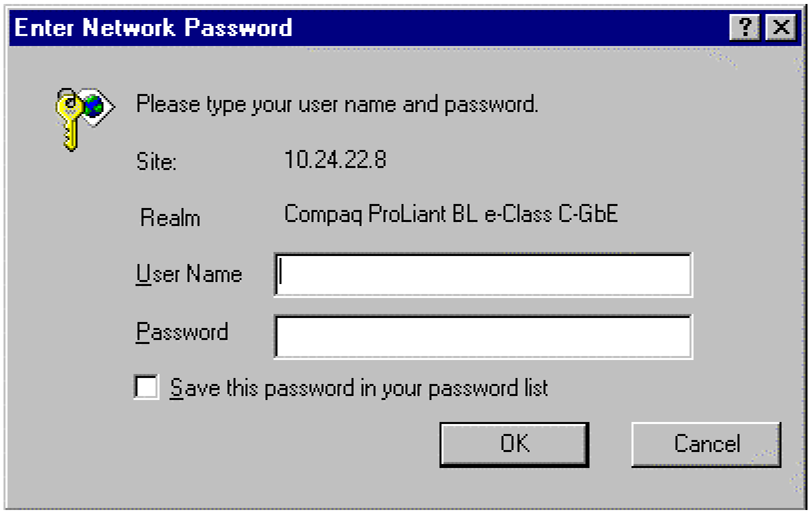
Before you can connect to a switch module using the Web-based management interface, you must set up the IP address on the switch module. By default, if there is a DHCP server on the network, a switch module obtains the IP address automatically. If there is no DHCP server on the network, configure the IP address of the switch modules using the console management interface.

NOTE: See the section, “Accessing the Switch Modules,” in Chapter 2 for information on how to connect to the console management interface. See the sections, “Logging on to the Switch Module” and “Configuring IP Address,” in Chapter 3 for information on how to use the console interface management system to manually configure a switch module’s IP address.

To connect to a switch module using the Web-based management interface:

1. Start a Web browser, for example, Microsoft Internet Explorer version 5.5 or higher or Netscape Navigator version 6.1 or higher.
2. Type the IP address you have defined for the switch module in the browser address bar. The URL in the address bar should read something like: http://10.24.22.8.
3. Press the **Enter** key. The **Enter Network Password** dialog box for the switch module is displayed.

IMPORTANT: The proxy for session connection should be turned off.



Please type your user name and password.

Site: 10.24.22.8

Realm Compaq ProLiant BL e-Class C-GbE

User Name

Password

☐ Save this password in your password list

Logging on to the Switch Module

IMPORTANT: The switch module does not have any initial user names or passwords set. Compaq recommends that after logging on, you create at least one Root-level user as the switch administrator. (See Table 2-1 in Chapter 2, “Setting up and Installing the Interconnect Switch,” for an explanation of user privileges.) If you forget your password after it has been set up, call Compaq Customer Support for assistance.

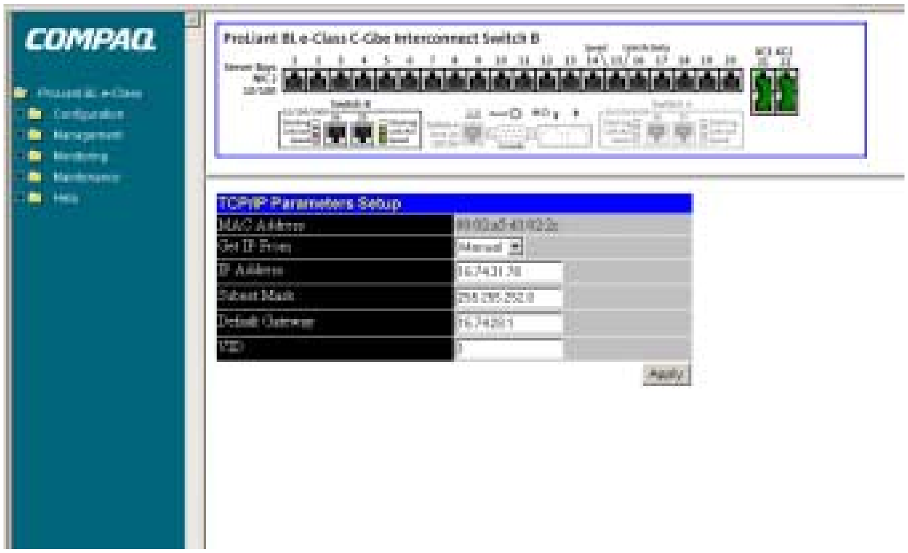
To log on to the switch module for the first time:

1. Click **OK** at the **Enter Network Password** dialog box. No initial user name or password is set for the first user. The main page in the Web-based management module is displayed.

   The main page displays the main menu, an active graphic of the switch module, and the **TCP/IP Parameters Setup** window.

   The active graphic of the switch module allows you to monitor the switch module status. Graphical LEDs display current link speed and activity. Graphical RJ-45 connectors allow you to display statistics for individual ports. See the section, “Monitoring the Switch Module using the Active Switch Graphic,” for detailed information.

   The **TCP/IP Parameters Setup** window is used to determine whether the interconnect switch should get its IP address settings from the user (Manual), a BOOTP server, or a DHCP server. See the section “Configuring IP Address.”



TCP/IP Parameters Setup	
MAC Address	[illegible]
Get IP From	Manual
IP Address	[illegible]
Subnet Mask	[illegible]
Default Gateway	[illegible]
VID	1

2. Click the small square hyperlink to the left of the folder icons to display a list of additional menus used to configure, manage, monitor, and maintain the switch module.

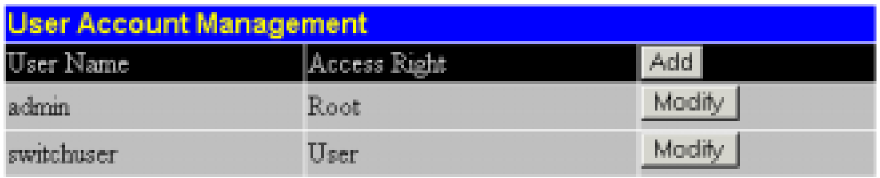
Setting Up New Users

You can set up a maximum of eight users on a switch module.

NOTE: After logging on to the switch module for the first time, you need to set up at least one user account with Root privileges.

To create a new user account:

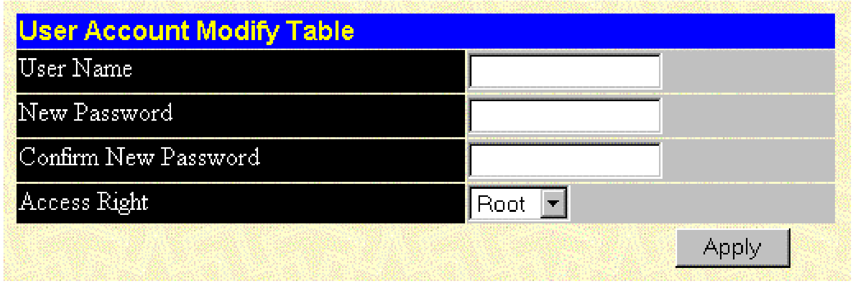
1. Click the small square to the left of the **Management** folder on the main menu. The Management menus are displayed.
2. Click **User Accounts.** The following window is displayed.



User Account Management

User Name	Access Right	Add
admin	Root	Modify
switchuser	User	Modify

3. Click **Add** to add a new user to the table. The following window is displayed.



User Account Modify Table

User Name	
New Password	
Confirm New Password	
Access Right	Root

4. Type the user name in the **User Name** field.
5. Type the user's password in the **New Password** field.
6. Type the new password a second time in the **Confirm Password** field.
7. Click the drop-down arrow in the **Access Right** field to select the access level. There are three access levels: **User, User+,** and **Root.** A **Root** user has full read/write access, while a **User** has read only access. A **User+** has the same privileges as a **User,** but with the added ability to restart the switch module.

   NOTE: See Table 2-1 in Chapter 2 for an explanation of access rights.

8. Click **Apply.** The **Enter Network Password** dialog box is displayed.
9. Type the new user's name in the **User Name** field.

10. Type the user’s password in the **Password** field.
11. Click **OK.** The **User Account Management** window is displayed with the new user listed. You are now ready to configure the switch module.

NOTE: To save the configuration settings permanently, you must enter them into the non-volatile RAM (NVRAM) using the **Save Changes** option on the **Maintenance** menu. See the section, “Saving Changes” in this chapter.

Saving Changes

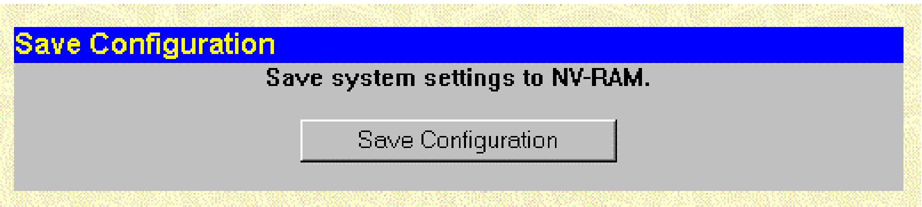
The switch module has two levels of memory, normal RAM and NVRAM. Configuration changes on a screen are made effective by clicking the **Apply** button. The settings are then immediately applied to the switching software in RAM.

If you want configuration changes to be permanent, you must save them to NVRAM using the **Save Changes** option on the **Maintenance** menu before rebooting the system.

NOTE: Some settings require you to restart the switch module before they take effect. Restarting the switch module erases all settings in RAM and reloads the stored settings from the NVRAM.

To retain any configuration changes permanently:

1. Open the **Maintenance** folder on the main menu.
2. Click **Save Changes.** The **Save Configuration** window is displayed.



3. Click **Save Configuration** to save all the changes made in the current session to the switch module’s NVRAM memory. A message box is displayed telling you that the save is complete.
4. Click **OK.** After the switch module configuration settings have been saved to NVRAM, they become the default settings for the switch module. These settings are used every time the switch module is rebooted.

IMPORTANT: After saving your final configuration, Compaq highly recommends that you save the switch module configuration image to TFTP server storage. See the section, “Saving Settings to TFTP Server,” in this chapter.

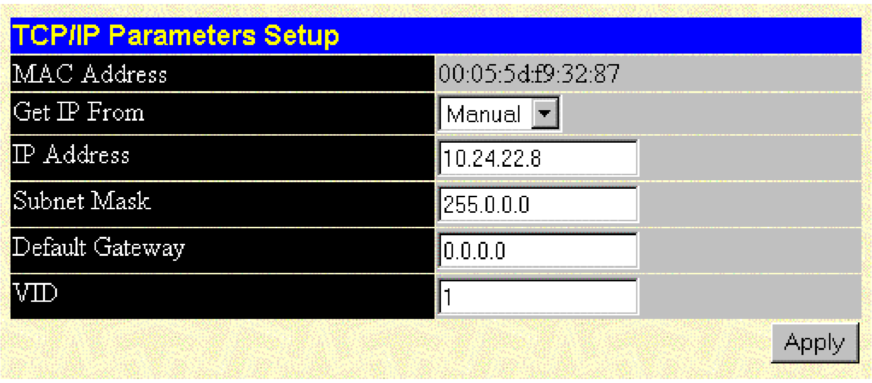
Configuring the Switch Module

The Configuration menu has the following features:

- IP Address
- Switch Information
- Advanced Settings
- Port Configuration
- Port Mirroring
- Port Trunking
- IGMP Snooping

Configuring IP Address

When you select **IP Address** from the **Configuration** menu, the following screen is displayed.



TCP/IP Parameters Setup

MAC Address	00:05:5d:f9:32:87
Get IP From	Manual
IP Address	10.24.22.8
Subnet Mask	255.0.0.0
Default Gateway	0.0.0.0
VID	1

The **TCP/IP Parameters Setup** window is used to determine whether the switch module should get its IP address settings from the user (Manual), a BOOTP server, or a DHCP server.

The window displays the following information:

- **MAC Address**—The Ethernet address for the device, also known as the physical address.
- **Get IP From**—There are three choices for how the switch module receives its IP address settings: **Manual, BOOTP,** and **DHCP.**
- **IP Address**—The host address for the device on the TCP/IP network.
- **Subnet Mask**—The address mask that controls subnetting on your TCP/IP network.

- **Default Gateway**—The IP address of the device, usually a router, which handles connections to other subnets or other TCP/IP networks.
- **VID**—The VLAN ID number.

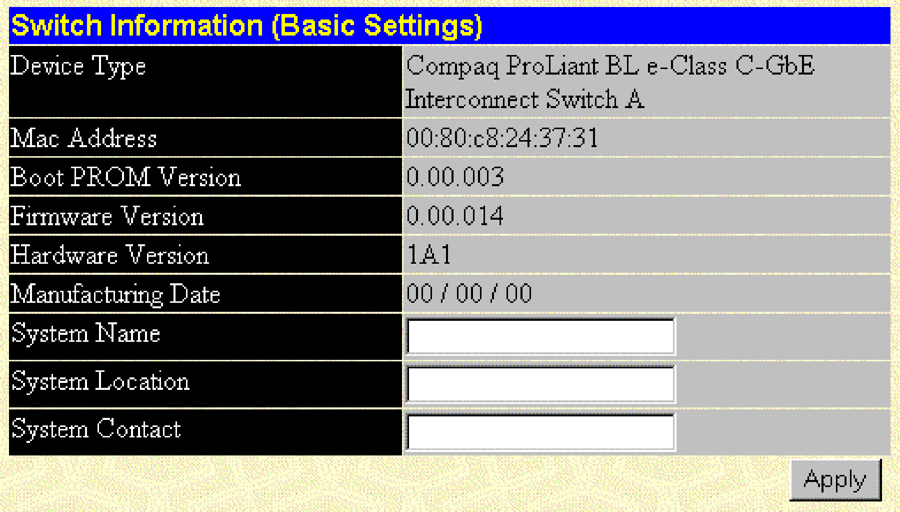
To set the IP address:

1. Select Manual, BOOTP, or DHCP in the **Get IP From** field:
   - — If you select **Manual,** enter the **IP Address, Subnet Mask,** and **Default Gateway** of the switch module.
   - — If you select **BOOTP,** you do not need to configure any IP parameters, because a BOOTP server automatically assigns IP configuration parameters to the switch module.
   - — If you select **DHCP,** a DHCP request will be sent when the switch module is powered up.
2. Click **Apply** to activate the new settings.

NOTE: To save the configuration settings permanently, you must enter them into the NVRAM using the **Save Changes** option on the **Maintenance** menu. See the section, "Saving Changes," earlier in this chapter.

Setting Basic Switch Module Information

When you select **Switch Information** from the **Configuration** menu, the following screen is displayed.



Switch Information (Basic Settings)

Device Type	Compaq ProLiant BL e-Class C-GbE Interconnect Switch A
Mac Address	00:80:c8:24:37:31
Boot PROM Version	0.00.003
Firmware Version	0.00.014
Hardware Version	1A1
Manufacturing Date	00 / 00 / 00
System Name	
System Location	
System Contact	

The **Switch Information (Basic Settings)** window displays the following information:

- **Device Type**—A description of the switch module type.
- **External Module Type**—A description of the optional module plugged into the front slot.

- **MAC Address**—The Ethernet address for the device.
- **Boot PROM Version**—The version number for the firmware chip. This information is needed for new runtime software downloads.
- **Firmware Version**—The version number of the firmware installed on the switch module. This information can be updated by using the **Update Firmware** window in the **Reset and Update** section.
- **Base Module Version**—The version number of the base module.
- **External Module Version**—The version of the optional module plugged into the front slot.
- **System Name**—A user-assigned name for the switch module.
- **System Location**—A user-assigned description for the physical location of the switch module.
- **System Contact**—The name of the person to contact if there are any problems or questions with the system. You may also want to include a phone number or extension.

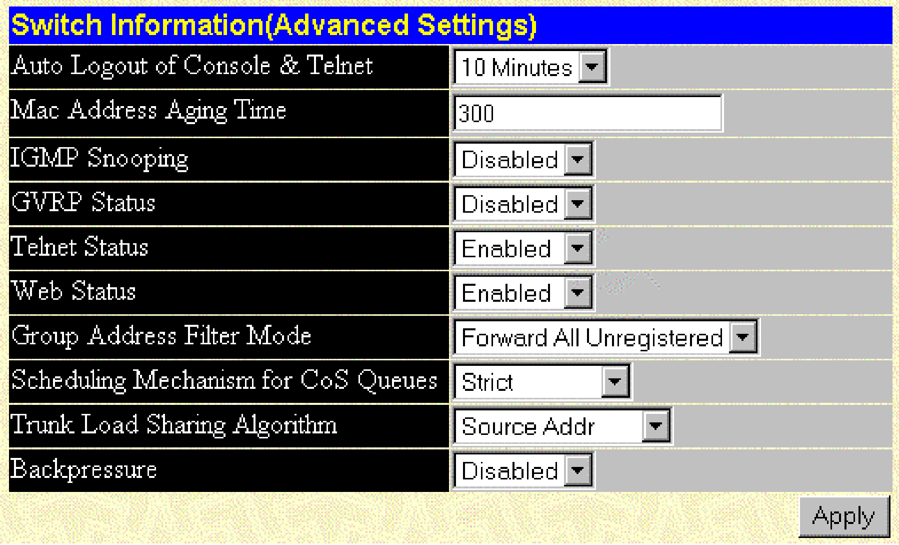
To complete the user-assigned switch module information:

1. Type the system name in the **System Name** field.
2. Type the physical location of the switch module in the **System Location** field.
3. Type the name of the contact person responsible for the switch module (and telephone or other contact information) in the **System Contact** field.
4. Click **Apply.**

NOTE: To save the configuration settings permanently, they must be entered into the NVRAM using the **Save Changes** option on the **Maintenance** menu. See the section, “Saving Changes,” earlier in this chapter.

Configuring Advanced Settings

When you select **Advanced Setting** from the **Configuration** menu, the following screen is displayed.



Switch Information(Advanced Settings)

Auto Logout of Console & Telnet	10 Minutes
Mac Address Aging Time	300
IGMP Snooping	Disabled
GVRP Status	Disabled
Telnet Status	Enabled
Web Status	Enabled
Group Address Filter Mode	Forward All Unregistered
Scheduling Mechanism for CoS Queues	Strict
Trunk Load Sharing Algorithm	Source Addr
Backpressure	Disabled

You can change the following parameters:

- **Auto-Logout of Console & Telnet**—Select the time that the interface can be idle before the switch module automatically logs-out the user. The options are **2 minutes, 5 minutes, 10 minutes, 15 minutes,** and **Never**.
- **MAC Address Aging Time**—Select the length of time a learned MAC address remains in the forwarding table without being accessed (that is, how long a learned MAC address is allowed to remain idle). The aging time can be set to any value between 10 and 1,000,000 seconds.

  NOTE: A very long aging time can result in out-of-date dynamic entries that may cause incorrect packet filtering/forwarding decisions. A very short aging time may cause entries to be aged out too soon, resulting in a high percentage of received packets whose source addresses cannot be found in the address table, in which case the switch module will broadcast the packet to all ports, negating many of the benefits of having a switch module.

- **IGMP Snooping**—Choose to enable or disable Internet Group Management Protocol (IGMP) Snooping. IGMP Snooping enables the switch module to read IGMP packets being forwarded through the switch module in order to obtain forwarding information from them, such as which ports contain Multicast members.
- **GVRP Status**—Choose to enable or disable GVRP on the switch module. Group VLAN Registration Protocol is a protocol that allows members to dynamically join VLANs.

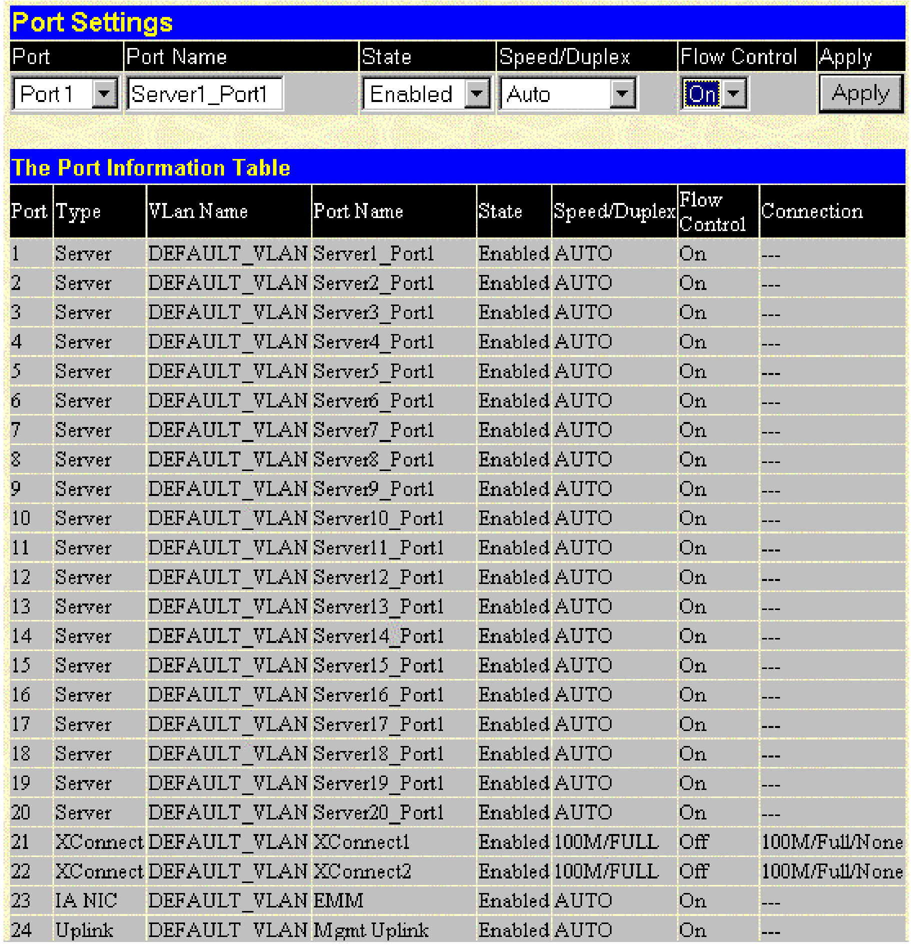
- **Telnet Status**—Choose to enable or disable access to the switch module over the network using the TCP/IP Telnet protocol.
- **Web Status**—Choose to enable or disable management of the switch module over the Web.
- **Group Address Filter Mode**—Select one of the forwarding or filtering options to set the IGMP filter mode for processing multicast packets.
- **Scheduling Mechanism for CoS Queues**—Choose one of the **Class of Service** queue options. If you select **Strict**, then when the highest priority queue is full, those packets will be the first to be forwarded. If you select **RoundRobin,** the forwarding is based on the settings made on the **Class of Service Configuration** screen.
- **Trunk Load Sharing Algorithm**—Select one of the trunk load sharing options, **Source Addr, Destination Addr,** or **Both,** to determine if load balancing decisions will be made by the source MAC address, destination MAC address, or both addresses.
- **Backpressure**—Select Enabled or Disabled to initiate or terminate traffic flow control in and out of the interconnect switch.

After making your choices in **Advanced Settings,** click **Apply.**

NOTE: To save the configuration settings permanently, they must be entered into the NVRAM using the **Save Changes** option on the **Maintenance** menu. See the section, “Saving Changes,” earlier in this chapter.

Configuring Port Settings

When you select **Port Configuration** from the **Configuration** menu, the following screen is displayed.



Port Settings

Port	Port Name	State	Speed/Duplex	Flow Control	Apply
Port 1	Server1_Port1	Enabled	Auto	On	Apply

The Port Information Table

Port	Type	VLan Name	Port Name	State	Speed/Duplex	Flow Control	Connection
1	Server	DEFAULT_VLAN	Server1_Port1	Enabled	AUTO	On	---
2	Server	DEFAULT_VLAN	Server2_Port1	Enabled	AUTO	On	---
3	Server	DEFAULT_VLAN	Server3_Port1	Enabled	AUTO	On	---
4	Server	DEFAULT_VLAN	Server4_Port1	Enabled	AUTO	On	---
5	Server	DEFAULT_VLAN	Server5_Port1	Enabled	AUTO	On	---
6	Server	DEFAULT_VLAN	Server6_Port1	Enabled	AUTO	On	---
7	Server	DEFAULT_VLAN	Server7_Port1	Enabled	AUTO	On	---
8	Server	DEFAULT_VLAN	Server8_Port1	Enabled	AUTO	On	---
9	Server	DEFAULT_VLAN	Server9_Port1	Enabled	AUTO	On	---
10	Server	DEFAULT_VLAN	Server10_Port1	Enabled	AUTO	On	---
11	Server	DEFAULT_VLAN	Server11_Port1	Enabled	AUTO	On	---
12	Server	DEFAULT_VLAN	Server12_Port1	Enabled	AUTO	On	---
13	Server	DEFAULT_VLAN	Server13_Port1	Enabled	AUTO	On	---
14	Server	DEFAULT_VLAN	Server14_Port1	Enabled	AUTO	On	---
15	Server	DEFAULT_VLAN	Server15_Port1	Enabled	AUTO	On	---
16	Server	DEFAULT_VLAN	Server16_Port1	Enabled	AUTO	On	---
17	Server	DEFAULT_VLAN	Server17_Port1	Enabled	AUTO	On	---
18	Server	DEFAULT_VLAN	Server18_Port1	Enabled	AUTO	On	---
19	Server	DEFAULT_VLAN	Server19_Port1	Enabled	AUTO	On	---
20	Server	DEFAULT_VLAN	Server20_Port1	Enabled	AUTO	On	---
21	XConnect	DEFAULT_VLAN	XConnect1	Enabled	100M/FULL	Off	100M/Full/None
22	XConnect	DEFAULT_VLAN	XConnect2	Enabled	100M/FULL	Off	100M/Full/None
23	IA NIC	DEFAULT_VLAN	EMM	Enabled	AUTO	On	---
24	Uplink	DEFAULT_VLAN	Mgmt Uplink	Enabled	AUTO	On	---

To change the port settings:

1. Select the port you want to configure in the **Port** field, or click the port on the switch module front panel display.
2. Choose **Enabled** or **Disabled** in the **State** field. If you choose **Disabled,** devices connected to that port cannot use the switch module, and the switch module purges their addresses from its address table after the MAC address aging time elapses.

3. Configure the **Speed/Duplex** setting for the port:
   - Select **Auto** to allow the port to select the best transmission speed, duplex mode, and flow control settings based on the capabilities of the device at the other end. The other selections allow you to force the port to operate in the specified manner.
   - Select **100M/FULL** for port operation at 100 Mb/s and full duplex.
   - Select **100M/HALF** for port operation at 100 Mb/s and half duplex.
   - Select **10M/FULL** for port operation at 10 Mb/s and full duplex.
   - Select **10M/HALF** for port operation at 10 Mb/s and half duplex.
4. Configure the **Flow Control** setting for the port:
   - Choose **On** in full-duplex mode to implement IEEE 802.3x flow control.
   - Choose **Off** for no flow control.

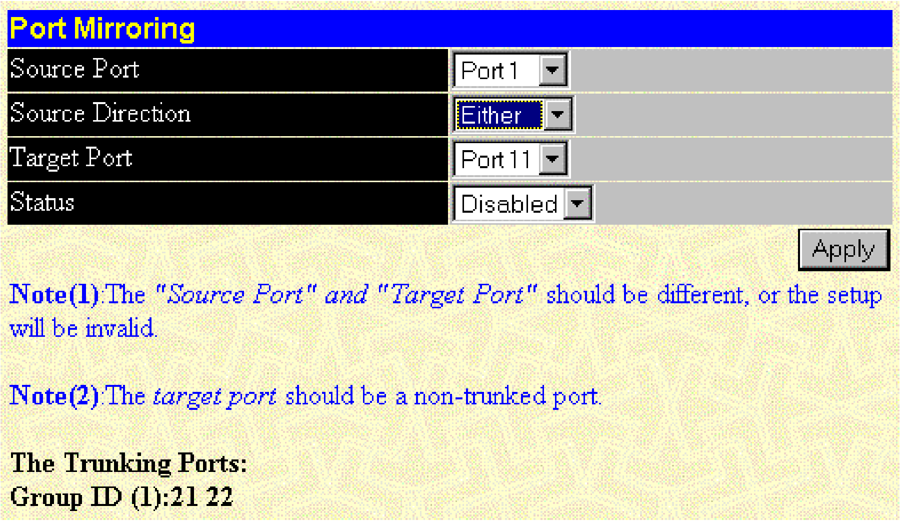
   IMPORTANT: You must reboot the switch module before a flow control change can take effect.

5. Click **Apply.**

   NOTE: To save the configuration settings permanently, you must enter them into the NVRAM using the **Save Changes** option on the **Maintenance** menu. See the section, “Saving Changes,” earlier in this chapter.

Configuring Port Mirroring

When you select **Port Mirroring** from the **Configuration** menu, the following screen is displayed



Port Mirroring

Source Port	Port 1
Source Direction	Either
Target Port	Port 11
Status	Disabled

Note(1):The *"Source Port" and "Target Port"* should be different, or the setup will be invalid.

Note(2):The *target port* should be a non-trunked port.

The Trunking Ports:
Group ID (1):21 22

The switch module allows you to copy frames transmitted and received on a port, and to redirect the copies to another port. You can attach a monitoring device to the mirrored port, such as a sniffer or an RMON probe, to view details about the packets passing through the first port.

IMPORTANT: You cannot mirror a faster port onto a slower port. For example, if you try to mirror the traffic from a 100 Mb/s port onto a 10 Mb/s port, you can cause throughput problems. The port you are copying frames from should always support an equal or lower speed than the port to which you are sending the copies. Also, the target port for mirroring cannot be a member of a trunk group. A target port and a source port also cannot be the same port.

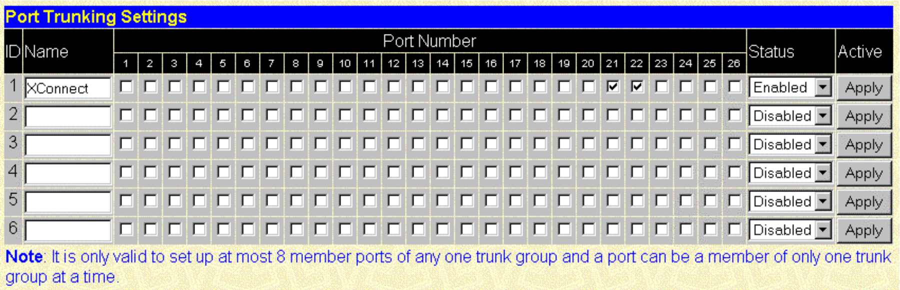
To configure a mirror port:

1. Select the **Source Port** from which you want to copy frames.
2. Select the **Source Direction,** either **Ingress, Egress,** or **Either.**
3. Select the **Target Port** that receives the copies from the source port. This is the port where you would connect a monitoring/troubleshooting device, such as a sniffer or an RMON probe.
4. Select **Enabled** in the **Status** field.
5. Click **Apply.**

NOTE: To save the configuration settings permanently, you must enter them into the NVRAM using the **Save Changes** option on the **Maintenance** menu. See the section, “Saving Changes,” earlier in this chapter.

Configuring Port Trunking

When you select **Port Trunking** from the **Configuration** menu, the following screen is displayed.



Port Trunking Settings

ID	Name	Port Number																										Status	Active
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26		
1	XConnect	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☑	☐	☐	☐	☐	Enabled	Apply
2		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Disabled	Apply
3		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Disabled	Apply
4		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Disabled	Apply
5		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Disabled	Apply
6		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Disabled	Apply

Note: It is only valid to set up at most 8 member ports of any one trunk group and a port can be a member of only one trunk group at a time.

The switch module supports up to six trunk groups. Trunks are groups of ports that are banded together to form a single, logical, high-bandwidth data pipe.

You can change the following parameters:

- **Name**—Type the user-assigned name of the trunk group.
- **Port Numbers**—Check the number of ports that will be members of the trunk group.
- **Status**—Choose to enable or disable the trunk group.

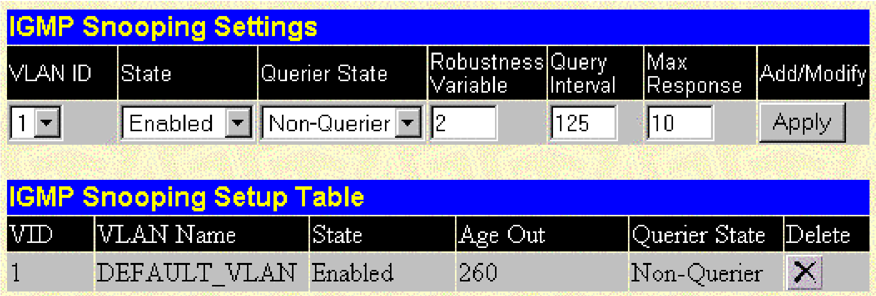
To create or modify a trunk group:

1. Type a name in the **Name** field.
2. Check the ports that will compose the port trunk.
3. Change the **Status** field to **Enabled**.
4. Click **Apply.**

NOTE: To save the configuration settings permanently, you must enter them into the NVRAM using the **Save Changes** option on the **Maintenance** menu. See the section, "Saving Changes," earlier in this chapter.

Configuring IGMP Snooping

When you select **IGMP Snooping** from the **Configuration** menu, the following screen is displayed.



IGMP Snooping Settings

VLAN ID	State	Querier State	Robustness Variable	Query Interval	Max Response	Add/Modify
1	Enabled	Non-Querier	2	125	10	Apply

IGMP Snooping Setup Table

VID	VLAN Name	State	Age Out	Querier State	Delete
1	DEFAULT_VLAN	Enabled	260	Non-Querier	☒

Internet Group Management Protocol (IGMP) Snooping allows the switch module to recognize IGMP queries and reports sent between network stations or devices and an IGMP host. When enabled for IGMP Snooping, the switch module can open or close a port to a specific device based on IGMP messages passing through the switch module.

You can change the following parameters:

- **VLAN ID**—Select a VLAN ID number in this field.
- **State**—Choose to enable or disable the IGMP settings.
- **Querier State**—Select the IGMP version that will be used by the IGMP interface when making queries. Select from **Non-Querier, V1-Querier,** and **V2-Querier.**
- **Robustness Variable**—This is a tuning variable that allows you to configure the acceptable number of packets that may be lost. Type a value between 1 and 255, with larger values being specified for subnets that are expected to lose larger numbers of packets.
- **Query Interval**—Type a value between 1 and 65,500 seconds to specify the length of time between sending IGMP queries. The default is 125 seconds.
- **Max Response**—Type the maximum amount of time allowed before sending an IGMP response report. The range is 1 to 25 seconds.

To set up IGMP Snooping:

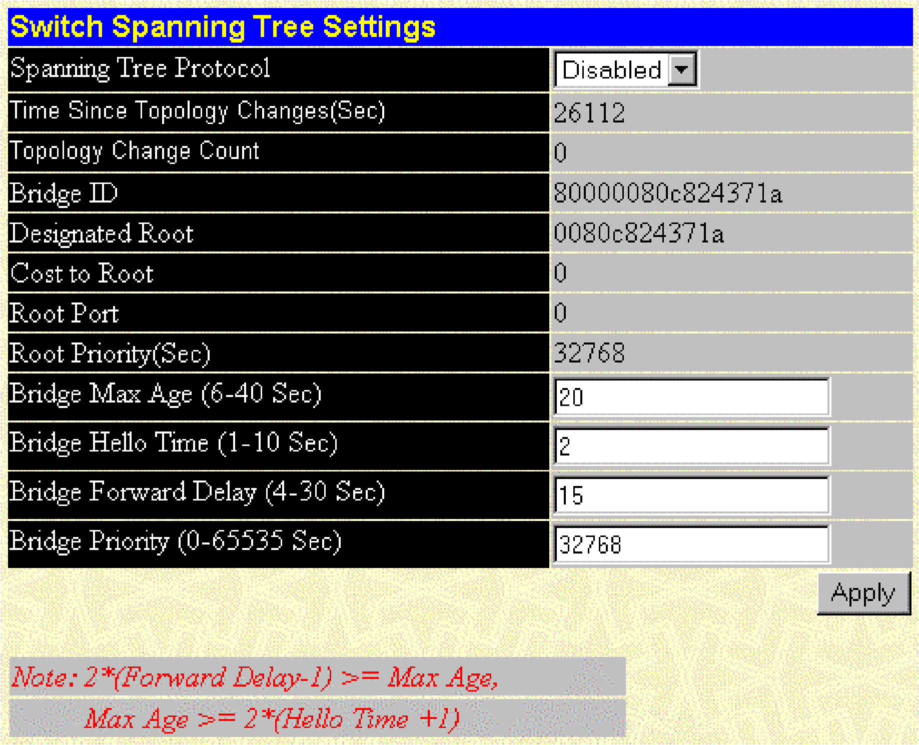
1. Type a VLAN ID number in the **VLAN ID** field.
2. Select **Enabled** in the **State** field.
3. Select the desired setting in the **Querier State** field. This setting determines the version of IGMP that is used in your network.
4. Type a value between 1 and 255 in the **Robustness Variable** field. The default is 2.
5. Type a value between 1 and 65,500 seconds in the **Query Interval** field. This setting sets the time between IGMP queries.
6. Type a value between 1 and 25 seconds in the **Max Response** field. This setting specifies the maximum amount of time allowed before sending a response report.
7. Click **Apply.**

NOTE: To save the configuration settings permanently, you must enter them into the NVRAM using the **Save Changes** option on the **Maintenance** menu. See the section, “Saving Changes,” earlier in this chapter.

Configuring Spanning Tree Protocol Switch Module Settings

The switch module supports 801.2d Spanning Tree Protocol (STP), which allows you to create alternative paths (with multiple switches or other types of bridges) in your network.

When you select **STP Switch Settings** from the **Spanning Tree** menu, the following screen is displayed.



Switch Spanning Tree Settings

Spanning Tree Protocol	Disabled ▾
Time Since Topology Changes(Sec)	26112
Topology Change Count	0
Bridge ID	80000080c824371a
Designated Root	0080c824371a
Cost to Root	0
Root Port	0
Root Priority(Sec)	32768
Bridge Max Age (6-40 Sec)	20
Bridge Hello Time (1-10 Sec)	2
Bridge Forward Delay (4-30 Sec)	15
Bridge Priority (0-65535 Sec)	32768

Note: 2(Forward Delay-1) >= Max Age,*
Max Age >= 2(Hello Time +1)*

You can change the following Spanning Tree parameters:

- **Spanning Tree Protocol**—Choose to enable or disable the STP setting.
- **Bridge Max Age (6–40 Sec)**—Type in the maximum age. The range is 6 to 40 seconds. When the maximum age is reached, if a Bridge Protocol Data Unit (BPDU) has still not been received from the Root bridge, your switch module will start sending its own BPDU to all other switches for permission to become the Root Bridge. If your switch module has the lowest bridge identifier, it will become the Root bridge.
- **Bridge Hello Time (1–10 Sec)**—Type in the hello time. The range is 1 to 10 seconds. This time is the interval between two transmissions of BPDU packets sent by the Root bridge to tell all other switches that it is indeed the Root bridge. If you set a hello time for your switch module and it is not the Root bridge, the default hello time will be used until your switch module becomes the Root bridge.

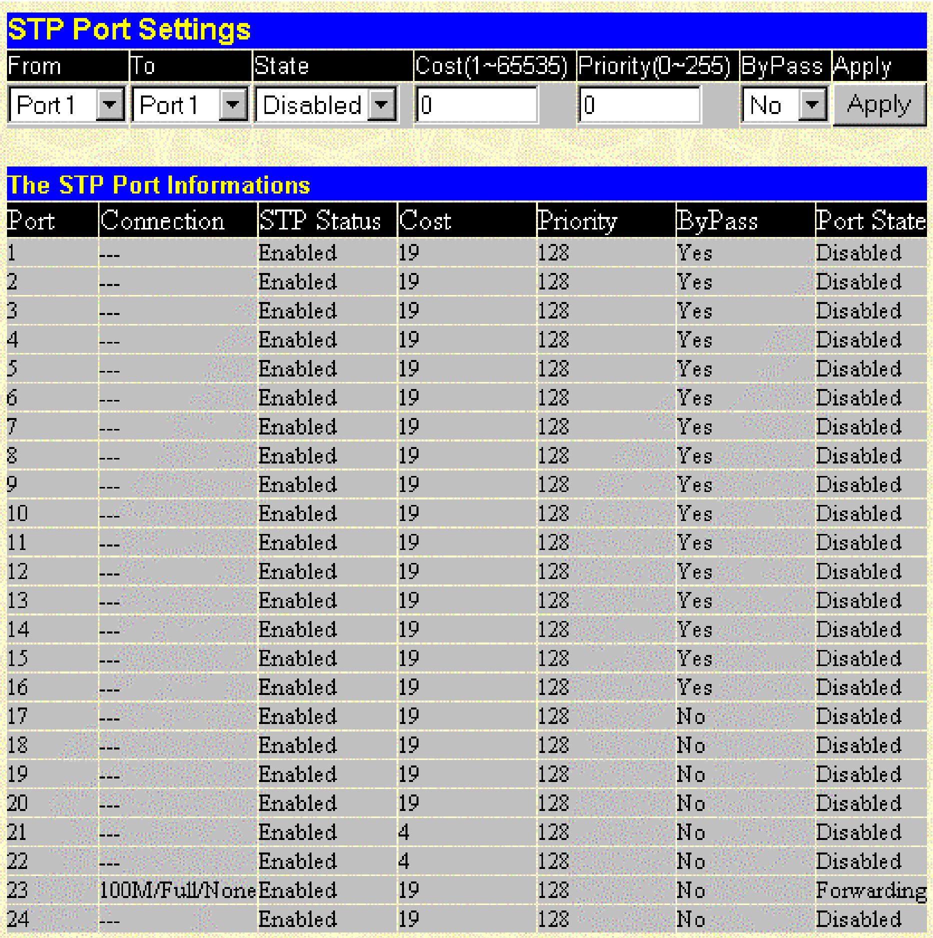
- **Bridge Forward Delay (4–30 Sec)**—Type in the forward delay time. The range is 4 to 30 seconds. This interval is the time any port on the switch module spends in the listening state while moving from the blocking state to the forwarding state.
- **Bridge Priority (0–65535 Sec)**—Type in the bridge priority. The range is from 0 to 65,535. Zero is equal to the highest bridge priority.

Click **Apply** after making changes to the settings.

NOTE: To save the configuration settings permanently, you must enter them into the NVRAM using the **Save Changes** option on the **Maintenance** menu. See the section, “Saving Changes,” earlier in this chapter.

Configuring Spanning Tree Protocol Port Settings

When you select **STP Port Settings** from the **Spanning Tree** menu, the following screen is displayed.



STP Port Settings

From	To	State	Cost(1~65535)	Priority(0~255)	ByPass	Apply
Port 1	Port 1	Disabled	0	0	No	Apply

The STP Port Informations

Port	Connection	STP Status	Cost	Priority	ByPass	Port State
1	---	Enabled	19	128	Yes	Disabled
2	---	Enabled	19	128	Yes	Disabled
3	---	Enabled	19	128	Yes	Disabled
4	---	Enabled	19	128	Yes	Disabled
5	---	Enabled	19	128	Yes	Disabled
6	---	Enabled	19	128	Yes	Disabled
7	---	Enabled	19	128	Yes	Disabled
8	---	Enabled	19	128	Yes	Disabled
9	---	Enabled	19	128	Yes	Disabled
10	---	Enabled	19	128	Yes	Disabled
11	---	Enabled	19	128	Yes	Disabled
12	---	Enabled	19	128	Yes	Disabled
13	---	Enabled	19	128	Yes	Disabled
14	---	Enabled	19	128	Yes	Disabled
15	---	Enabled	19	128	Yes	Disabled
16	---	Enabled	19	128	Yes	Disabled
17	---	Enabled	19	128	No	Disabled
18	---	Enabled	19	128	No	Disabled
19	---	Enabled	19	128	No	Disabled
20	---	Enabled	19	128	No	Disabled
21	---	Enabled	4	128	No	Disabled
22	---	Enabled	4	128	No	Disabled
23	100M/Full/None	Enabled	19	128	No	Forwarding
24	---	Enabled	19	128	No	Disabled

The **STP Port Settings** window allows you to configure Spanning Tree Protocol functions for individual ports.

You can change the following parameters:

- **From**—Select the first port to be configured.
- **To**—Select the last port to be configured.
- **State**—Choose the STP state for the port, either **Enabled** or **Disabled.**
- **Cost (1–65535)**—Type a port cost between 1 and 65,535. The lower the cost, the greater the probability that the port will be chosen as the designated port (chosen to forward packets).
- **Priority (0–255)**—Type a port priority between 0 to 255. The lower the priority, the greater the probability that the port will be chosen as the root port.
- **Bypass**—Choose **Yes** or **No.** The bypass sets the forward delay timer to zero, thus bypassing the waiting time before the listening state. (This procedure is also known as fast forward.)

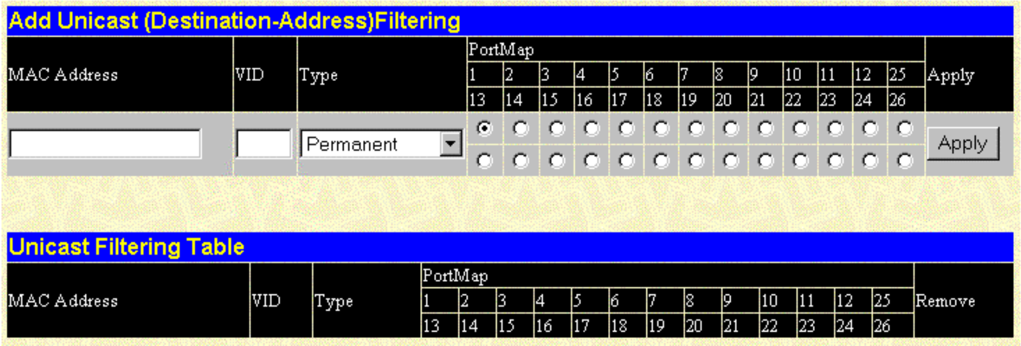
Click **Apply** after making changes to the settings.

NOTE: To save the configuration settings permanently, you must enter them into the NVRAM using the **Save Changes** option on the **Maintenance** menu. See the section, “Saving Changes,” earlier in this chapter.

Configuring Unicast Filtering

The **Static Filtering Table** menu allows you to change the parameters for unicast filtering and multicast filtering.

When you select **Unicast Filtering** from the **Static Filtering Table** menu, the following screen is displayed.



The **Add Unicast Filtering** window allows you to set up static packet filtering on the switch module.

You can change the following parameters:

- **MAC Address**—Type the MAC address from which packets will be statically filtered.
- **VID**—Type the VLAN ID number of the VLAN to which the MAC address belongs.

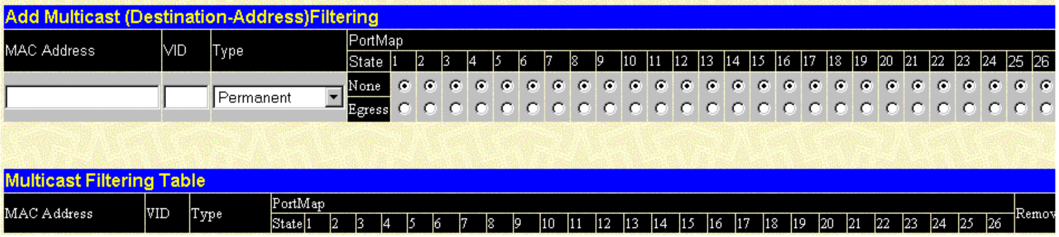
- **Type**—Choose the filter type, either **Permanent** or **DeleteOnReset.**
- **Port Map**—Select the port on which the MAC address resides.

Click **Apply** after making changes to the settings.

NOTE: To save the configuration settings permanently, you must enter them into the NVRAM using the **Save Changes** option on the **Maintenance** menu. See the section, “Saving Changes,” earlier in this chapter.

Configuring Multicast Filtering

When you select **Multicast Filtering** from the **Static Filtering Table** menu, the following screen is displayed.



Add Multicast (Destination-Address)Filtering

MAC Address	VID	Type	PortMap																									
			State	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
		Permanent	None	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
			Egress	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Multicast Filtering Table

MAC Address	VID	Type	PortMap																										Remov
			State	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	

The **Add Multicast Filtering** window allows you to set up multicast filtering on the switch module.

You can change the following parameters:

- **MAC Address**—Type the MAC address of the static source of multicast packets.
- **VID**—Type the VLAN ID number of the VLAN to which the MAC address belongs.
- **Type**—Choose the filter type, either **Permanent** or **DeleteOnReset.**
- **Port Map**—Select the ports that will be members of the static multicast group and ports that have no restrictions from joining dynamically.

Click **Apply** after making changes to the settings.

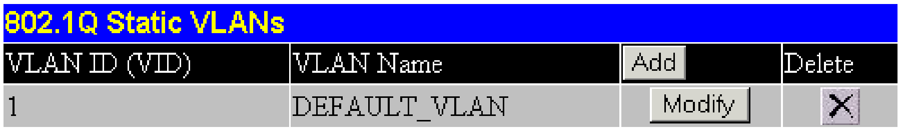
NOTE: To save the configuration settings permanently, you must enter them into the NVRAM using the **Save Changes** option on the **Maintenance** menu. See the section, “Saving Changes,” earlier in this chapter.

Configuring the Static VLAN Entry

The **VLAN** menu allows you to configure the following:

- Static VLAN entry
- Port VLAN ID (PVID)

When you select **Static VLAN Entry** from the **VLAN** menu, the following screen is displayed.

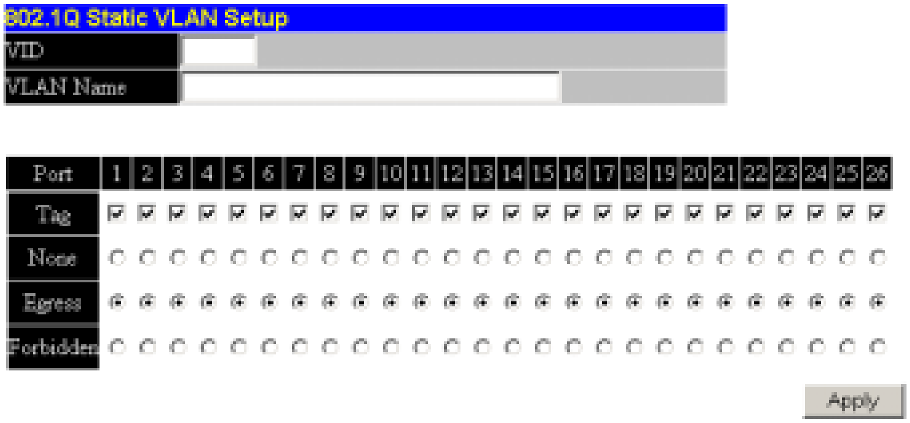


802.1Q Static VLANs

VLAN ID (VID)	VLAN Name	Add	Delete
1	DEFAULT_VLAN	Modify	☒

The **802.1Q Static VLANs** window allows you to add, modify, or delete entries to the 802.1Q Static VLAN table.

To add an entry to this table, click **Add** and then fill in the appropriate information in the following window. To modify an entry, click **Modify** beside the appropriate VID. To delete an entry, click the icon in the **Delete** column beside the appropriate VID.



802.1Q Static VLAN Setup

VID

VLAN Name

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Tag	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
None	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Egress	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Forbidden	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

The **802.1Q Static VLAN Setup** window allows you to change the following parameters for each VLAN ID (VID):

- **VID**—Allows you to type the VLAN ID number of the VLAN you want to add. The range is 1-4094. This field is grayed out in the modify mode.
- **VLAN Name**—Allows you to type the name of the VLAN that is being created.
- **Tag**—Specifies the port as either 802.1Q tagging or 802.1Q untagging. Select the check box to designate the port as tagging.
- **None**—Allows you to click the radio button to specify the port as not being a static member of the VLAN, but with no restrictions for joining the VLAN dynamically through GVRP.
- **Egress**—Allows you to click the radio button to specify the port as being a static member of the VLAN. Egress member ports are ports that will be transmitting traffic for the VLAN.
- **Forbidden**—Specifies the port as not being a member of the VLAN and that the port is forbidden from becoming a member of the VLAN dynamically.

To configure an 802.1Q static VLAN entry:

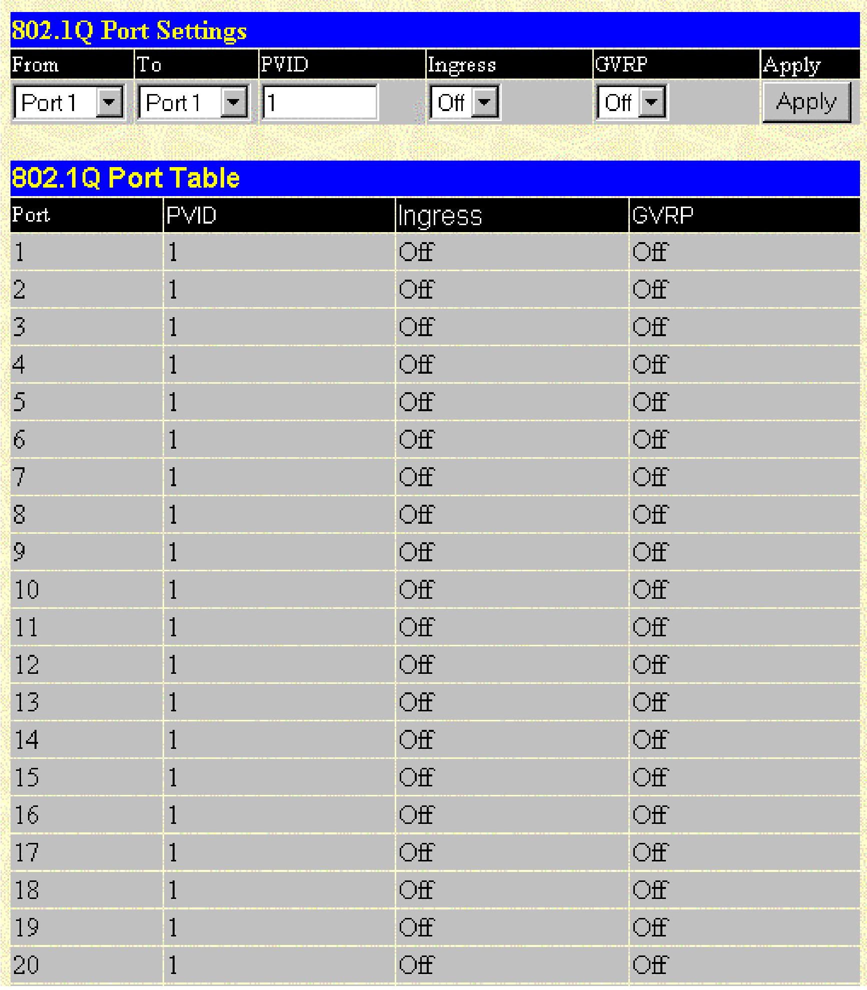
1. Type the VLAN ID number in the **VID** field.

2. Type the VLAN name in the **VLAN Name** field.
3. Select the **Tag** check box if you want a member port to be a tagging port. Leave it unselected if you do not want it to be a tagging port.
4. Select **None** if you do not want a port to belong to the VLAN, or select **Egress** to statically set a port to belong to a VLAN. Select **Forbidden** if you do not want a port to become a member of the VLAN dynamically.
5. Click **Apply** to let the changes take effect.

NOTE: To save the configuration settings permanently, you must enter them into the NVRAM using the **Save Changes** option on the **Maintenance** menu. See the section, “Saving Changes,” earlier in this chapter.

Configuring the Port VLAN ID

When you select **Port VLAN ID (PVID)** from the **VLANs** menu, the following screen is displayed.



802.1Q Port Settings

From	To	PVID	Ingress	GVRP	Apply
Port 1	Port 1	1	Off	Off	Apply

802.1Q Port Table

Port	PVID	Ingress	GVRP
1	1	Off	Off
2	1	Off	Off
3	1	Off	Off
4	1	Off	Off
5	1	Off	Off
6	1	Off	Off
7	1	Off	Off
8	1	Off	Off
9	1	Off	Off
10	1	Off	Off
11	1	Off	Off
12	1	Off	Off
13	1	Off	Off
14	1	Off	Off
15	1	Off	Off
16	1	Off	Off
17	1	Off	Off
18	1	Off	Off
19	1	Off	Off
20	1	Off	Off

The **802.1Q Port Settings** window allows you to assign a Port VLAN ID (PVID) number, enable or disable the ingress filtering check, and enable or disable GVRP for individual ports.

Ingress filtering means that a receiving port will check to see if it is a member of the VLAN ID in the packet before forwarding the packet.

GARP VLAN Registration Protocol (GVRP) is a Generic Attribute Registration Protocol (GARP) application that provides 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports. With GVRP, the switch module can exchange VLAN configuration information with other GVRP switches, prune unnecessary broadcast and unknown unicast traffic, and dynamically create and manage VLANs on switches connected through 802.1Q trunk ports.

You can change the following parameters:

- **From** and **To**—Select the range of ports in the **From** and **To** fields.

- **PVID**—Type the PVID. This tuning variable allows for sub-networks that are expected to lose a large number of packets. The PVID is used by the port to tag outgoing, untagged packets, and to make filtering decisions about incoming packets. If the port is specified as tagging, and an untagged packet is forwarded to the port for transmission, the port will add an 802.1Q tag using the PVID to write the VID in the tag.

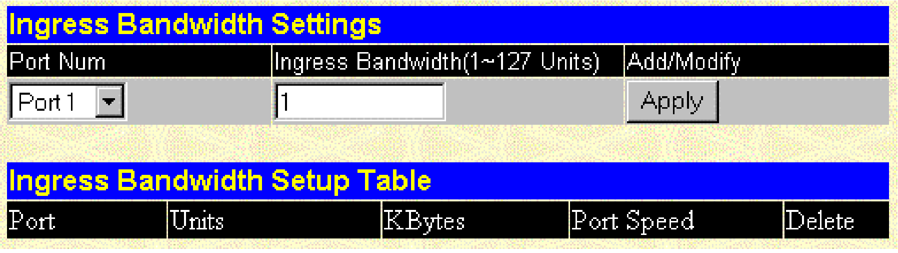
  When the packet arrives at its destination, the receiving device will use the PVID to make VLAN forwarding decisions. If a packet is received by the port, and ingress filtering is enabled, the port will compare the VID of the incoming packet to its PVID. If the two are unequal, the port will drop the packet. If the two are equal, the port will receive the packet.
- **Ingress Filter**—Choose **Off** or **On** to specify the port that checks the VID of incoming packets against its VID or PVID. If the two are equal, the port will receive the packet. It the two are unequal, the port will drop the packet. This setting is used to limit traffic to a single VLAN.
- **GVRP**—Choose **Off** or **On** to enable or disable GARP VLAN Registration Protocol.

Click **Apply** after making changes to the settings.

NOTE: To save the configuration settings permanently, you must enter them into the NVRAM using the **Save Changes** option on the **Maintenance** menu. See the section, “Saving Changes,” earlier in this chapter.

Configuring the Restart Ingress Bandwidth Settings

When you select **Restart Ingress Bandwidth** from the **Port Bandwidth** menu, the following screens are displayed.



Ingress Bandwidth Settings

Port Num	Ingress Bandwidth(1~127 Units)	Add/Modify
Port 1	1	Apply

Ingress Bandwidth Setup Table

Port	Units	KBytes	Port Speed	Delete

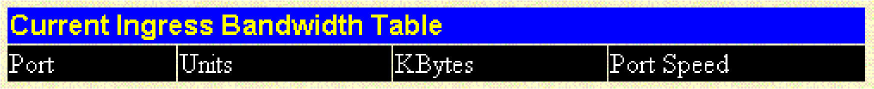
To configure ingress bandwidth for a specific port:

1. Select the desired port in the **Port Num** field.
2. Type a number between 1 and 127 in the **Ingress Bandwidth (1–127 Units)** field.
3. Click **Apply.**
4. Select **Restart System** from the **Maintenance** menu.
5. Select **Yes** to save the settings.
6. Click **Restart.** The system reboots and saves your settings.

NOTE: To delete an entry, click the **Delete** icon on the **Ingress Bandwidth Setup Table.**

Displaying the Current Ingress Bandwidth Table

When you select **Current Ingress Bandwidth** from the **Port Bandwidth** menu, the following screen is displayed.



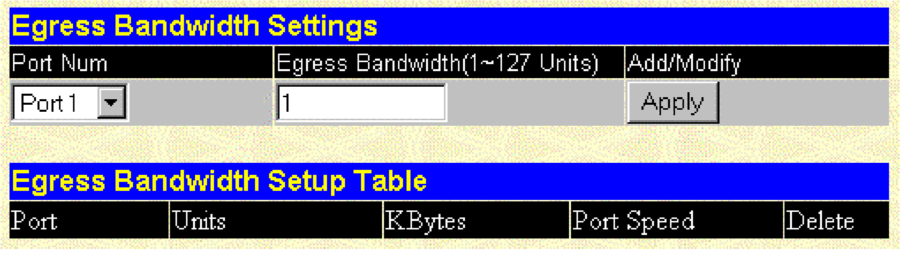
Current Ingress Bandwidth Table

Port	Units	KBytes	Port Speed

Current Ingress Bandwidth Table is a read-only screen displaying current ingress bandwidth information.

Configuring the Restart Egress Bandwidth Settings

When you select **Restart Egress Bandwidth** from the **Port Bandwidth** menu, the following screen is displayed.



Egress Bandwidth Settings

Port Num	Egress Bandwidth(1~127 Units)	Add/Modify
Port 1	1	Apply

Egress Bandwidth Setup Table

Port	Units	KBytes	Port Speed	Delete

To configure egress bandwidth for a specific port:

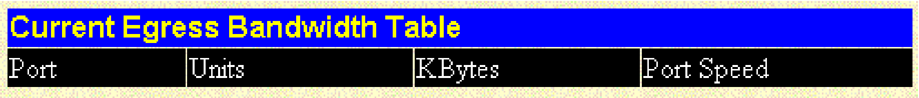
1. Select the desired port under **Port Num.**
2. Type a number between 1 and 127 in the **Egress Bandwidth (1–127 Units)** field.
3. Click **Apply** to save the change or addition.
4. Select **Restart System** from the **Maintenance** menu.

5. Select **Yes** to save the settings.
6. Click **Restart.** The system reboots and saves your settings.

NOTE: To delete an entry, click the **Delete** icon on the **Egress Bandwidth Setup Table.**

Displaying the Current Egress Bandwidth Table

When you select **Current Egress Bandwidth** from the **Port Bandwidth** menu, the following screen is displayed.



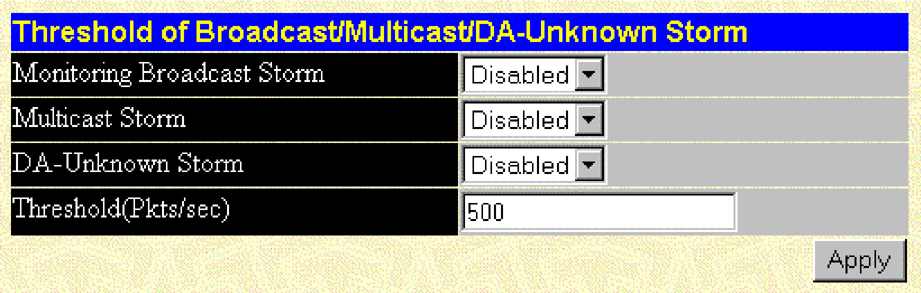
Current Egress Bandwidth Table

Port	Units	KBytes	Port Speed

Current Egress Bandwidth Table is a read-only screen displaying current egress bandwidth information.

Configuring the Threshold of Broadcast

When you select **Threshold of Broadcast** from the **Configuration** menu, the following screen is displayed.



Threshold of Broadcast/Multicast/DA-Unknown Storm

Monitoring Broadcast Storm	Disabled
Multicast Storm	Disabled
DA-Unknown Storm	Disabled
Threshold(Pkts/sec)	500

The switch module allows you to set the threshold for three types of storms: broadcast, multicast, and one where the destination address is unknown. The higher the threshold, the more packets the switch module can accept per second. If the threshold is exceeded, any additional packets received are dropped. Entering a low value means packets have a greater chance to exceed the threshold and be dropped from the switch module.

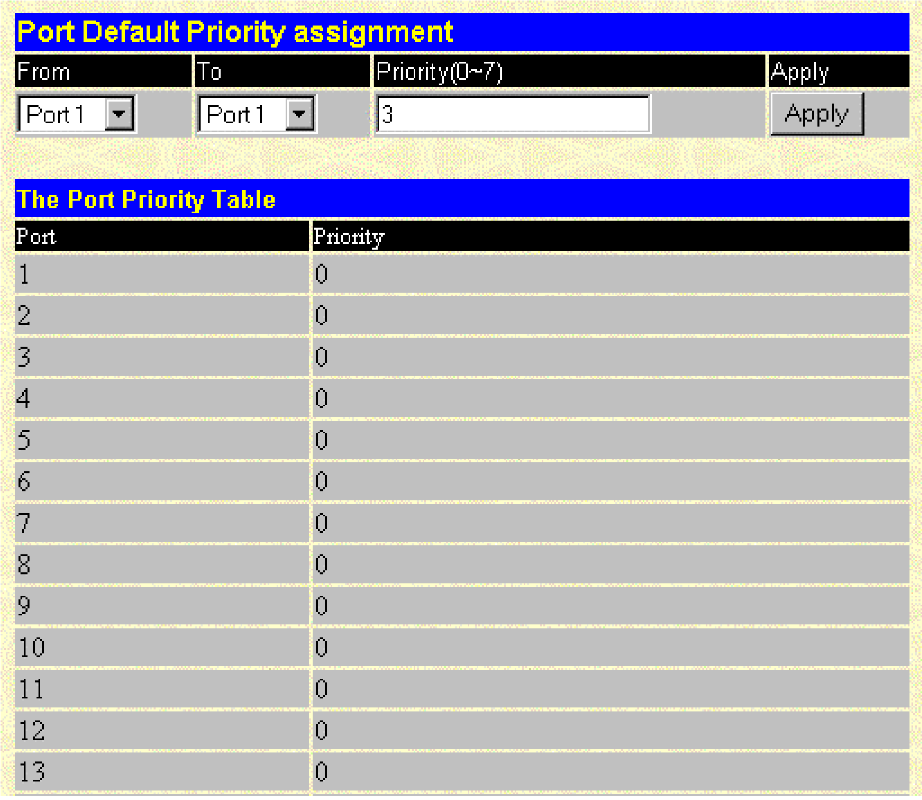
To set a threshold:

1. Choose **Enabled** for the appropriate option.
2. Type a threshold value in the **Threshold(Pkts/sec)** field.
3. Click **Apply** to save the changes.

NOTE: To save the configuration settings permanently, you must enter them into the NVRAM using the **Save Changes** option on the **Maintenance** menu. See the section, “Saving Changes,” earlier in this chapter.

Configuring the Port Priority

When you select **Port Priority** from the **Configuration** menu, the following screen is displayed.



Port Default Priority assignment

From	To	Priority(0~7)	Apply
Port 1	Port 1	3	Apply

The Port Priority Table

Port	Priority
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0

The **Port Default Priority assignment** window allows you to set a default priority for packets that have not already been assigned a priority value.

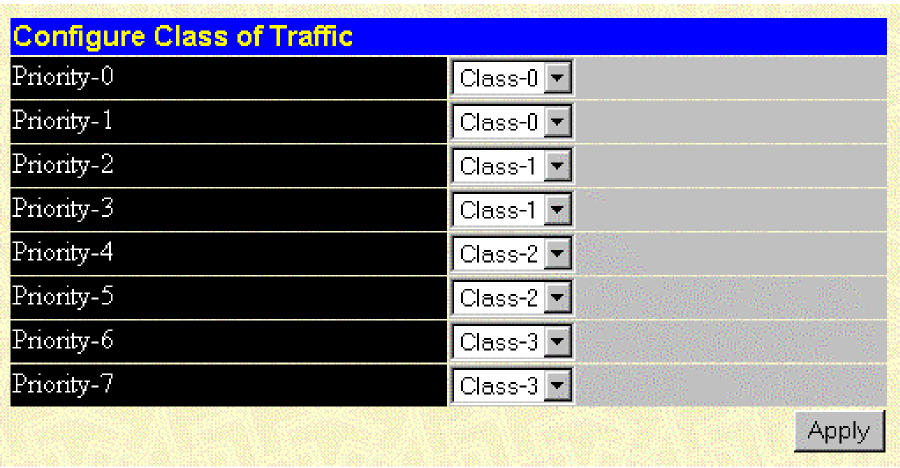
To set a default priority:

1. Select the appropriate port in the **From** and **To** fields.
2. Type the priority in the **Priority (0–7)** field.
3. Click **Apply** to save the changes.

NOTE: To save the configuration settings permanently, you must enter them into the NVRAM using the **Save Changes** option on the **Maintenance** menu. See the section, “Saving Changes,” earlier in this chapter.

Configuring the Class of Traffic

When you select **Class of Traffic** from the **Configuration** menu, the following screen is displayed.



Priority-0	Class-0
Priority-1	Class-0
Priority-2	Class-1
Priority-3	Class-1
Priority-4	Class-2
Priority-5	Class-2
Priority-6	Class-3
Priority-7	Class-3

The **Configure Class of Traffic** window allows you to configure traffic class priority by specifying the class value, from 0 to 3, of the switch module's eight levels of priority.

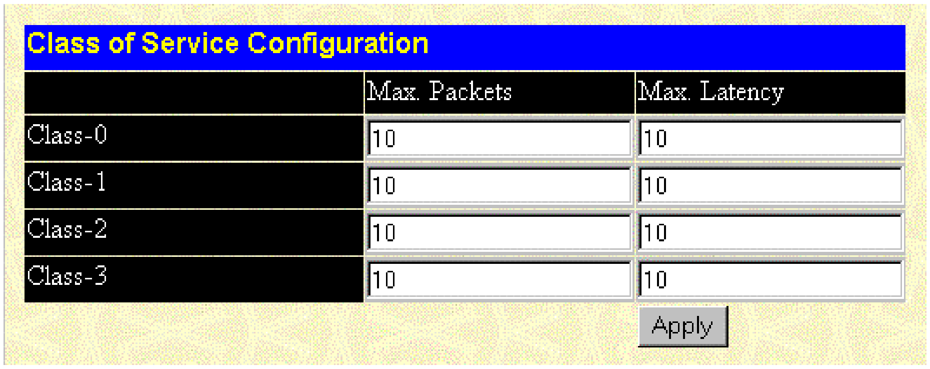
To set traffic class priority:

1. Select the class value for each priority.
2. Click **Apply** to save the changes.

NOTE: To save the configuration settings permanently, you must enter them into the NVRAM using the **Save Changes** option on the **Maintenance** menu. See the section, "Saving Changes," earlier in this chapter.

Configuring the Class of Service

When you select **Class of Service** from the **Configuration** menu, the following screen is displayed.



Class of Service Configuration

	Max. Packets	Max. Latency
Class-0	10	10
Class-1	10	10
Class-2	10	10
Class-3	10	10

The **Class of Service Configuration** window allows you to set the maximum number of packets and the maximum allowable time a packet stays in the CoS queue.

You can change the following parameters:

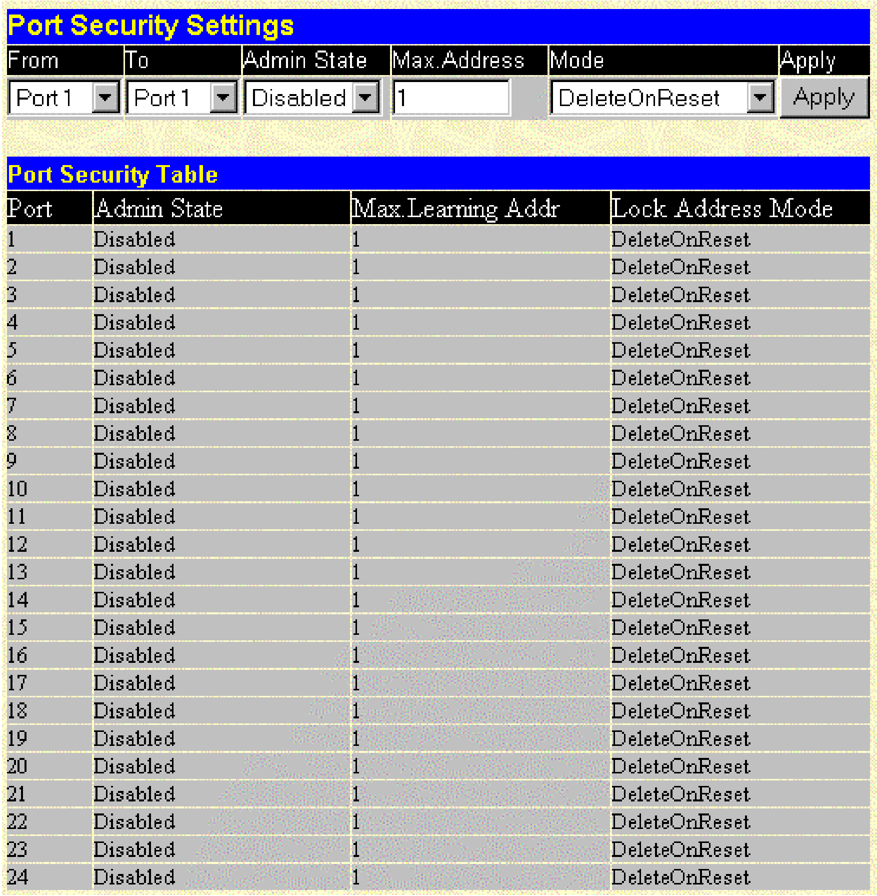
- **Max. Packets**—Type a value between 0 and 255. The Class of Service scheduling algorithm starts from the highest CoS for a given port, sends the maximum number of packets, then moves on to the next lower CoS. Entering zero instructs the switch module to continue processing packets until there are no more packets in the CoS transaction queue.
- **Max. Latency**—Type the maximum allowable time a packet stays in the CoS queue. The packets in this queue are not delayed more than the maximum allowable latency entered in this field. The timer is disabled when this field is set to zero. Each unit of this timer is equal to 17 microseconds.

Click **Apply** after making changes to the settings.

NOTE: To save the configuration settings permanently, you must enter them into the NVRAM using the **Save Changes** option on the **Maintenance** menu. See the section, “Saving Changes,” earlier in this chapter.

Configuring Port Security

When you select **Port Security** from the **Configuration** menu, the following screen is displayed.



Port Security Settings

From	To	Admin State	Max.Address	Mode	Apply
Port 1	Port 1	Disabled	1	DeleteOnReset	Apply

Port Security Table

Port	Admin State	Max.Learning Addr	Lock Address Mode
1	Disabled	1	DeleteOnReset
2	Disabled	1	DeleteOnReset
3	Disabled	1	DeleteOnReset
4	Disabled	1	DeleteOnReset
5	Disabled	1	DeleteOnReset
6	Disabled	1	DeleteOnReset
7	Disabled	1	DeleteOnReset
8	Disabled	1	DeleteOnReset
9	Disabled	1	DeleteOnReset
10	Disabled	1	DeleteOnReset
11	Disabled	1	DeleteOnReset
12	Disabled	1	DeleteOnReset
13	Disabled	1	DeleteOnReset
14	Disabled	1	DeleteOnReset
15	Disabled	1	DeleteOnReset
16	Disabled	1	DeleteOnReset
17	Disabled	1	DeleteOnReset
18	Disabled	1	DeleteOnReset
19	Disabled	1	DeleteOnReset
20	Disabled	1	DeleteOnReset
21	Disabled	1	DeleteOnReset
22	Disabled	1	DeleteOnReset
23	Disabled	1	DeleteOnReset
24	Disabled	1	DeleteOnReset

The Port Security Settings window is used to set up security for a port or a range of ports.

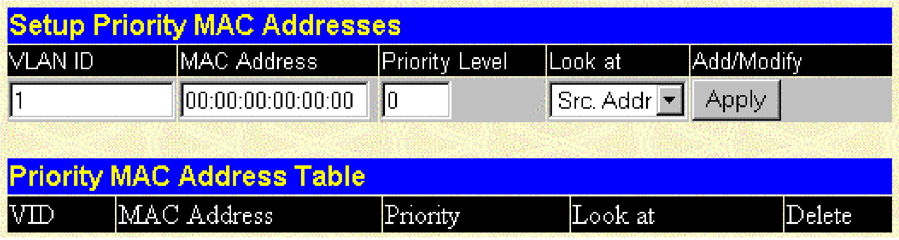
To set up security for a port or ports:

1. Select the range of ports in the **From** and **To** fields.
2. Choose **Enabled** in the **Admin State** field.
3. Type the maximum number of addresses in **Max. Address** field.
4. Select the **Mode** that you want.
5. Click **Apply** to apply your settings.

NOTE: To save the configuration settings permanently, you must enter them into the NVRAM using the **Save Changes** option on the **Maintenance** menu. See the section, “Saving Changes,” earlier in this chapter.

Configuring Priority MAC Addresses

When you select **Priority MAC Addresses** from the **Configuration** menu, the following screens are displayed.



Setup Priority MAC Addresses

VLAN ID	MAC Address	Priority Level	Look at	Add/Modify
1	00:00:00:00:00:00	0	Src. Addr	Apply

Priority MAC Address Table

VID	MAC Address	Priority	Look at	Delete

The **Setup Priority MAC Address** window allows you to set up the priority, between 0 and 7 with 0 being the highest, for a specified MAC address.

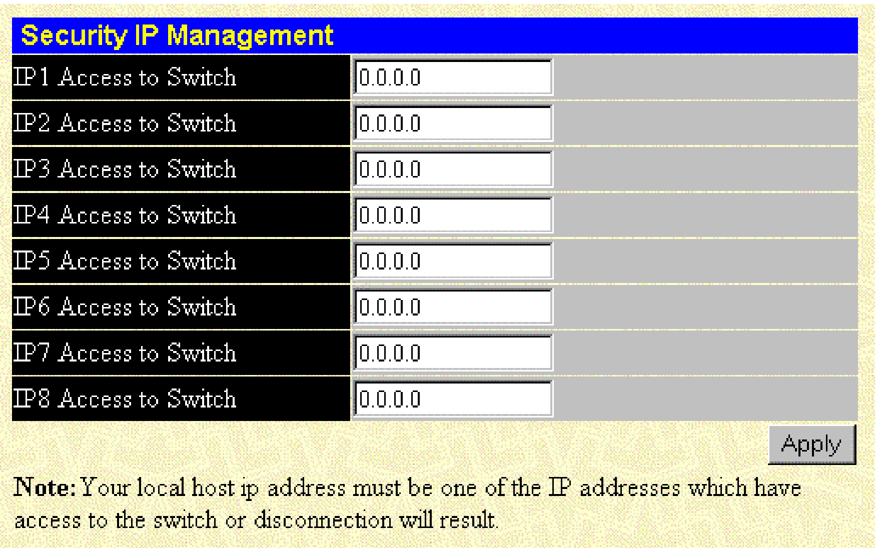
To set the priority level for a MAC address:

1. Type the VLAN ID in the **VLAN ID** field.
2. Type the MAC address for which priority on the switch module is to be established in the **MAC Address** field.
3. Type the priority level for the MAC address in the **Priority Level** field. The range is from 0 to 7, with 0 being the highest priority.
4. Select the state under which the above priority will be active in the **Look at** field. The options are:
    a. **Dst.Addr**—Packets with the selected MAC address as their destination will be given the selected priority.
    b. **Src.Addr**—Packets with the selected MAC address as their source will be given the selected priority.
    c. **Either**—All packets with the selected MAC address will be given the selected priority.
5. Click **Apply** to apply the changes.

NOTE: To save the configuration settings permanently, you must enter them into the NVRAM using the **Save Changes** option on the **Maintenance** menu. See the section, “Saving Changes,” earlier in this chapter.

Configuring the Security IP

When you select **Security IP** from the **Management** menu, the following screen is displayed.



Security IP Management

IP1 Access to Switch	0.0.0.0
IP2 Access to Switch	0.0.0.0
IP3 Access to Switch	0.0.0.0
IP4 Access to Switch	0.0.0.0
IP5 Access to Switch	0.0.0.0
IP6 Access to Switch	0.0.0.0
IP7 Access to Switch	0.0.0.0
IP8 Access to Switch	0.0.0.0

Note: Your local host ip address must be one of the IP addresses which have access to the switch or disconnection will result.

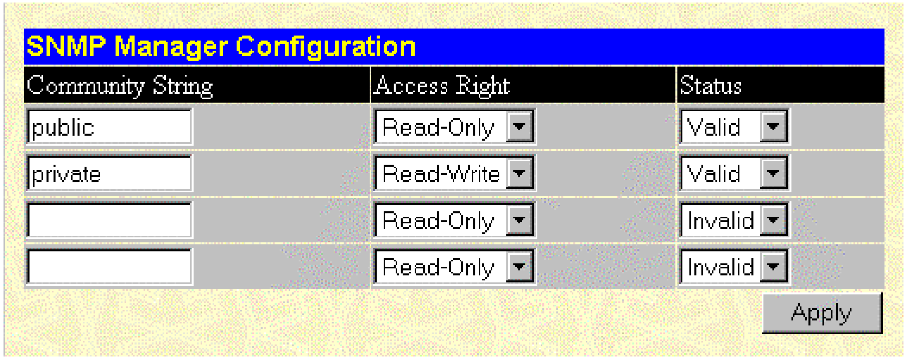
The **Security IP Management** window allows you to specify IP addresses that are allowed to access the switch module.

To specify which IP addresses are allowed to access the switch module:

1. Type the appropriate IP address.
2. Click **Apply.**

Configuring the SNMP Manager

When you select **SNMP Manager** from the **Management** menu, the following screen is displayed.



SNMP Manager Configuration

Community String	Access Right	Status
public	Read-Only	Valid
private	Read-Write	Valid
	Read-Only	Invalid
	Read-Only	Invalid

The **SNMP Manager Configuration** window allows you to configure SNMP parameters.

You can change the following parameters:

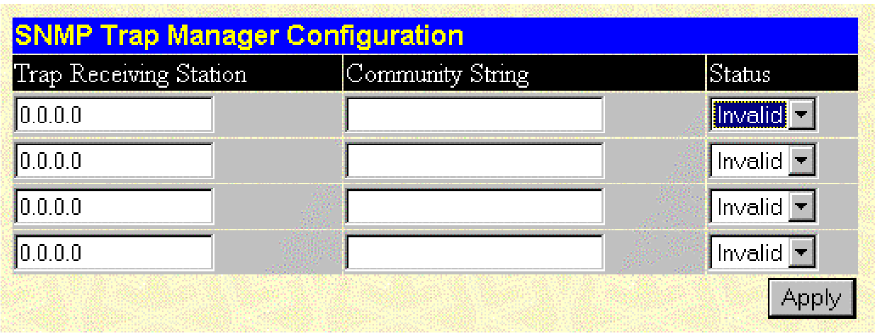
- **Community String**—Type a user-defined SNMP community name.
- **Access Right**—Choose the access **Read-Only** or **Read-Write** using the SNMP community name.
- **Status**—Set the status of the current community string to **Valid** or **Invalid.**

Click **Apply** after making changes to the settings.

NOTE: To save the configuration settings permanently, you must enter them into the NVRAM using the **Save Changes** option on the **Maintenance** menu. See the section, "Saving Changes," earlier in this chapter.

Configuring the Trap Manager

When you select **Trap Manager** from the **Management** menu, the following screen is displayed.



SNMP Trap Manager Configuration

Trap Receiving Station	Community String	Status
0.0.0.0		Invalid
0.0.0.0		Invalid
0.0.0.0		Invalid
0.0.0.0		Invalid

The SNMP **Trap Manager Configuration** window allows you to set the trap receiving station, which runs a network management application to receive and store traps.

You can change the following parameters:

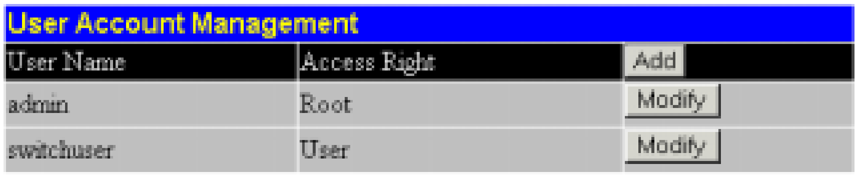
- **Trap Receiving Station**—Type the IP address of the trap receiving station.
- **Community String**—Type a user-defined SNMP community name.
- **Status**—Set the trap receiving station status to **Valid** or **Invalid.**

Click **Apply** after making changes to the settings.

NOTE: To save the configuration settings permanently, you must enter them into the NVRAM using the **Save Changes** option on the **Maintenance** menu. See the section, "Saving Changes," earlier in this chapter.

Setting Up and Managing User Accounts

When you select **User Accounts** from the **Management** menu, the following screen is displayed.



User Account Management

User Name	Access Right
admin	Root
switchuser	User

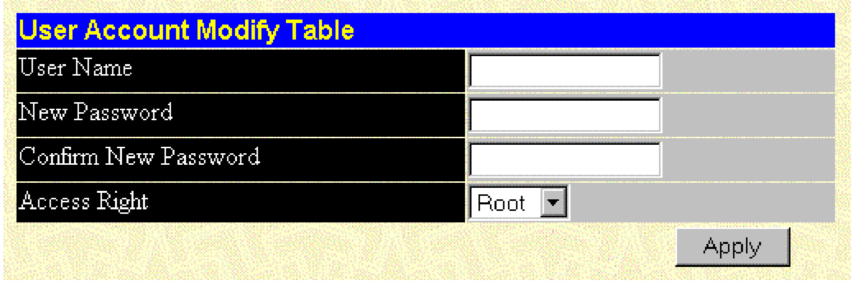
The **User Account Management** window displays all current users for the switch module and their current access level.

The following information is displayed:

- **User Name**—Displays all current users for the switch module.
- **Access Right**—Displays the current access level assigned to each corresponding user. (**User, User+,** or **Root**). A **Root** user has full read/write access, while a **User** has read only access. A **User+** has the same privileges as a **User,** but with the added ability to restart the switch module.
- **Add**—Click this button to add a new user to the table.

The **User Account Modify Table** is displayed.

The **User Account Modify Table** allows you to add or delete user account information.



User Account Modify Table

User Name	
New Password	
Confirm New Password	
Access Right	Root

To add a user account:

1. Type the user name in the **User Name** field.
2. Type the user's password in the **New Password** field.
3. Type the new password a second time in the **Confirm Password** field.

4. Select one of the access levels.

   NOTE: See Table 2-1 in Chapter 2 for an explanation of access rights.

5. Click **Apply**.

   NOTE: To delete a user, click **Delete**.

   NOTE: To save the configuration settings permanently, you must enter them into the NVRAM using the **Save Changes** option on the **Maintenance** menu. See the section, “Saving Changes,” earlier in this chapter.

Monitoring Switch Module Functions

The Monitoring menu has the following sections:

- Port Utilization
- Packets—Received (RX), UMB-cast (RX), Transmitted (TX)
- Errors—(Received (RX) and Transmitted (TX))
- Size (Packet Size)
- Trunk Utilization
- MAC Address Table
- IGMP Snooping Table
- Dynamic Group Registration
- VLAN Status Table

Monitoring the Switch Module using the Active Switch Graphic

At the top of the main page, an active graphic of the switch module displays.

NOTE:

- RJ-45 connectors that are grayed out on the graphic of the current switch module belong to the other switch module.
- Pointing on an RJ-45 connector that belongs to this switch module displays the port number.
- Selecting an RJ-45 connector that belongs to this switch module displays the port statistics.

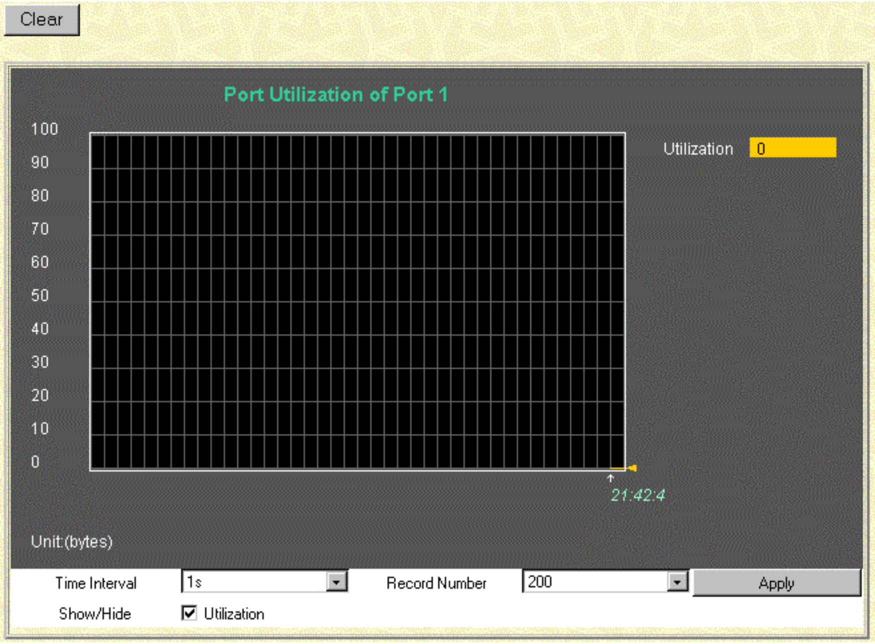
You can monitor the switch module status using the following:

- Graphical LEDs display current link speed and activity.
- RJ-45 connectors labeled 1 through 20 represent NIC 1 (on Switch A) or NIC 2 (on Switch B) of server bays 1 through 20.
- RJ-45 connectors labeled 21 and 22 on Switch A and Switch B represent cross-connect ports.

- RJ-45 connector labeled 23 on Switch A represents the port connected to the Integrated Administrator.
- RJ-45 connector labeled Mgmt represents the Integrated Administrator Management connector (Switch A port 24 – 10/100 Ethernet).
- RJ-45 connectors labeled UpLink1 and UpLink2 represent Gigabit Ethernet Port 25 and Port 26 of the switch module.

Monitoring Port Utilization

When you select **Port Utilization** from the **Monitoring** menu, the following screen is displayed.



Utilization 0

Time Interval 1s

Record Number 200

Show/Hide ☑ Utilization

The **Port Utilization** window shows the percentage of the total available bandwidth being used on a specified port.

The following information is displayed:

- **Utilization**—The percentage of the total bandwidth being used on the specified port.
- **Time Interval**—The frequency at which the information on the screen is refreshed. The default is two seconds.
- **Record Number**—The number of polling attempts. The default is 200.
- **Show/Hide**—Shows or hides the line graph for utilization.

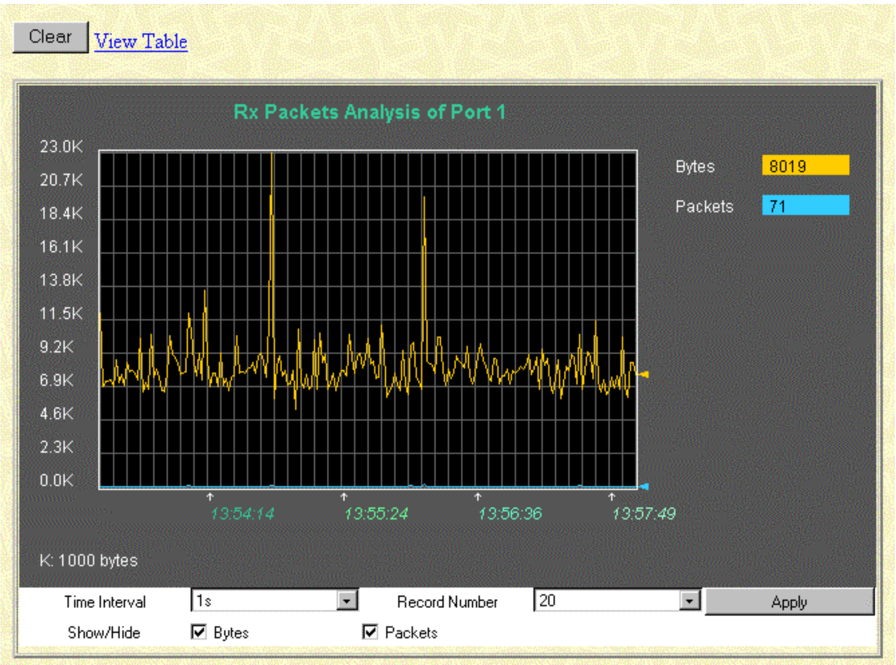
Click **Clear** to reset the counters.

Monitoring Packets

The Web Manager allows various packet statistics to be viewed as either a line graph or a table. You can choose the type of graphic to display by clicking **View Table** or **View Line Chart.**

Monitoring Received (RX) Packets

When you select **Received (RX) Packets** from the **Packets** menu, the following screens are displayed.



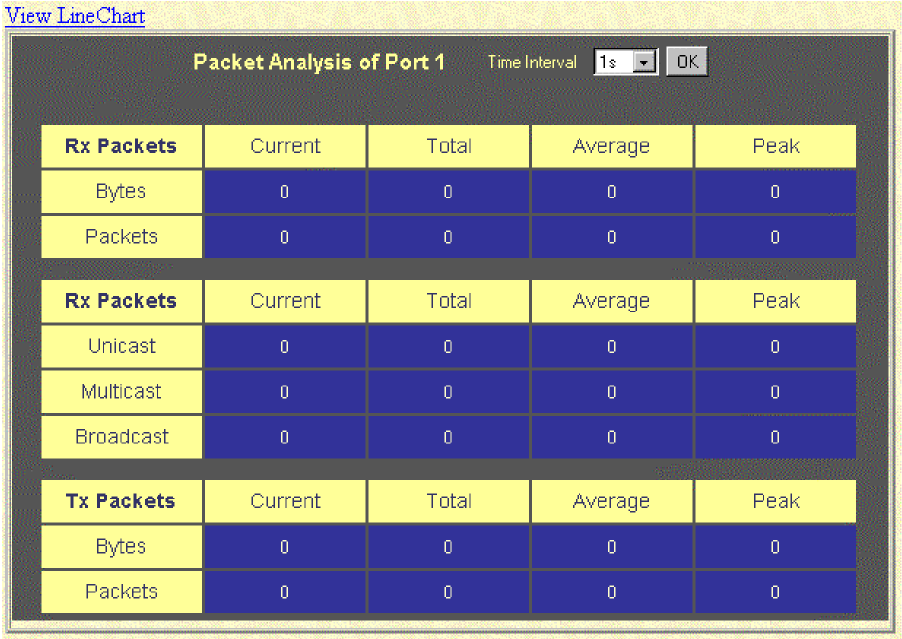
Bytes 8019

Packets 71

Time Interval 1s

Record Number 20

Show/Hide ☑ Bytes ☑ Packets



Packet Analysis of Port 1

Time Interval 1s

Rx Packets	Current	Total	Average	Peak
Bytes	0	0	0	0
Packets	0	0	0	0

Rx Packets	Current	Total	Average	Peak
Unicast	0	0	0	0
Multicast	0	0	0	0
Broadcast	0	0	0	0

Tx Packets	Current	Total	Average	Peak
Bytes	0	0	0	0
Packets	0	0	0	0

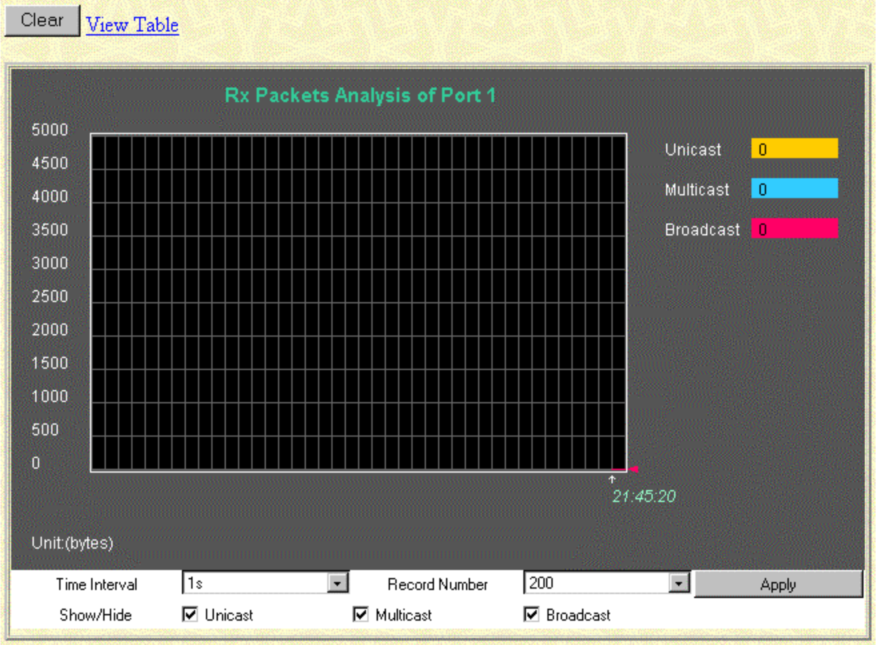
The **Rx Packets Analysis** window displays the number of bytes and packets received on the port.

The following information is displayed:

- **Time Interval**—The frequency at which the information on the screen is refreshed. The setting is between 1s and 60s, where "s" stands for seconds. The default value is one second.
- **Record Number**—Displays the number of times that the switch module will be polled. The setting can be between 20 and 200. The default value is 20.
- **Bytes**—Counts the number of bytes received on the port.
- **Packets**—Counts the number of packets received on the port.
- **Show/Hide**—Displays or hides bytes and packets information.
- **Clear**—Clears all statistics counters on this window.
- **View Table**—Displays a table rather than a line graph.
- **View Line Chart**—Displays a line graph rather than a table.

Monitoring UMB-cast (RX) Packets

When you select **UMB-cast (RX) Packets** from the **Packets** menu, the following screens are displayed.



Unicast 0

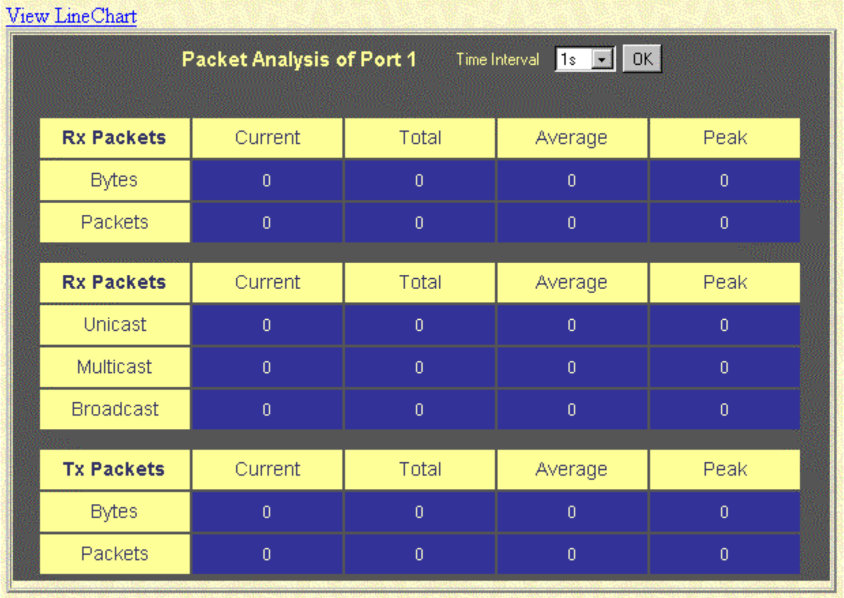
Multicast 0

Broadcast 0

Time Interval 1s

Record Number 200

Show/Hide ☑ Unicast ☑ Multicast ☑ Broadcast



Packet Analysis of Port 1 Time Interval 1s

Rx Packets	Current	Total	Average	Peak
Bytes	0	0	0	0
Packets	0	0	0	0

Rx Packets	Current	Total	Average	Peak
Unicast	0	0	0	0
Multicast	0	0	0	0
Broadcast	0	0	0	0

Tx Packets	Current	Total	Average	Peak
Bytes	0	0	0	0
Packets	0	0	0	0

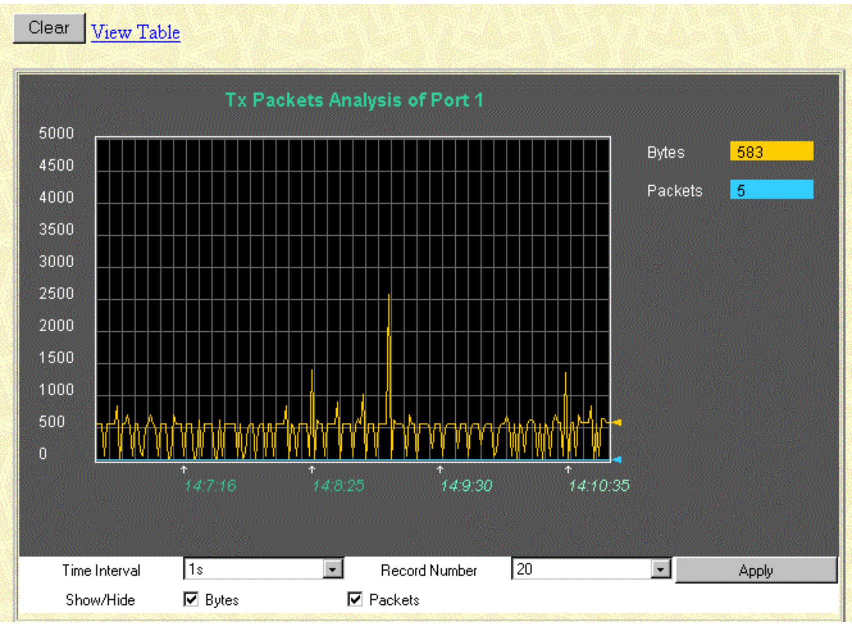
The **UMB-cast (RX) Packets** window displays the number of good bytes and packets that were received by a multicast, broadcast, or unicast address.

The following information is displayed:

- **Time Interval**—The frequency at which the information on the screen is refreshed. The setting can be between 1s and 60s, where “s” stands for seconds.
- **Record Number**—Displays the number of times the switch module will be polled. The setting can be between 20 and 200.
- **Multicast**—Counts the total number of good packets that were received by a multicast address.
- **Broadcast**—Counts the total number of good packets that were received by a broadcast address.
- **Unicast**—Counts the total number of good packets that were received by a unicast address.
- **Show/Hide**—Displays or hides multicast, broadcast, or unicast packets.
- **Clear**—Clears all statistics counters on this window.
- **View Table**—Displays a table rather than a line graph.
- **View Line Chart**—Displays a line graph rather than a table.

Monitoring Transmitted (TX) Packets

When you select **Transmitted (TX) Packets** from the **Packets** menu, the following screens are displayed.



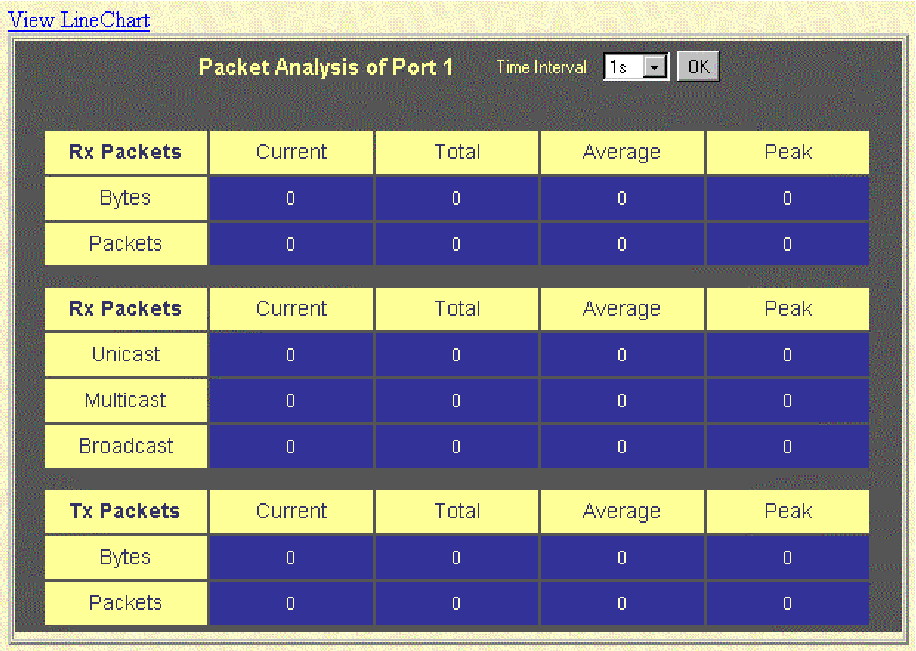
Bytes 583

Packets 5

Time Interval 1s

Record Number 20

Show/Hide ☑ Bytes ☑ Packets



Rx Packets	Current	Total	Average	Peak
Bytes	0	0	0	0
Packets	0	0	0	0

Rx Packets	Current	Total	Average	Peak
Unicast	0	0	0	0
Multicast	0	0	0	0
Broadcast	0	0	0	0

Tx Packets	Current	Total	Average	Peak
Bytes	0	0	0	0
Packets	0	0	0	0

The **Tx Packets Analysis** window displays the number of bytes and packets successfully sent from the port.

The following information is displayed:

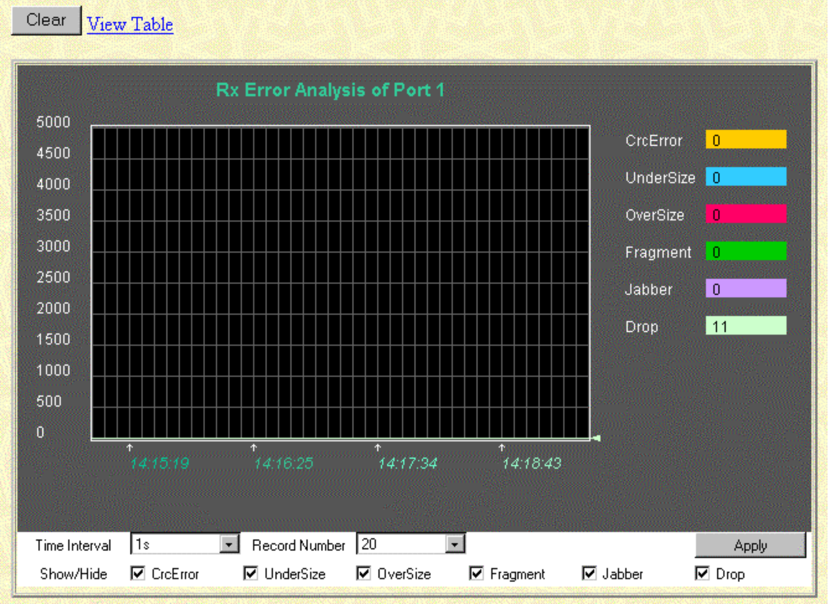
- **Time Interval**—The frequency at which the information on the screen is refreshed. The setting can be between 1s and 60s, where “s” stands for seconds. The default value is one second.
- **Record Number**—Displays the number of times the switch module will be polled. The setting can be between 20 and 200. The default value is 20.
- **Bytes**—Counts the number of bytes successfully sent from the port.
- **Packets**—Counts the number of packets successfully sent from the port.
- **Show/Hide**—Displays or hides bytes and packets information.
- **Clear**—Clears all statistics counters on this window.
- **View Table**—Displays a table rather than a line graph.
- **View Line Chart**—Displays a line graph rather than a table.

Monitoring Errors

The Web Manager allows port error statistics compiled by the switch module’s management agent to be viewed as either a line graph or a table.

Monitoring Received (RX) Errors

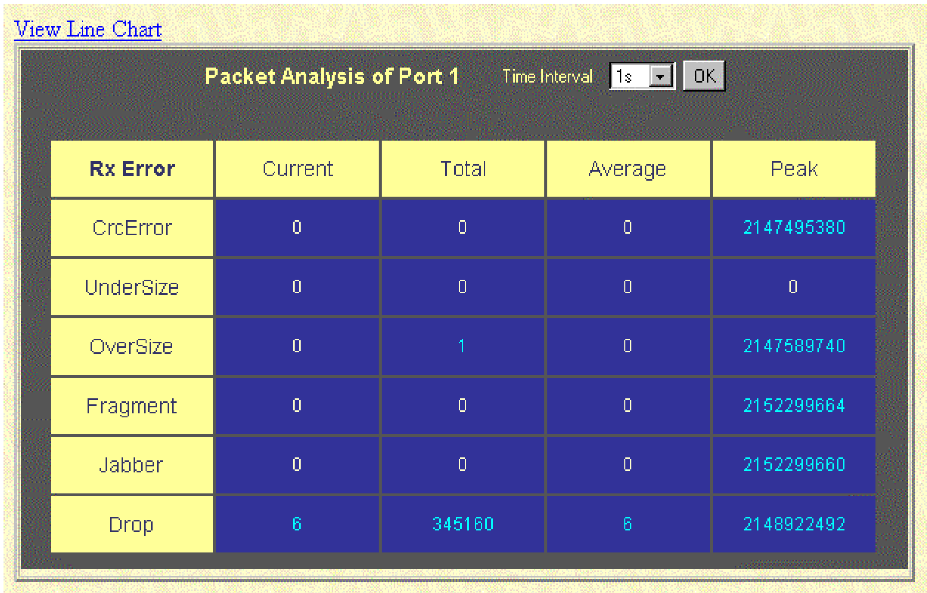
When you select **Received (RX) Errors** from the **Errors** menu, the following screens are displayed.



CrcError	0
UnderSize	0
OverSize	0
Fragment	0
Jabber	0
Drop	11

Time Interval 1s Record Number 20

Show/Hide ☑ CrcError ☑ UnderSize ☑ OverSize ☑ Fragment ☑ Jabber ☑ Drop



Time Interval 1s

Rx Error	Current	Total	Average	Peak
CrcError	0	0	0	2147495380
UnderSize	0	0	0	0
OverSize	0	1	0	2147589740
Fragment	0	0	0	2152299664
Jabber	0	0	0	2152299660
Drop	6	345160	6	2148922492

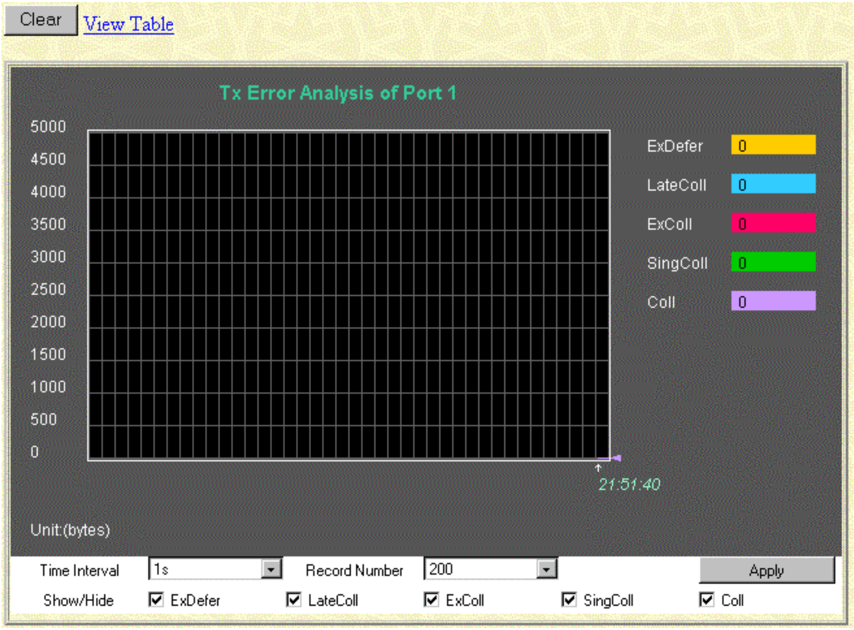
The **Rx Error Analysis** window displays the number of errors received.

The following information is displayed:

- **Time Interval**—The frequency at which the information on the screen is refreshed. The setting can be between 1s and 60s, where “s” stands for seconds. The default value is one second.
- **Record Number**—Displays the number of times the switch module will be polled. The setting can be between 20 and 200. The default value is 20.
- **CRCError**—Counts otherwise valid frames that did not end on a byte (octet) boundary.
- **UnderSize**—Displays the number of frames detected that are less than the minimum permitted frame size of 64 bytes and have a good CRC. Undersized frames usually indicate collision fragments, a normal network occurrence.
- **OverSize**—Counts packets received that were longer than 1518 octets, or if a VLAN frame, 1522 octets, and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1522.
- **Fragment**—Displays the number of packets less than 64 bytes with either bad framing or an invalid CRC. These packets are normally the result of collisions.
- **Jabber**—Displays the number of frames with lengths more than the MAX_PKT_LEN bytes. Internally, MAX_PKT_LEN is equal to 1522.
- **Drop**—Displays the number of frames that were dropped by this port since the last switch module reboot.
- **Show/Hide**—Displays or hides CrcError, UnderSize, OverSize, Fragment, Jabber, and Drop errors.
- **Clear**—Clears all statistics counters on this window.
- **View Table**—Displays a table rather than a line graph.
- **View Line Chart**—Displays a line graph rather than a table.

Monitoring Transmitted (TX) Errors

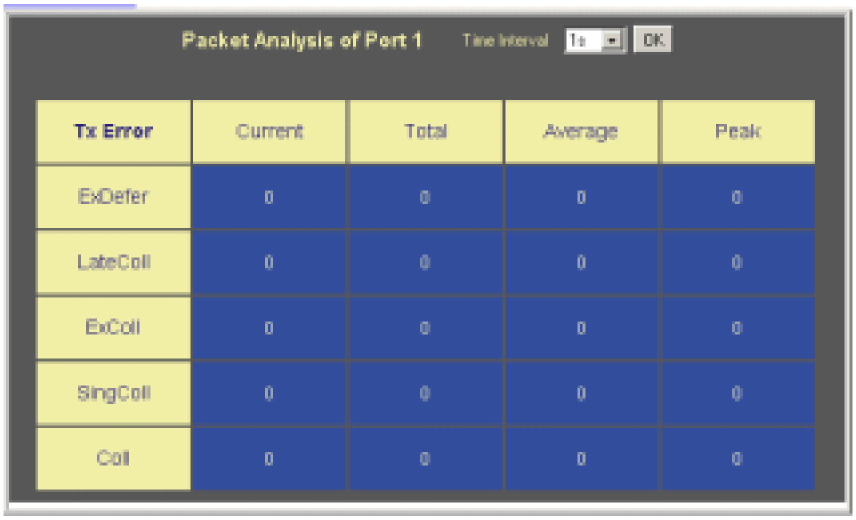
When you select **Transmitted (TX) Errors** from the **Errors** menu, the following screens are displayed.



Time Interval 1s

Record Number 200

Show/Hide ☑ ExDefer ☑ LateColl ☑ ExColl ☑ SingColl ☑ Coll



Time Interval 1s

Tx Error	Current	Total	Average	Peak
ExDefer	0	0	0	0
LateColl	0	0	0	0
ExColl	0	0	0	0
SingColl	0	0	0	0
Coll	0	0	0	0

The **Tx Error Analysis** window displays the number of errors that occurred during transmission.

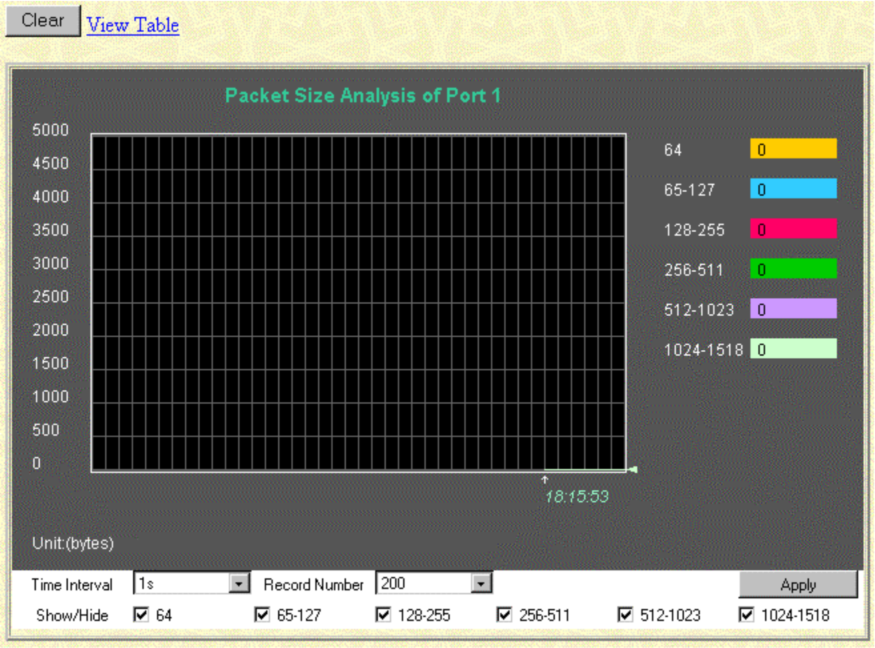
The following information is displayed:

- **Time Interval**—The frequency at which the information on the screen is refreshed. The setting can be between 1s and 60s, where “s” stands for seconds. The default value is one second.
- **Record Number**—Displays the number of times the switch module will be polled. This setting can be between 20 and 200. The default value is 20.
- **ExDefer**—Counts the number of frames for which the first transmission attempt on a particular interface was delayed because the medium was busy.
- **LateColl**—Counts the number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
- **ExColl**—Counts the number of frames that experienced 16 collisions during transmission and were aborted.
- **SingColl**—Counts the number frames that experienced exactly one collision during transmission.
- **Coll**—Counts the number of collisions that occurred during the transmission of a frame.
- **Show/Hide**—Displays or hides ExDefer, CRCError, and LateColl errors.
- **Clear**—Clears all statistics counters on this window.
- **View Table**—Displays a table rather than a line graph.
- **View Line Chart**—Displays a line graph rather than a table.

Monitoring Packet Size

The Web Manager allows packets received by the switch module, arranged in six groups, to be viewed as either a line graph or a table.

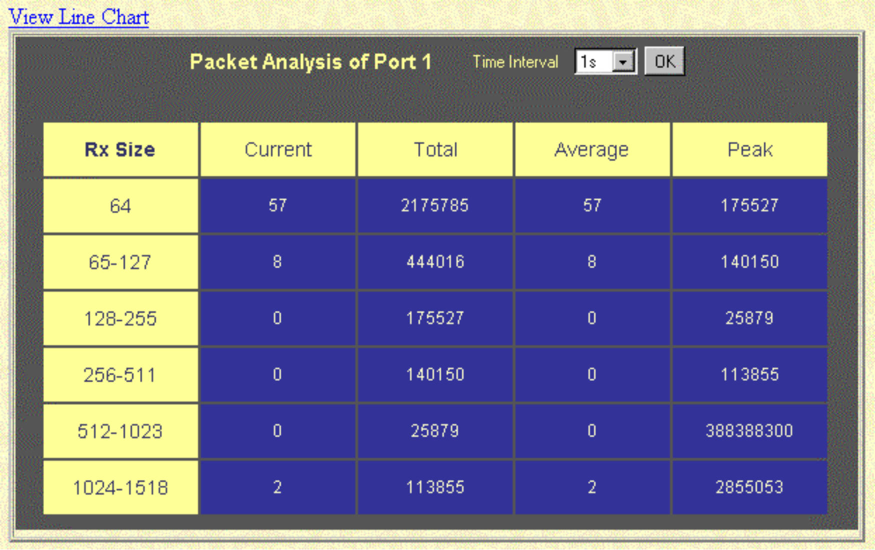
When you select **Packet Size** from the **Size** menu, the following screens are displayed.



64	0
65-127	0
128-255	0
256-511	0
512-1023	0
1024-1518	0

Time Interval 1s Record Number 200

Show/Hide ☑ 64 ☑ 65-127 ☑ 128-255 ☑ 256-511 ☑ 512-1023 ☑ 1024-1518



Packet Analysis of Port 1 Time Interval 1s

Rx Size	Current	Total	Average	Peak
64	57	2175785	57	175527
65-127	8	444016	8	140150
128-255	0	175527	0	25879
256-511	0	140150	0	113855
512-1023	0	25879	0	388388300
1024-1518	2	113855	2	2855053

The **Rx Size Analysis** window displays the number packets received that were within a certain range of octets in length.

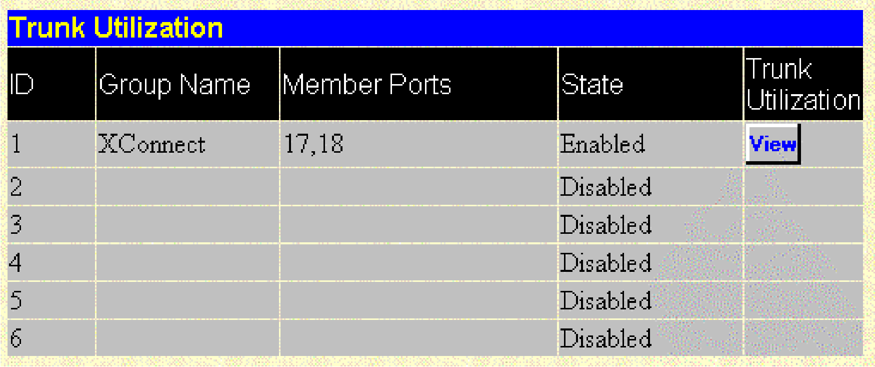
The following information is displayed:

- **Time Interval**—The frequency at which the information on the screen is refreshed. The setting can be between 1s and 60s, where “s” stands for seconds. The default value is one second.

- **Record Number**—Displays the number of times the switch module will be polled. The setting can be between 20 and 200. The default value is 20.
- **64**—Displays the total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
- **65–127**—Displays the total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
- **128–255**—Displays the total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
- **256–511**—Displays the total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
- **512–1023**—Displays the total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
- **1024–1518**—Displays the total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
- **Show/Hide**—Displays or hides packets of the following lengths: 64, 65–127, 128–255, 256–511, 512–1023, and 1024–1518 packets received.
- **Clear**—Clears all statistics counters on this window.
- **View Table**—Displays a table rather than a line graph.
- **View Line Chart**—Displays a line graph rather than a table.

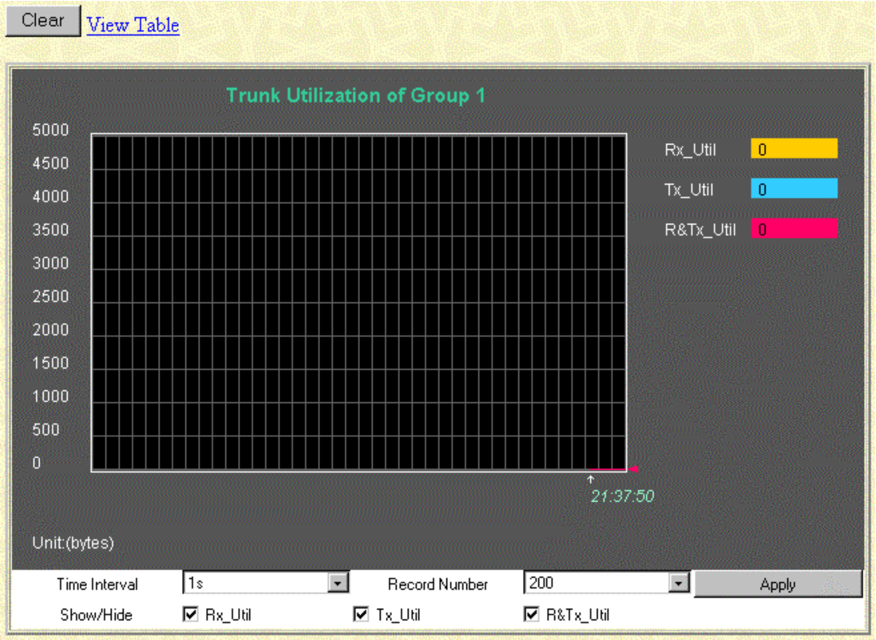
Monitoring Trunk Utilization

When you select **Trunk Utilization** from the **Monitoring** menu, the following screens are displayed.



Trunk Utilization

ID	Group Name	Member Ports	State	Trunk Utilization
1	XConnect	17,18	Enabled	View
2			Disabled	
3			Disabled	
4			Disabled	
5			Disabled	
6			Disabled	



Time Interval: 1s

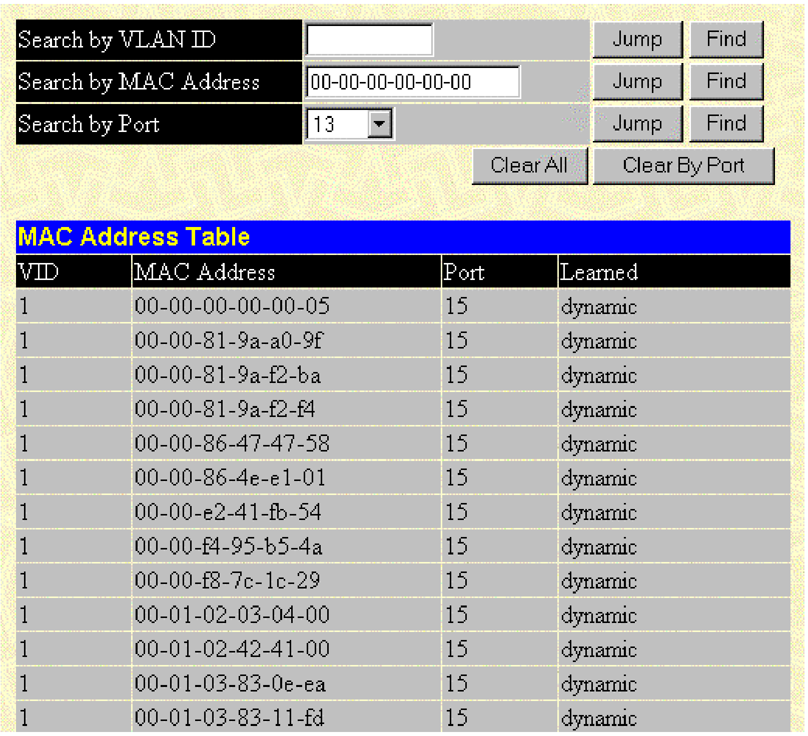
Record Number: 200

Show/Hide: ☑ Rx_Util ☑ Tx_Util ☑ R&Tx_Util

The **Trunk Utilization** window allows you to view graphs of three items for an individual port trunking group: the percentage of total available bandwidth being utilized by the group, the percentage of packets transmitted, and the percentage of packets being received per second.

Monitoring MAC Address Table

When you select **MAC Address** from the **Monitoring** menu, the following screens are displayed.



Search by VLAN ID	
Search by MAC Address	00-00-00-00-00-00
Search by Port	13

MAC Address Table

VID	MAC Address	Port	Learned
1	00-00-00-00-00-05	15	dynamic
1	00-00-81-9a-a0-9f	15	dynamic
1	00-00-81-9a-f2-ba	15	dynamic
1	00-00-81-9a-f2-f4	15	dynamic
1	00-00-86-47-47-58	15	dynamic
1	00-00-86-4e-e1-01	15	dynamic
1	00-00-e2-41-fb-54	15	dynamic
1	00-00-f4-95-b5-4a	15	dynamic
1	00-00-f8-7c-1c-29	15	dynamic
1	00-01-02-03-04-00	15	dynamic
1	00-01-02-42-41-00	15	dynamic
1	00-01-03-83-0e-ea	15	dynamic
1	00-01-03-83-11-fd	15	dynamic

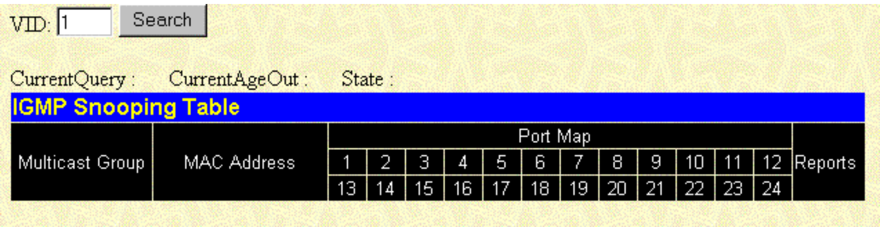
The Web Manager allows the switch module's MAC address table (sometimes referred to as a forwarding table) to be viewed.

The following information is displayed:

- **Search by VLAN ID**—Type the VLAN ID you want to search for.
- **Search by MAC Address**—Type the MAC address you want to search for.
- **Search by Port**—Type the port number you want to search by.
- **Jump**—Click this button to move to a sector of the database corresponding to a user defined port, VLAN, or MAC address.
- **Find**—Click this button to find the data entry.
- **Clear All**—Click this button to clear all forwarding table entries.
- **Clear By Port**—Click this button to clear the forwarding table entries that have the entered port number.
- **VID**—View the VLAN ID of the VLAN that the port is a member of.
- **MAC Address**—View the MAC address entered into the address table.
- **Port**—View the port that the MAC address corresponds to.
- **Learned**—View the method that the switch module used to discover the MAC address.
- **Next**—Click this button to view the next page of the address table.

Monitoring IGMP Snooping Table

When you select **IGMP Snooping** from the **Monitoring** menu, the following screen is displayed.



VID: 1

CurrentQuery : CurrentAgeOut : State :

IGMP Snooping Table

Multicast Group	MAC Address	Port Map												Reports
		1	2	3	4	5	6	7	8	9	10	11	12	
		13	14	15	16	17	18	19	20	21	22	23	24	

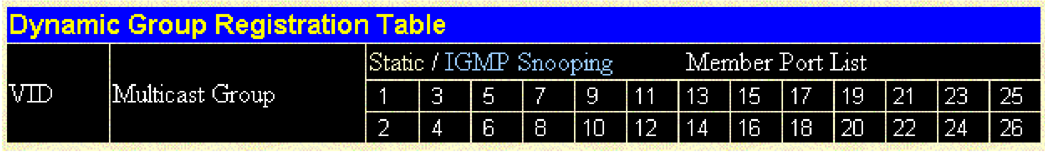
The IGMP Snooping table can be browsed using the Web Manager. The table is organized by VLAN ID (VID).

The following information is displayed:

- **VID**—Type the VLAN ID of the VLAN for which the IGMP Snooping table is to be displayed.
- **Search**—Click this button to display the IGMP Snooping Table for the current VID.
- **Multicast Group**—View the IP address of a multicast group discovered by IGMP Snooping.
- **MAC Address**—View the corresponding MAC address discovered by IGMP Snooping.
- **Port Map**—View the ports that have forwarded multicast packets.
- **Reports**—View the number of IGMP reports for the listed source.

Monitoring Dynamic Group Registration

When you select **Dynamic Group Registration** from the **Monitoring** menu, the following screen is displayed.



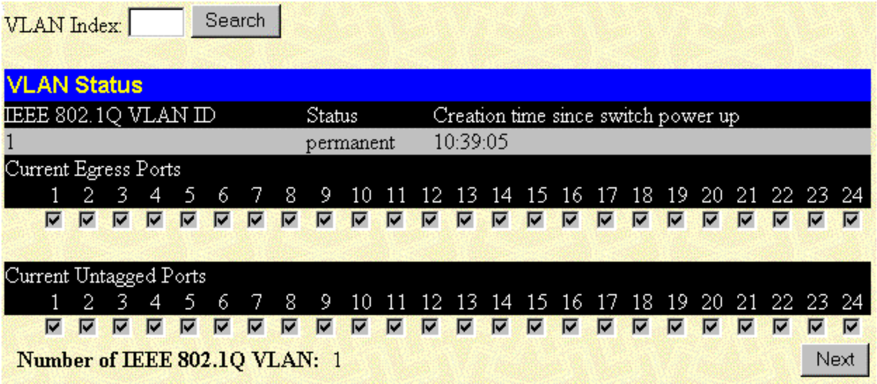
Dynamic Group Registration Table

VID	Multicast Group	Static / IGMP Snooping Member Port List												
		1	3	5	7	9	11	13	15	17	19	21	23	25
		2	4	6	8	10	12	14	16	18	20	22	24	26

The **Dynamic Group Registration Table** displays filtering information for VLANs configured into the bridge by local or network management, or discovered dynamically. It specifies the set of ports that are allowed to be forwarded, based on the frames received on a VLAN for this forwarding database (FDB) and the specific group destination address for the VLAN.

Monitoring VLAN Status

When you select **VLAN Status** from the **Monitoring** menu, the following screen is displayed.



VLAN Status

IEEE 802.1Q VLAN ID	Status	Creation time since switch power up
1	permanent	10:39:05

Current Egress 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
☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Current Untagged 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
☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Number of IEEE 802.1Q VLAN: 1

The **VLAN Status** window displays information on which VLAN ports are in egress and which are untagged.

The following information is displayed:

- **IEEE 802.1Q VLAN ID**—Displays the VLAN for which the VLAN table is displayed.
- **Status**—Displays the current status of the VID.
- **Creation time since switch power up**—Displays the hours, minutes, and seconds since the switch module was last rebooted.
- **Current Egress Ports**—Displays the current egress ports on the VLAN.
- **Current Untagged Ports**—Displays the current untagged ports on the VLAN.
- **Prev**—Displays the previous VLAN.
- **Next**—Displays the next VLAN.

To display the **VLAN Status** window for the desired VLAN:

1. Type a VLAN ID number in the **VLAN Index** field.
2. Click **Search.** The VLAN status is displayed.

Maintaining the Switch Module

The **Maintenance** menu has the following sections:

- TFTP Services (Update Firmware, Configuration File, Save Settings, and Save History Log)
- Switch History
- Ping Test

- Save Changes
- Factory Reset
- Restart System
- Connection Timeout
- Logout

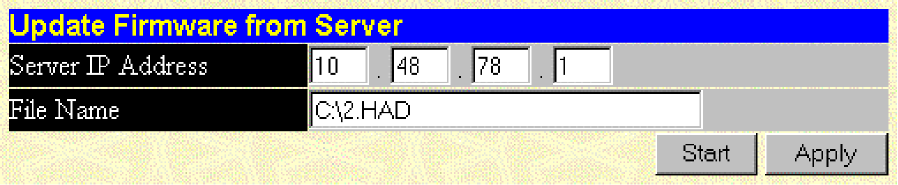
Using TFTP Services

Trivial File Transfer Protocol (TFTP) services allow the switch module firmware to be upgraded by downloading a new firmware file from a TFTP server to the switch module. A configuration file can also be loaded into the switch module, and switch module settings can be saved to a TFTP server. In addition, the switch module's history log can be uploaded from the switch module to a TFTP server.

Please note that TFTP server software must be running on the management station for the TFTP services to function.

Updating the Firmware File Path

When you select **Update Firmware** from the **TFTP Services** menu, the following screen is displayed.



Update Firmware from Server

Server IP Address: 10 . 48 . 78 . 1

File Name: C:\2.HAD

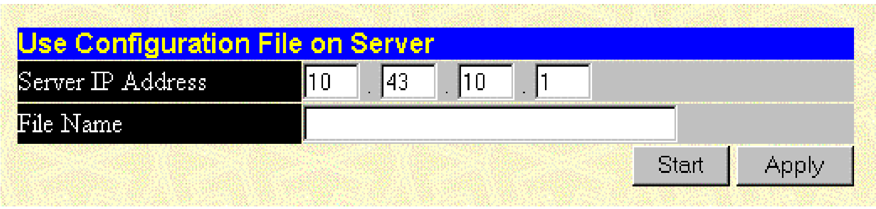
The **Update Firmware from Server** window allows you to update the path of a new firmware file on the TFTP server.

To update the path:

1. Type the IP address of the TFTP Server in the **Server IP Address** field.
2. Type the complete path and file name of the firmware file for the switch module in the **File Name** field.
3. Click **Apply** to enter the server's IP address into the switch module's RAM.
4. Click **Start** to initiate the file transfer. The system automatically reboots after the file transfer.

Downloading a Configuration File on a TFTP Server

When you select **Configuration File** from the **TFTP Services** menu, the following screen is displayed.



Use Configuration File on Server

Server IP Address: 10 . 43 . 10 . 1

File Name:

A configuration file can be downloaded from a TFTP server to the switch module. This file is then used by the switch module to configure itself.

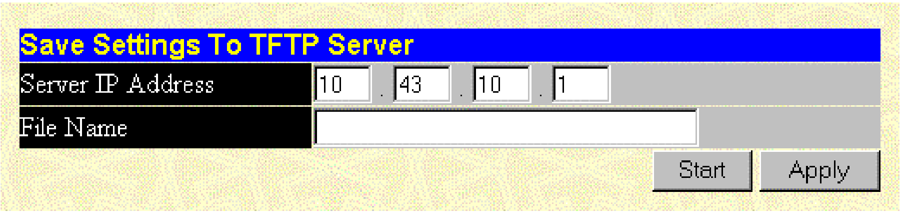
NOTE: Configuration files used in the earlier version of this switch module (firmware version 1.0) are not supported by the present version (firmware version 2.0). The switch module Information window displays the firmware version.

To download the file:

1. Type the IP address of the TFTP Server in the **Server IP Address** field.
2. Type the complete path and file name of the firmware file for the switch module in the **File Name** field.
3. Click **Apply** to enter the server's IP address into the switch module's RAM.
4. Click **Start** to initiate the file transfer. The system automatically reboots after the file transfer.

Saving Settings to TFTP Server

When you select **Save Settings** from the **TFTP Services** menu, the following screen is displayed.



Save Settings To TFTP Server

Server IP Address: 10 . 43 . 10 . 1

File Name:

After saving the switch module configuration to NVRAM, Compaq highly recommends that you upload the configuration image to TFTP server storage.

The switch module's management agent can upload the switch module's current settings to a TFTP Server.

To upload the current settings to a TFTP server:

1. Type the IP address of the TFTP Server in the **Server IP Address** field.

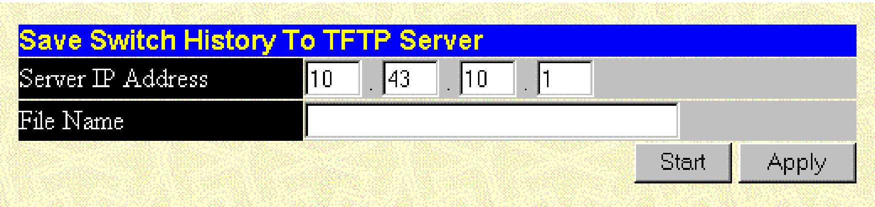
2. Type the complete path and file name of the firmware file for the switch module in the **File Name** field.
3. Click **Apply** to enter the server's IP address into the switch module's RAM.
4. Click **Start** to initiate the file transfer.

NOTE: To save the configuration settings permanently, you must enter them into the NVRAM using the **Save Changes** option on the **Maintenance** menu. See the section, "Saving Changes," earlier in this chapter.

NOTE: If you do not save configurations to NVRAM, the configurations you are uploading to a TFTP server will not be saved correctly.

Saving History Log

When you select **Save History Log** from the **TFTP Services Maintenance** menu, the following screen is displayed.



Save Switch History To TFTP Server

Server IP Address	10 . 43 . 10 . 1
File Name	

The switch module's management agent can upload its history log file to a TFTP server.

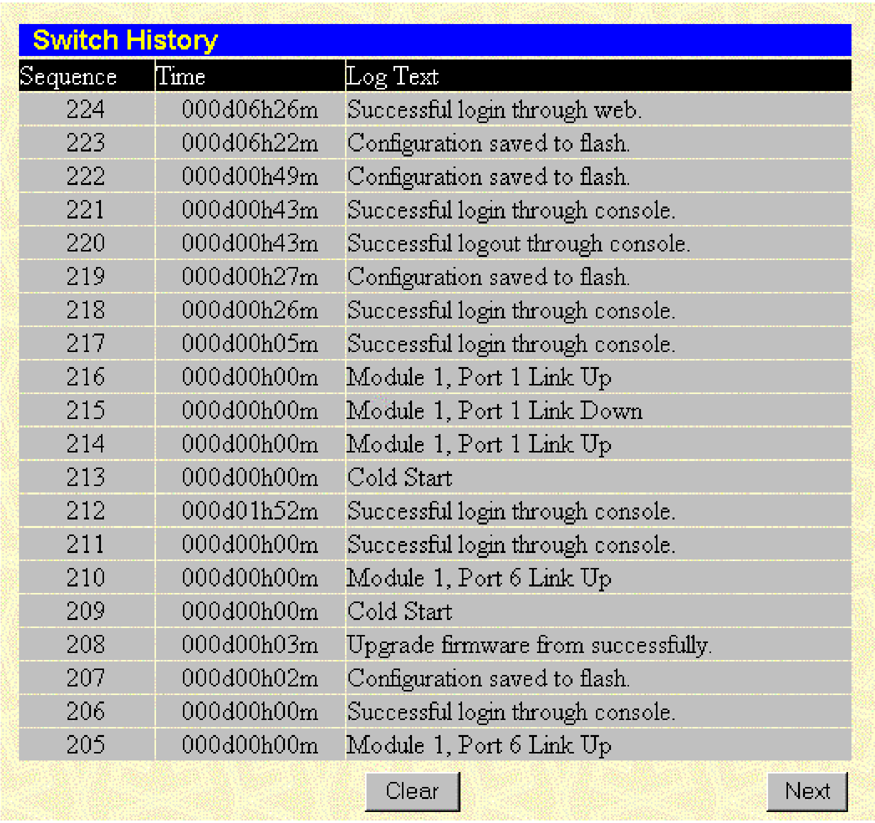
NOTE: An empty history file on the TFTP server must exist on the server before the switch module can upload its history file.

To upload the history log file to a TFTP server:

1. Type the IP address of the TFTP Server in the **Server IP Address** field.
2. Type the complete path and file name of the firmware file for the switch module in the **File Name** field.
3. Click **Apply** to enter the server's IP address into the switch module's RAM.
4. Click **Start** to initiate the file transfer.

Displaying Switch Module History

When you select **Switch History** from the **Maintenance** menu, the following screen is displayed.



Switch History

Sequence	Time	Log Text
224	000d06h26m	Successful login through web.
223	000d06h22m	Configuration saved to flash.
222	000d00h49m	Configuration saved to flash.
221	000d00h43m	Successful login through console.
220	000d00h43m	Successful logout through console.
219	000d00h27m	Configuration saved to flash.
218	000d00h26m	Successful login through console.
217	000d00h05m	Successful login through console.
216	000d00h00m	Module 1, Port 1 Link Up
215	000d00h00m	Module 1, Port 1 Link Down
214	000d00h00m	Module 1, Port 1 Link Up
213	000d00h00m	Cold Start
212	000d01h52m	Successful login through console.
211	000d00h00m	Successful login through console.
210	000d00h00m	Module 1, Port 6 Link Up
209	000d00h00m	Cold Start
208	000d00h03m	Upgrade firmware from successfully.
207	000d00h02m	Configuration saved to flash.
206	000d00h00m	Successful login through console.
205	000d00h00m	Module 1, Port 6 Link Up

The Web Manager allows the switch module’s history log, as compiled by the switch module’s management agent, to be viewed. The switch module can record event information in its own logs, to designated SNMP trap receiving stations, and to the PC connected to the console manager.

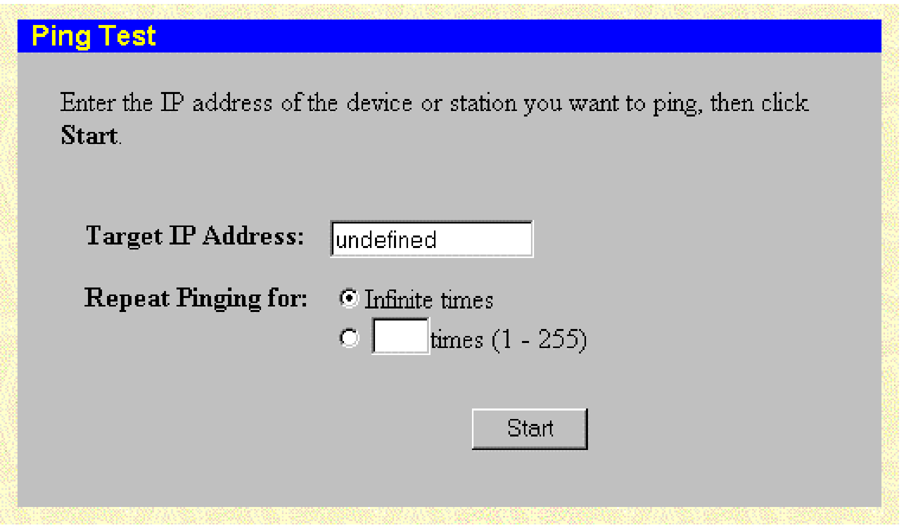
The following information is displayed:

- **Sequence**—Displays a counter incremented whenever an entry to the switch module’s history log is made. The table displays the last entry (highest sequence number) first.
- **Time**—Displays the time in days, hours, and minutes since the switch module was last restarted.
- **Log Text**—Displays text describing the event that triggered the history log entry.

Click **Next** to display all of the Switch Trap Logs.

Performing a Ping Test

When you select **Ping Test** from the **Maintenance** menu, the following screen is displayed.



Enter the IP address of the device or station you want to ping, then click **Start**.

Target IP Address: undefined

Repeat Pinging for: ● Infinite times
○ times (1 - 255)

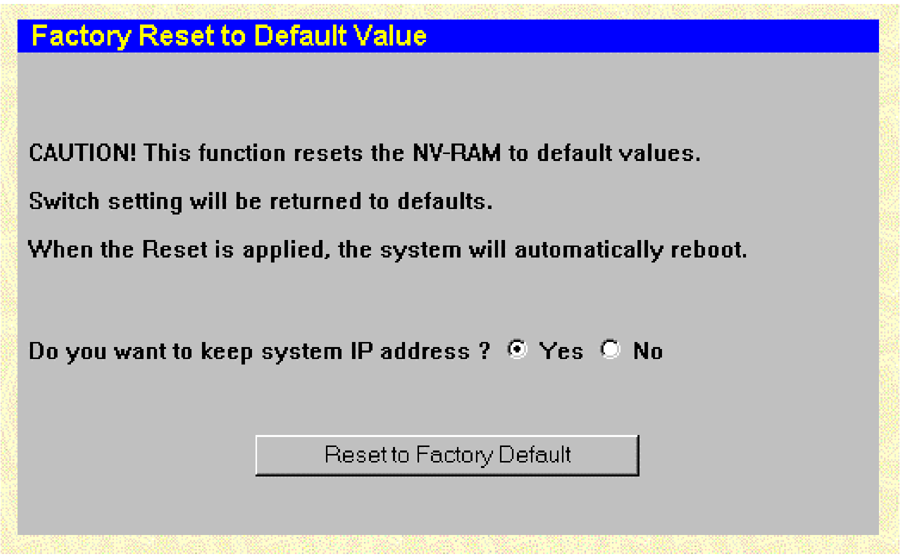
The switch module is able to test the connection with another network device by pinging it.

To initiate the Ping program:

1. Type the IP address of the network device to be pinged in the **Target IP Address** field.
2. Select the number of test packets to be sent (three is usually enough) in the **Repeat Pinging for** field.
3. Click **Start** to initiate the Ping program.

Resetting the Switch Module Configuration to Factory Defaults

When you select **Factory Reset** from the **Maintenance** menu, the following screen is displayed.



Factory Reset to Default Value

CAUTION! This function resets the NV-RAM to default values.

Switch setting will be returned to defaults.

When the Reset is applied, the system will automatically reboot.

Do you want to keep system IP address ? ● Yes ○ No

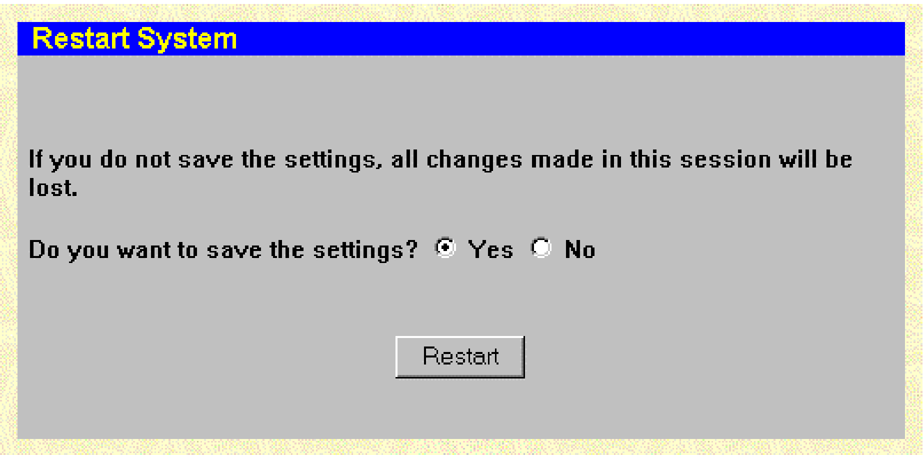
Factory Reset allows you to return the switch module settings to the factory defaults.

To return the settings to the factory defaults:

1. Select **Yes** or **No** to keep the system IP address. If you want your IP address to default from DHCP or BOOTP, select **No.**
2. Click **Reset to Factory Default** to reset the switch module.

Rebooting the Switch Module

When you select **Restart System** from the **Maintenance** menu, the following screen is displayed.



If you do not save the settings, all changes made in this session will be lost.

Do you want to save the settings? ● Yes ○ No

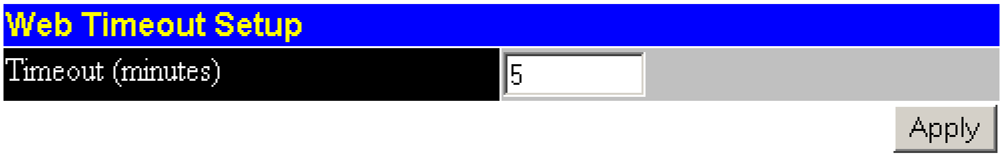
Restart System allows you to perform a reboot of the switch module, which resets the system.

To restart the system:

1. Select **Yes** or **No** to save the settings.
2. Click **Restart.**

Setting the Connection Timeout

When you select **Connection Timeout** from the **Maintenance** menu, the following screen is displayed.



Timeout (minutes) 5

The **Web Timeout Setup** screen allows you to set the timeout interval.

To enter Web timeout:

1. Type the desired age-out time in the **Timeout (minutes)** field.
2. Click **Apply.**

NOTE: To save the configuration settings permanently, you must enter them into the NVRAM using the **Save Changes** option on the **Maintenance** menu. See the section, “Saving Changes,” earlier in this chapter.

Logging out

To exit the setup pages, select **Logout** on the **Maintenance** menu. The **Account Login** screen is displayed.

A

Technical Specifications

Table A-1: General Specifications

Standards	IEEE 802.3 10Base-T Ethernet IEEE 802.3u 100Base-TX Fast Ethernet IEEE 802.3ab 1000Base-T Gigabit Ethernet IEEE 802.1Q VLAN IEEE 802.3x Full-Duplex Flow Control ANSI/IEEE 802.3 Nway Auto-Negotiation
Protocols	CSMA/CD
Data Transfer Rates	
Ethernet	Half-Duplex: 10-Mb/s Full-Duplex: 20-Mb/s
Fast Ethernet	Half-Duplex: 100-Mb/s Full-Duplex: 200-Mb/s
Gigabit Ethernet	Full Duplex: 2000-Mb/s
Network Cables	
10Base-T	2 Pair UTP Category 3,4,5 (100 m) EIA/TIA-568 100-ohm STP (100 m)
100Base-TX	2 Pair or 4 Pair UTP Category 5 (100 m) EIA/TIA-568 100-ohm STP (100 m)
1000Base and 1000Base-T	4 Pair UTP Category 5e (100 m) EIA/TIA-568 100-ohm STP (100 m)
Number of Ports	42—10/100-Mb/s Nway Ethernet Ports 4—10/100/1000 Base-T/TX/T Uplink Ethernet Ports 1—Serial RS-232 Console Management Port (through the Integrated Administrator) 1—10/100 Base T/TX Ethernet Management Port (through the Integrated Administrator)

Table A-2: Physical and Environmental Specifications

DC Inputs	12V: 3.5A per switch module 5V: 0.3A per switch module
Power Consumption	50 watts maximum per switch module
Operating Temperature	0 to 50 degrees Celsius
Storage Temperature	-30 to 70 degrees Celsius
Operating Humidity	5% to 95% RH noncondensing
Storage Humidity	0% to 95% RH noncondensing
Dimensions	11.2 inches x 16.1 inches
Weight	620 grams (1.4 lb)
EMI	FCC Class A CE Class A VCCI Class A
Safety	UL/CUL TUV/GS

Table A-3: Performance Specifications

Transmission Method	Store-and-forward
RAM Buffer	8MB per switch module
Filtering Address Table	8K
Packet Filtering/Forwarding Rate	Full-wire speed for all connections. 148,809.5 pps per port (for 100-Mb/s) 1,488,095 pps per port (for 1000-Mb/s)
MAC Address Learning	Automatic update
Forwarding Table Age Time	Maximum Age: 10-9999 seconds Default: 3000 seconds
Maximum Number of VLANs	64 (including default VLAN)

B

RJ-45 Pin Specification

When connecting the Compaq ProLiant BL e-class C-GbE Interconnect Switch to a switch, bridge, or hub, a Category 5 Ethernet cable is necessary. Review these products for matching cable pin assignments.

Figure B-1 displays the standard RJ-45 receptacle/connector. Table B-1 provides the pin assignments for the switch-to-network adapter card connection, and for the Category 5 Ethernet cable for a switch-to-switch, -hub, or –bridge connection.

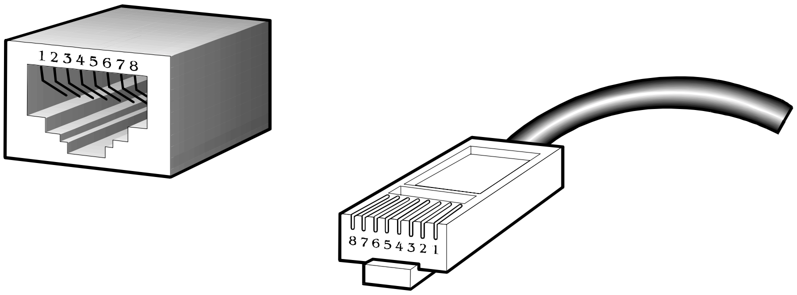


Figure B-1: Standard RJ-45 receptacle/connector

Table B-1: RJ-45 Connector Pin Assignments

Contact	Media Direct Interface Signal for 10/100	Media Direct Interface Signal for 1000T
1	Tx + (transmit)	BI_DA+
2	Tx – (transmit)	BI_DA-
3	Rx + (receive)	BI_DB+
4	Not used	BI_DC+
5	Not used	BI_DC-
6	Rx – (receive)	BI_DB-
7	Not used	BI_DD+
8	Not used	BI_DD-

C

Runtime Switching Software Default Settings

Default Settings

Table C-1: Default Settings

Setting	Value
User Name	None
Password	None
DHCP Service	Enabled
Bootp Service	Disabled
IP Address (if manual option is selected)	Switch A = 10.90.90.90 Switch B = 10.90.90.91
Subnet Mask (if manual option is selected)	255.0.0.0
Default Gateway (if manual option is selected)	0.0.0.0
Management VID	1
System Name	None
System Location	None
System Contact	None
Auto Logout	10 minutes
MAC Address Aging Time	300 seconds
IGMP Snooping	Disabled
Switch GVRP	Disabled
Telnet Status	Enabled
Web Status	Enabled
Group Address Filter Mode	Forward all unregistered
Scheduling Mechanism for COS Queues	Strict
Trunk Load Sharing Algorithm	Src Address
Backpressure	Disabled

continued

Table C-1: Default Settings *continued*

Setting	Value
Port Speed/Duplex	Auto
Flow Control	On
Setup Restart Ingress Bandwidth	None
Setup Restart Egress Bandwidth	None
Switch STP	Enabled
Bridge Max Age	20 seconds
Bridge Hello Time	2 seconds
Bridge Forward Delay	15 seconds
Bridge Priority	32768
Configure Static Unicast Filtering Table	None
Configure Static Multicast Filtering Table	None
Configure Static VLAN Entry	Default VLAN (VID = 1)
Default Port VID	1
Default Port Ingress Rule Checking	Disabled
Port GVRP Setting	Disabled
IGMP Snooping—VLAN ID	1
IGMP Snooping—State	Enabled
IGMP Snooping—Querier State	Non-querier
IGMP Snooping—Robustness Variable	2
IGMP Snooping—Query Interval	125 seconds
IGMP Snooping—Max Response	10 seconds
Port Trunking	Xconnect (Port 21-22)
Port Mirroring—Source Port	1
Port Mirroring—Source Direction	Ingress and egress
Port Mirroring—Target Port	11
Port Mirroring—Mirror Status	Disabled
Broadcast Storm	Disabled
Multicast Storm	Disabled
DA Unknown Storm	Disabled
Storm Threshold	500 packets/second

continued

Table C-1: Default Settings *continued*

Setting	Value	
Port State	Enabled	
Class of Service—Max Packets	10	
Class of Service—Max Latency	0	
Default Port Priority	0	
Class of Traffic	Priority 0, 1: Class 0	Priority 4, 5: Class 2
	Priority 2, 3: Class 1	Priority 6, 7: Class 3
Port Security—Admin State	Disabled	
Port Security—Max Address	1	
Port Security—Mode	DeleteOnReset	
Priority MAC Address	None	
SNMP Community String	“public”, “private”	
SNMP Trap Manager IP	None	
Security IP	0.0.0.0	
User Account	None	
Firmware Update	Disabled	
Configuration File on TFTP Server	Disabled	
Save Setting to TFTP Server	Disabled	
Save History Log to TFTP Server	Disabled	
PING Test	Disabled	
Out-of-band Baud Rate	Fixed 115,200	
TFTP Server IP Address	0.0.0.0	
VLAN Mode	IEEE 802.1Q	

Port Names, VLANs, STP/By Pass, Trunking Default Settings

Table C-2: Switch Module A

Port Type	UI Port #	Speed	VID	VLAN Member AS	VLAN Name	Port Name	STP / ByPass Enabled	Multi-link Trunk
Server	1	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server1_Port1	Yes	
Server	2	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server2_Port1	Yes	
Server	3	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server3_Port1	Yes	
Server	4	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server4_Port1	Yes	
Server	5	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server5_Port1	Yes	
Server	6	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server6_Port1	Yes	
Server	7	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server7_Port1	Yes	
Server	8	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server8_Port1	Yes	
Server	9	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server9_Port1	Yes	
Server	10	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server10_Port1	Yes	
Server	11	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server11_Port1	Yes	
Server	12	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server12_Port1	Yes	
Server	13	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server13_Port1	Yes	
Server	14	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server14_Port1	Yes	
Server	15	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server15_Port1	Yes	
Server	16	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server16_Port1	Yes	
Server	17	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server17_Port1	Yes	

continued

Table C-2: Switch Module A *continued*

Port Type	UI Port #	Speed	VID	VLAN Member AS	VLAN Name	Port Name	STP / ByPass Enabled	Multi-link Trunk
Server	18	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server18_Port1	Yes	
Server	19	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server19_Port1	Yes	
Server	20	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server20_Port1	Yes	
X-Connect	21	10/100 (Auto)	1	Egress	DEFAULT_VLAN	XConnect1	No	XCon-nect
X-Connect	22	10/100 (Auto)	1	Egress	DEFAULT_VLAN	XConnect2	No	XCon-nect
IA NIC	23	10/100 (Auto)	1	Egress	DEFAULT_VLAN	IA Mgmt Module	Yes	
Mgmt Uplink	24	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Mgmt Uplink	Yes	
D Uplink	25	10/100 /1000 (Auto)	1	Egress	DEFAULT_VLAN	SwitchA_Uplink1	No	
D Uplink	26	10/100 /1000 (Auto)	1	Egress	DEFAULT_VLAN	SwitchA_Uplink2	No	

Table C-3: Switch Module B

Port Type	UI Port #	Speed	VID	VLAN Member AS	VLAN Name	Port Name	STP / ByPass Enabled	Multi-link Trunk
Server	1	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server1_Port2	Yes	
Server	2	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server2_Port2	Yes	
Server	3	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server3_Port2	Yes	
Server	4	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server4_Port2	Yes	
Server	5	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server5_Port2	Yes	
Server	6	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server6_Port2	Yes	
Server	7	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server7_Port2	Yes	
Server	8	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server8_Port2	Yes	
Server	9	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server9_Port2	Yes	
Server	10	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server10_Port2	Yes	
Server	11	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server11_Port2	Yes	
Server	12	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server12_Port2	Yes	
Server	13	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server13_Port2	Yes	
Server	14	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server14_Port2	Yes	
Server	15	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server15_Port2	Yes	
Server	16	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server16_Port2	Yes	
Server	17	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server17_Port2	Yes	
Server	18	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server18_Port2	Yes	

continued

Table C-3: Switch Module B *continued*

Port Type	UI Port #	Speed	VID	VLAN Member AS	VLAN Name	Port Name	STP / ByPass Enabled	Multi-link Trunk
Server	19	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server19_Port2	Yes	
Server	20	10/100 (Auto)	1	Egress	DEFAULT_VLAN	Server20_Port2	Yes	
X-Connect	21	10/100 (Auto)	1	Egress	DEFAULT_VLAN	XConnect1	No	XConnect
X-Connect	22	10/100 (Auto)	1	Egress	DEFAULT_VLAN	XConnect2	No	XConnect
IA NIC	23	10/100 (Auto)	NA	NA	NA	NA	NA	
Mgmt Uplink	24	10/100 (Auto)	NA	NA	NA	NA	NA	
D Uplink	25	10/100 /1000 (Auto)	1	Egress	DEFAULT_VLAN	SwitchB_Uplink1	No	
D Uplink	26	10/100 /1000 (Auto)	1	Egress	DEFAULT_VLAN	SwitchB_Uplink2	No	

D

Spanning Tree Protocol

Introduction

When Spanning Tree Protocol determines a port should be transitioned to the forwarding state, the following occurs:

- The port is put into the listening state where it receives Bridge Protocol Data Units (BPDUs) and passes them to the GbE Interconnect Switch’s CPU.
- If no BPDUs that suggest the port should go to the blocking state are received, the BPDU packets from the CPU are processed
  - The port waits for the expiration of the forward delay timer. The port then moves to the learning state.
  - In the learning state, the port learns station location information from the source address of packets and adds this information to its forwarding database.
  - The expiration of the forwarding delay timer moves the port to the forwarding state, where both learning and forwarding are enabled. At this point, the port forwards packets.

Blocking State

A port in the blocking state does not forward packets. When the switch is booted, a BPDU is sent to each port in the switch putting these ports into the blocking state. A switch initially assumes it is the root, and then begins the exchange of BPDUs with other switches. This will determine which switch in the network is the best choice for the root switch. If there is only one switch on the network, no BPDU exchange occurs, the forward delay timer expires, and the ports move to the listening state. All STP enabled ports enter the blocking state following switch boot.

A port in the blocking state does the following:

- Discards packets received from the network segment to which it is attached.
- Discards packets sent from another port on the switch for forwarding.
- Does not add addresses to its forwarding database.
- Receives BPDUs and directs them to the CPU.

- Does not transmit BPDUs received from the CPU.
- Receives and responds to network management messages.

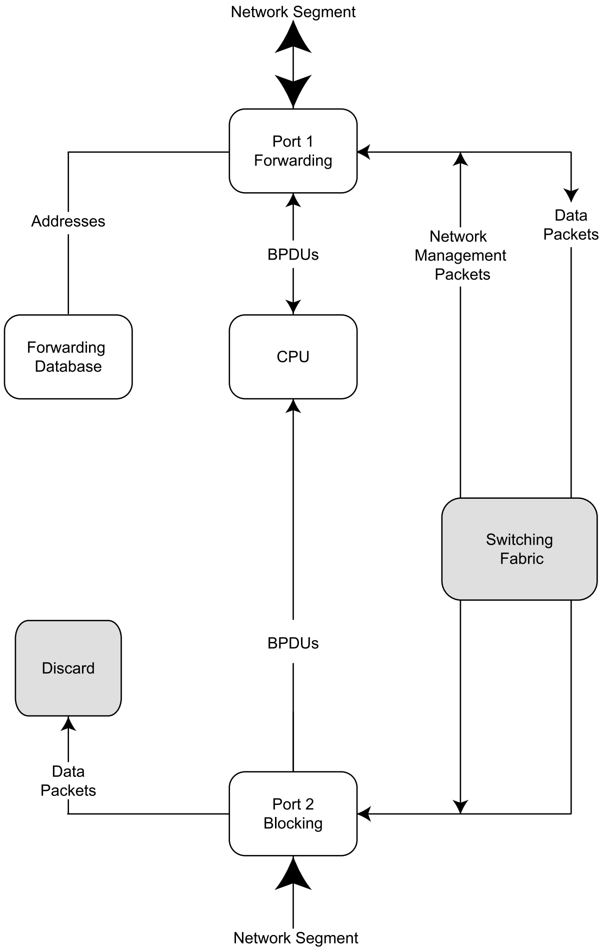


Figure D-1: Blocking State

Listening State

The listening state is the first transition for a port from the blocking state. Listening is an opportunity for the switch to receive BPDUs that may tell the switch that the port should not continue to transition to the forwarding state, but should return to the blocking state (that is, a different port is a better choice).

There is no address learning or packet forwarding from a port in the listening state.

A port in the listening state does the following:

- Discards frames received from the network segment to which it is attached.
- Discards packets sent from another port on the switch for forwarding.

- Does not add addresses to its forwarding database.
- Receives BPDUs and directs them to the CPU.
- Processes BPDUs received from the CPU.
- Receives and responds to network management messages.

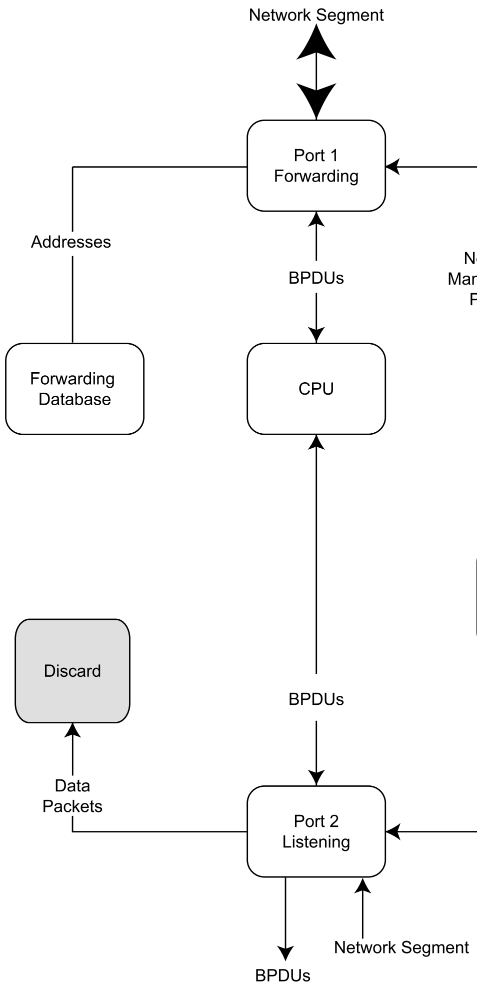


Figure D-2: Listening State

Learning State

A port in the learning state prepares to participate in frame forwarding. The port enters the learning state from the listening state.

A port in the learning state does the following:

- Discards frames received from the network segment to which it is attached.
- Discards packets sent from another port on the switch for forwarding.

- Adds addresses to its forwarding database.
- Receives BPDUs and directs them to the CPU.
- Processes and transmits BPDUs received from the CPU.
- Receives and responds to network management messages.

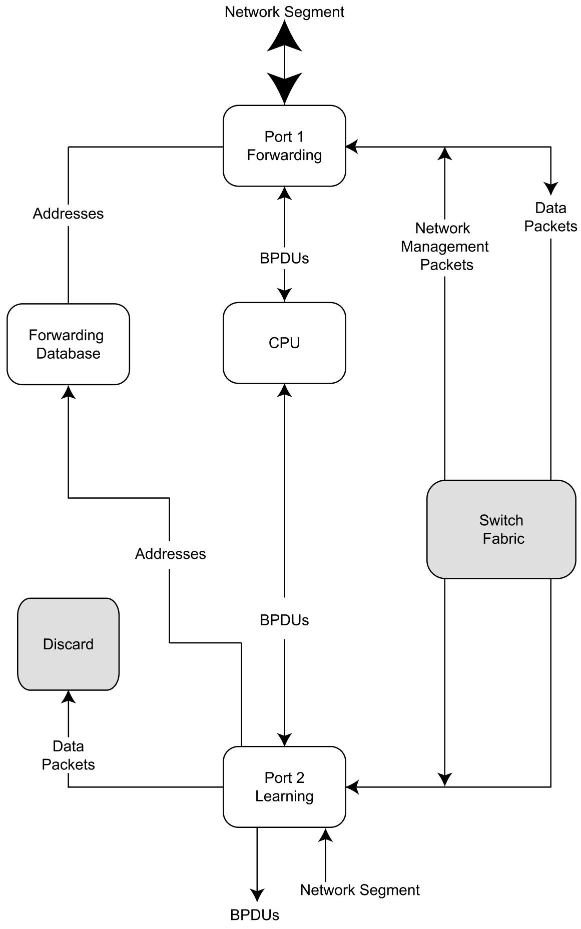


Figure D-3: Learning State

Forwarding State

A port in the forwarding state forwards packets. The port enters the forwarding state from the learning state when the forward delay timer expires.

A port in the forwarding state does the following:

- Forwards packets received from the network segment to which it is attached.
- Forwards packets sent from another port on the switch for forwarding.
- Incorporates station location information into its address database.

- Receives BPDUs and directs them to the system CPU.
- Receives and responds to network management messages.

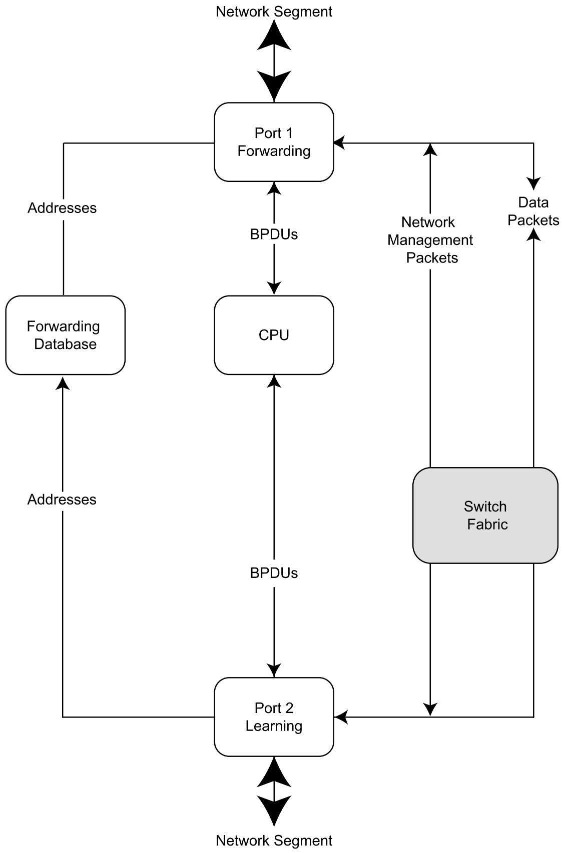


Figure D-4: Forwarding State

Disabled State

A port in the disabled state does not participate in frame forwarding or STP. A port in the disabled state is virtually non-operational.

A disabled port does the following:

- Discards packets received from the network segment to which it is attached.
- Discards packets sent from another port on the switch for forwarding.
- Does not add addresses to its forwarding database.
- Receives BPDUs, but does not direct them to the system CPU.

- Does not receive BPDUs for transmission from the system CPU.
- Receives and responds to network management messages.

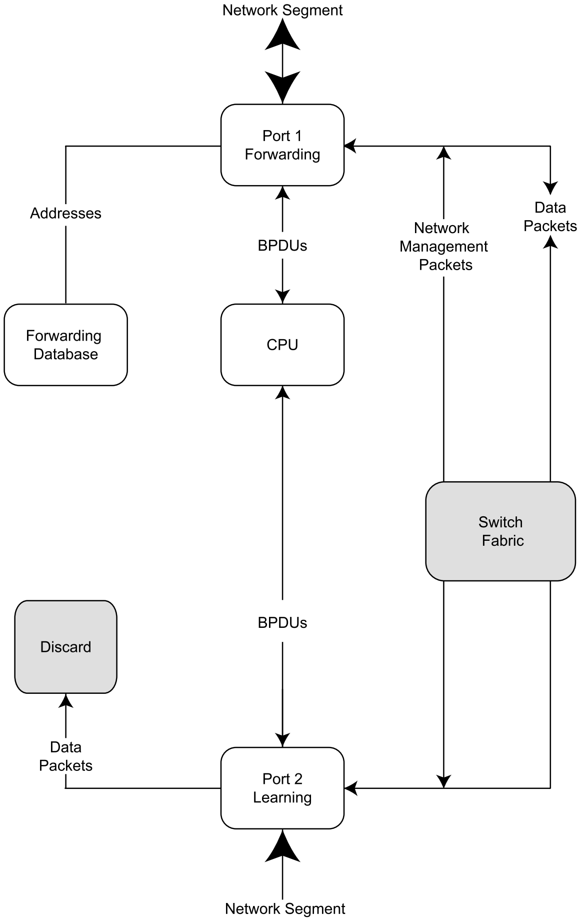


Figure D-5: Disabled State

Troubleshooting STP

This section describes several troubleshooting tips.

Spanning Tree Protocol Failure

A failure in the STP generally leads to a bridging loop. A bridging loop in an STP environment comes from a port that should be in the blocking state, but is forwarding packets.

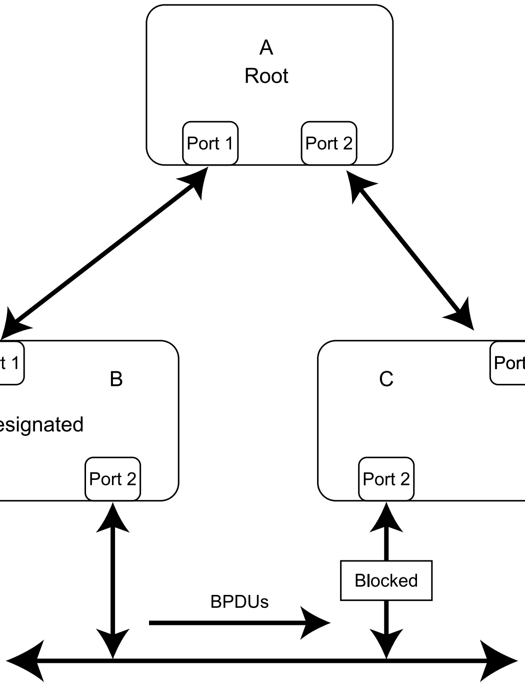


Figure D-6: Example of Spanning Tree Protocol failure

In this example, B has been elected as the designated bridge, and Port 2 on C is in the blocking state. The election of B as the designated bridge is determined by the exchange of BPDUs between B and C. B had a better BPDU than C. B continues sending BPDUs advertising its superiority over the other bridges on this LAN. Should C fail to receive these BPDUs for longer than the MAX AGE (default of 20 seconds), it could start to transition its Port 2 from the blocking state to the forwarding state.

NOTE: A port must continue to receive BPDUs advertising superior paths to remain in the blocking state.

There are a number of circumstances in which the STP can fail, mostly related to the loss of a large number of BPDUs. These situations will cause a port in the blocking state to transition to the forwarding state.

Full/Half Duplex Mismatch

A mismatch in the duplex state of two ports is a very common configuration error for a point-to-point link. If one port is configured as full-duplex, and the other port is left in auto-negotiation mode, the second port will end up in half-duplex because ports configured as half- or full-duplex do not negotiate.

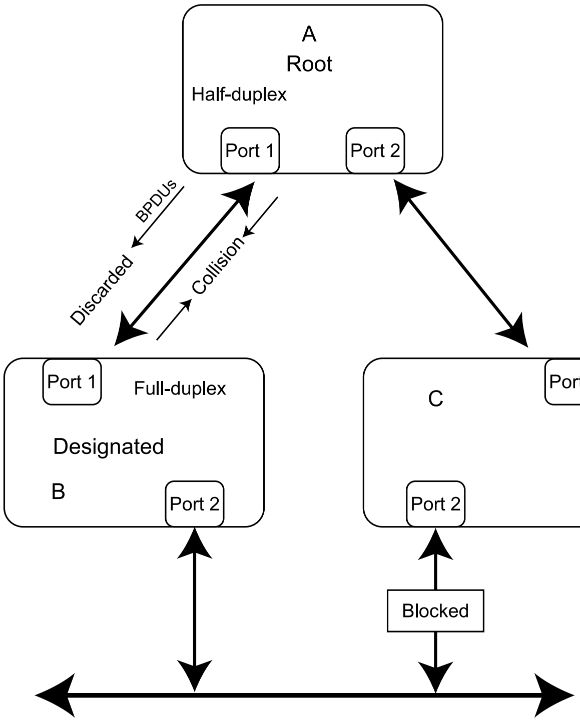


Figure D-7: Example of full/half duplex mismatch

In the above example, Port 1 on B is configured as a full-duplex port, and Port 1 on A is either configured as a half-duplex port, or left in auto-negotiation mode. Because Port 1 on B is configured as a full-duplex port, it does not do the carrier sense when accessing the link. B will then start sending packets even if A is using the link. A will then detect collisions and begin to run the flow control algorithm. If there is enough traffic between B and A, all packets (including BPDUs) will be dropped. If the BPDUs sent from A to B are dropped for longer than the MAX AGE, B will lose its connection to the root (A) and will unblock its connection to C. This will lead to a data loop.

Unidirectional Link

Unidirectional links can be caused by an undetected failure in one side of a fiber cable, or a problem with a ports transceiver. Any failure that allows a link to remain up while providing one-way communication is very dangerous for STP.

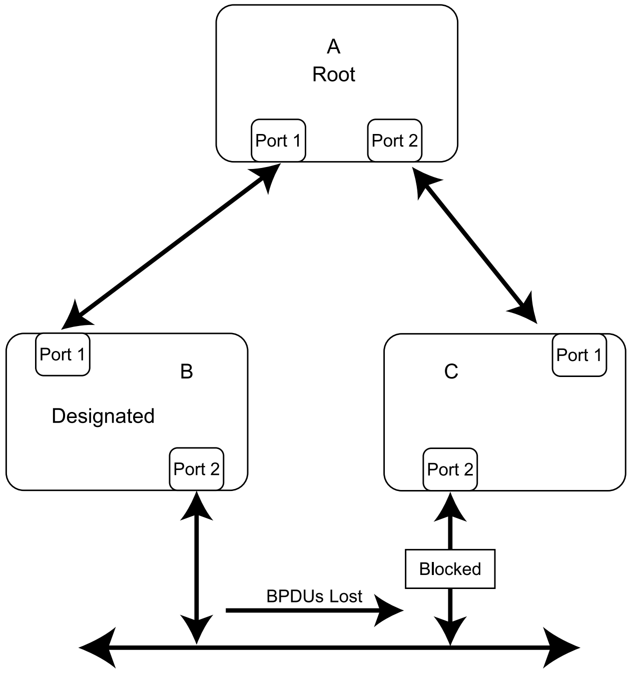


Figure D-8: Example unidirectional link

In this example, Port 2 on B can receive but not transmit packets. Port 2 on C should be in the blocking state, but since it can no longer receive BPDUs from Port 2 on B, it will transition to the forwarding state. If the failure exists at boot, STP will not converge and rebooting the bridges will have no effect.

NOTE: Rebooting would help temporarily in the previous example.

This type of failure is difficult to detect because the link-state LEDs for Ethernet links rely on the transmit side of the cable to detect a link. If a unidirectional failure on a link is suspected, it is usually required to go to the console or other management software and look at the packets received and transmitted for the port. For example, a unidirectional port will have many packets transmitted but none received, or vice versa.

Packet Corruption

Packet corruption can also lead to Spanning Tree Protocol failure. If a link is experiencing a high rate of physical errors, a large number of consecutive BPDUs can be dropped and a port in the blocking state would transition to the forwarding state. The blocking port would have to have the BPDUs dropped for 50 seconds (at the default settings) and a single BPDU would reset the timer. If the Max Age is set too low, this time is reduced.

Resource Errors

The ProLiant BL e-Class C-GbE Interconnect Switch performs its switching and routing functions primarily in hardware, using specialized ASICs. STP is implemented in software and is thus reliant upon the speed of the CPU and other factors to converge. If the CPU is over-utilized, it is possible that BPDUs may not be sent in a timely fashion. STP is generally not very CPU intensive and is given priority over other processes, so this type of error is rare.

Very low values for the Max Age and the Forward Delay can result in an unstable Spanning Tree. The loss of BPDUs can lead to data loops. The diameter of the network can also cause problems. The default values for STP give a maximum network diameter of about seven hops. This means that two switches in the network cannot be more than seven hops apart. Part of this diameter restriction is the BPDU age field. As BPDUs are propagated from the root bridge to the leaves of the spanning tree, each bridge increments the age field. When this field is beyond the maximum age, the packet is discarded. For large diameter networks, STP convergence can be very slow.

Identifying a Data Loop

Broadcast storms have a very similar effect on the network to data loops, but broadcast storm controls in modern switches (along with subnetting and other network practices) have been very effective in controlling broadcast storms. The best way to determine if a data loop exists is to capture traffic on a saturated link and check if similar packets are seen multiple times.

Generally, if all the users of a given domain are having trouble connecting to the network at the same time, a data loop can be suspected. The port utilization data in the switch’s console will give unusually high values in this case.

The priority for most cases is to restore connectivity as soon as possible. The simplest remedy is to manually disable all of the ports that provide redundant links. Disabling ports one at a time, and then checking for a restoration of the user’s connectivity will identify the link that is causing the problem, if time allows. Connectivity will be restored immediately after disabling a data loop.

Avoiding Trouble

Below are some tips for avoiding trouble.

Know Where the Root is Located

Although the STP can elect a root bridge, a well-designed network will have an identifiable root for each VLAN. Careful setup of the STP parameters will lead to the selection of this best interconnect switch as the root for each VLAN. Redundant links can then be built into the network. STP is well suited to maintaining connectivity in the event of a device failure or removal, but is poorly suited to designing networks.

Know Which Links are Redundant

Organize the redundant links and tune the port cost parameter of STP to force those ports to be in the blocking state.

For each VLAN, know which ports should be blocking in a stable network. A network diagram that shows each physical loop in the network and which ports break which loops is extremely helpful.

Minimize the Number of Ports in the Blocking State

A single blocking port transitioning to the forwarding state at an inappropriate time can cause a large part of a network to fail. Limiting the number of blocked ports helps to limit the risk of an inappropriate transition.

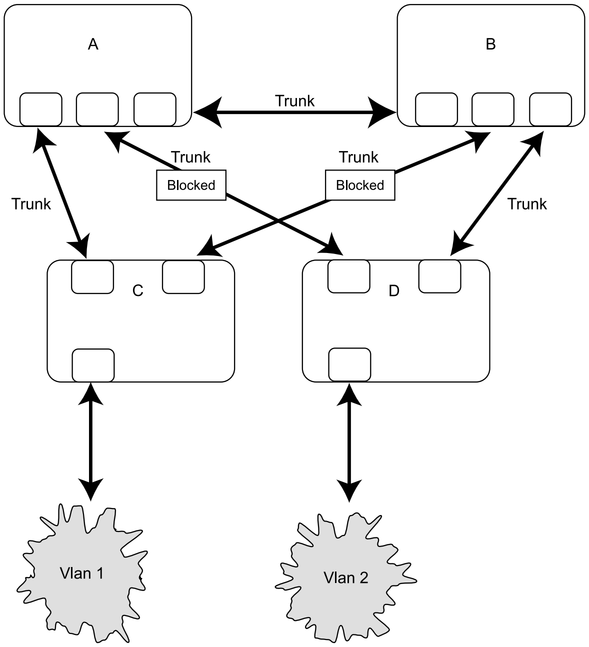


Figure D-9: Example 1: A common network design

The above graphic is an example of a common network design. The switches C and D have redundant links to the backbone switches A and B using trunks. Trunks, by default, carry all the VLAN traffic from VLAN 1 and VLAN 2. So switch C is not only receiving traffic for VLAN 1, but it is also receiving unnecessary broadcast and multicast traffic for VLAN 2. It is also blocking one port for VLAN 2. Thus, there are three redundant paths between switches A and B and two blocked ports per VLAN. This increases the chance of a data loop.

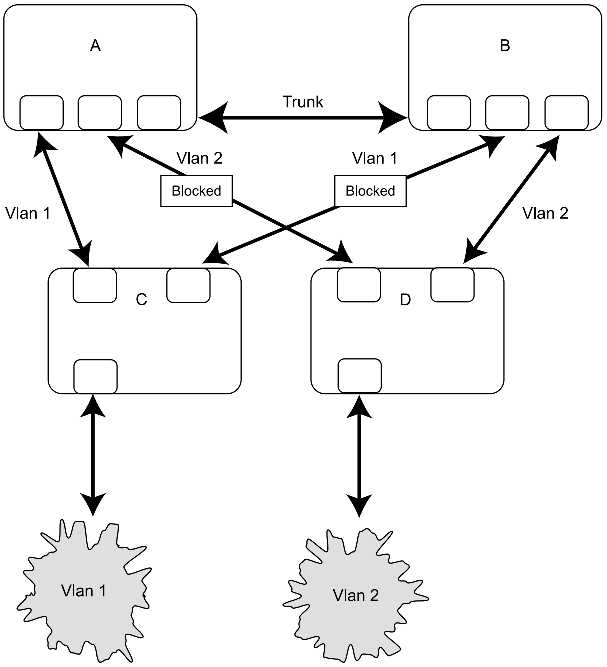


Figure D-10: Example 2: A common network design

In this example, the VLAN definitions are extended to switches A and B. This gives only a single blocked port per VLAN and allows the removal of all redundant links by removing switch A or B from the network.

E

SNMP/RMON MIBs Support

Introduction

Management and counter information are stored in the switch module in the Management Information Base (MIB). The switch module uses the standard MIB-II Management Information Base module. Values for MIB objects can be retrieved from any SNMP-based network management software. In addition to the standard MIB-II, the switch module also supports its own proprietary enterprise MIB as an extended Management Information Base. These MIBs may also be retrieved by specifying the MIB Object-Identity (OID) at the network manager station.

MIB values can be either read-only or read-write.

- Read-only MIB variables can be either constants that are programmed into the switch module or variables that change while the switch module is in operation. Examples of read-only constants include the number and types of ports. Examples of read-only variables are the statistics counters, such as the number of errors that have occurred, or how many kilobytes of data have been received and forwarded through a port.
- Read/write MIB variables are usually related to user-customized configurations. Examples include the IP address of the switch module, Spanning Tree Algorithm parameters, and port status.

SNMP Manager Software

If you use third-party vendor SNMP software to manage the switch module, a diskette listing the propriety enterprise MIBs for the switch can be obtained by request. If your software provides functions to browse or modify MIBs, you can also get the MIB values and change them (if the MIB attributes permit the write operation). This process can be quite involved, however, since you must know the MIB OIDs and retrieve them one by one.

Use an SNMP manager, such as HP OpenView or Tivoli NetView to access the enterprise-specific MIBs. Compile MIBs into the MIB database and then use a MIB browser to navigate them. For detailed information, access the individual descriptions of each MIB or go to the documentation that came with your SNMP manager software.

Standard MIBs

The SNMP agent for the switch module supports the following standard MIBs:

- Bridge MIB (RFC 1493)
- MIB-II (RFC 1213)
- Mini-RMON MIB (RFC 1757)—Groups 1 (Statistics), 2 (History), 3 (Alarm), and 9 (Event)
- 802.1p MIB (RFC 2674)
- 802.1q MIB (RFC 2674)
- Entity MIB (RFC 2737)
- IF-MIB (RFC 2233)
- Ethernet-like MIB (RFC 2358)—dot3StatsTable

Enterprise-Specific MIBs

The SNMP agent for the switch module supports the following enterprise-specific MIBs:

- cpqAgent.mib
    - agentBasicInfo—Basic information for the switch module
    - agentBasicConfig—Basic configuration management
    - agentIpProtoConfig—IP-related configuration management
    - agentIpTrapManager—Setting of the trap manager IP
- cpql2mgt.mib
    - swPortTrunkPackage—Management of the port trunk function
    - swPortMirrorPackage—Management of the port mirroring function
    - swIGMPPackage—Management of the IGMP function
- vesubio.mib
    - swL2BwMgmt—Management of the ingress and egress bandwidth
    - swL2CosMgmt—Management of the Class of Service
    - swL2PortSecurityMgmt—Management of port security
    - dswL2DevMgmt—Management of the device advanced settings
    - swL2PortMgmt—Management of the port link
- cpqSTrap.mib—Defining of trap objects
- CIMTrap.mib—Re-defining “entConfigChange” trap in SNMP

F

Upgrading Firmware through the Serial Port

You can upgrade the system firmware of a switch module by connecting your computer to the serial console port of the Integrated Administrator and using terminal emulation software that supports the ZModem or XModem protocol. This procedure is only necessary if your interconnect switch does not have access to a TFTP server, or if the firmware procedure was previously interrupted and the switch module is not booting properly.

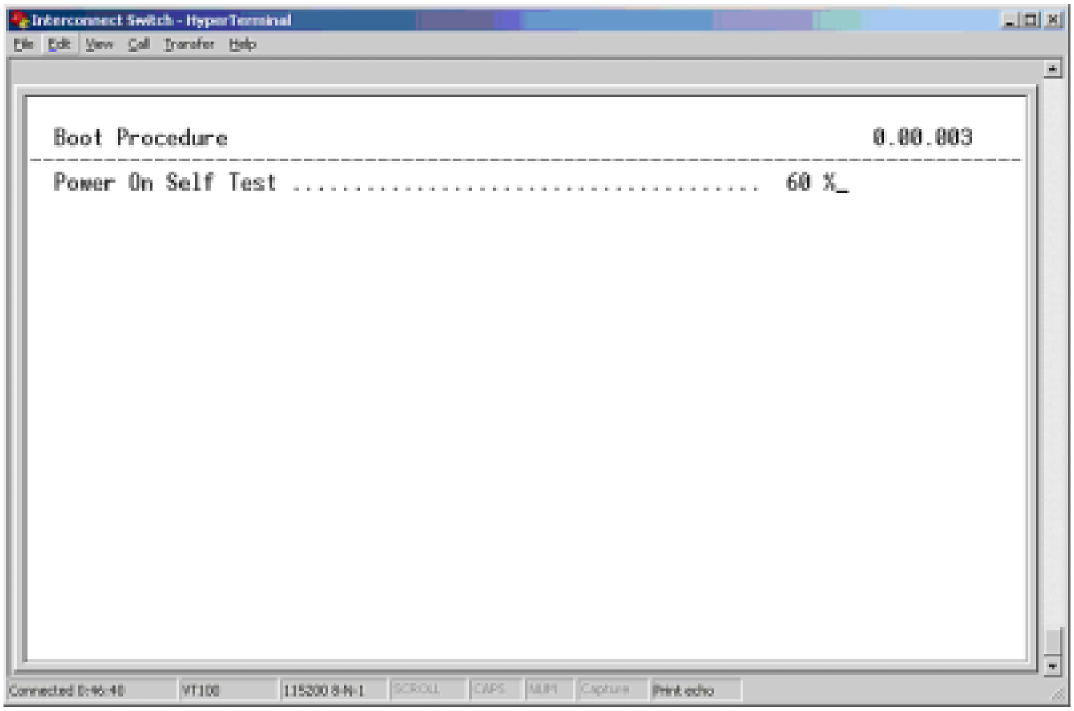
When connecting to a switch module through the Integrated Administrator console port, remember that there are two different serial links involved in the communication path. In addition to the external console port (whose default baud rate is 9600), the Integrated Administrator has an internal serial port that connects to the actual serial console of the switch module (at a default baud rate of 115200). It is only necessary to adjust the baud rate of the external console port and your PC (to 115200 from the default of 9600).

To download a firmware file to a switch module and change the external console port baud rate:

1. From a PC using Microsoft Windows HyperTerminal or any other terminal emulation program, connect to the serial console interface on the switch module at 9600 baud.

NOTE: For information on how to connect to the switch module console interface, see the section “Connecting to the Switch Modules” in Chapter 3.

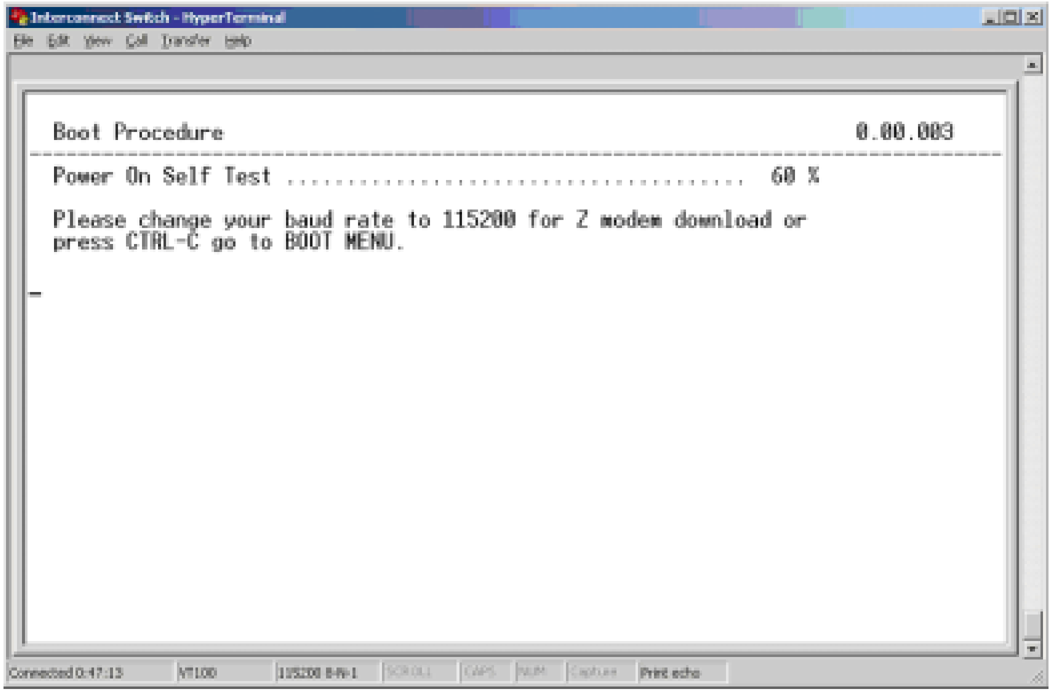
2. Reboot the switch module by using the **Reboot** menu option, or by pressing the connection escape keys (usually **Ctrl+Shift+**_) and accessing the Integrated Administrator **Reboot Switch** option. The boot procedure runs the Power-On Self-Test (POST) and a screen similar to the following is displayed.



```
Boot Procedure                                                 0.00.003
-------------------------------------------------------------------------
Power On Self Test ......................................  60 %_
```

Figure F-1: POST message

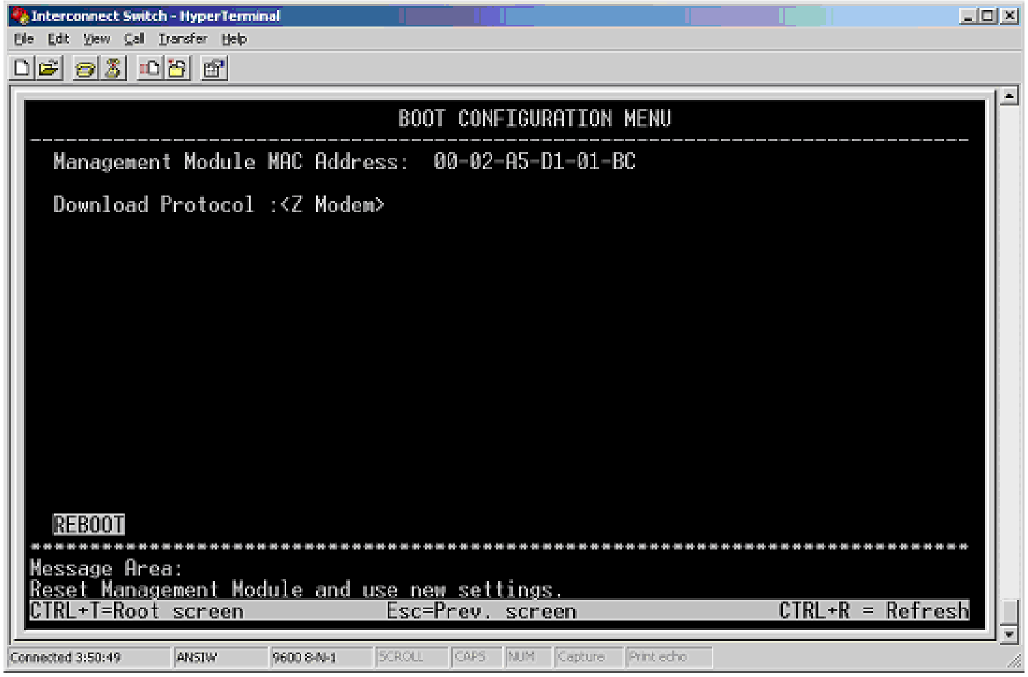
3. Press the **pound (#)** key as soon as you see the **Boot Procedure** header. This action forces the switch module into the download mode. A screen similar to the following is displayed.


Interconnect Switch - HyperTerminal
File Edit View Call Transfer Help
Connected 0:47:13
VT100
115200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
 Boot Procedure                                                 0.00.003
--------------------------------------------------------------------------
 Power On Self Test .....................................  60 %

 Please change your baud rate to 115200 for Z modem download or
 press CTRL-C go to BOOT MENU.

_
```

Figure F-2: Download mode message

4. Configure the download protocol (ZModem or XModem) or use the default boot configuration settings.
    a. To change the baud rate, press **Ctrl+C** to display the **Boot Configuration Menu.**
    b. To use the default boot configuration settings, go to step 10.



```
                         BOOT CONFIGURATION MENU
 ------------------------------------------------------------------------------
   Management Module MAC Address:  00-02-A5-D1-01-BC

   Download Protocol :<Z Modem>










   REBOOT
 ******************************************************************************
 Message Area:
 Reset Management Module and use new settings.
 CTRL+T=Root screen             Esc=Prev. screen              CTRL+R = Refresh
```

Figure F-3: Boot Configuration menu

5. Select **XModem** or **ZModem** as the download protocol.
6. Highlight **Reboot.**
7. Press the **Enter** key. The switch module reboots.

8. While the switch module is rebooting, press the **pound (#)** key again to force the switch module into download mode. The download mode message is displayed. (See Figure F-2.)

   NOTE: For faster transfers, you may want to change the speed of your console connection from 9600 to 115200.

9. Press the Integrated Administrator escape character **<Ctrl>_**. The following Integrated Administrator connect menu is displayed:

```
---------------------------------------------------------------------------------------------------------
Command: D)isconnect, C)hange settings, R)eboot Switch, E)xit
command mode >

---------------------------------------------------------------------------------------------------------
```

10. Press the following keys in sequence to change the settings: **C L C B I**

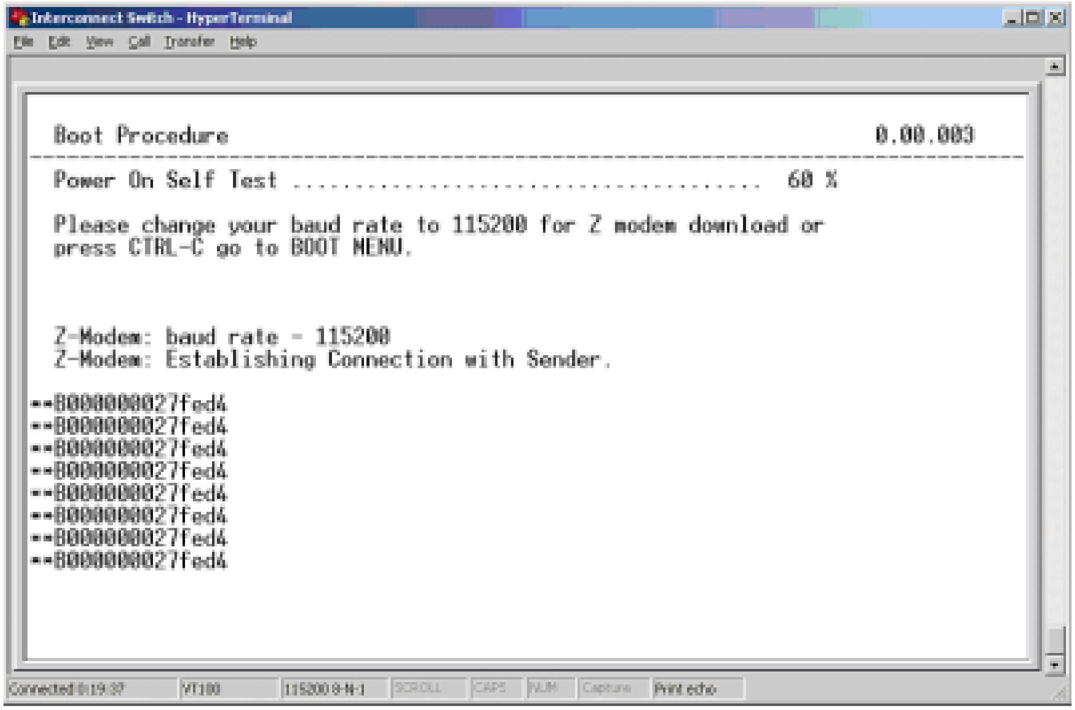
    Your screen displays the following lines:

```
---------------------------------------------------------------------------------------------------------
Command: D)isconnect, C)hange settings, R)eboot Switch, E)xit
command mode > C

Change settings for: L)ocal Session, R)emote Port [Switch B],
E)xit > L

Change Local: C)ommunication Settings, D)isable Escape Character,
E)xit > C

Settings: B)audrate; flow control: N)one H)ardware S)oftware;
E)xit > B

Baud: A)1200 B)2400 C)4800 D)9600 F)19200 G)38400 H)57600
I)115200; E)xit > I

All communication setting changes are only temporary, and defaults
are restored at exit.

---------------------------------------------------------------------------------------------------------
```

11. Change your local speed to 115200, and press the **Enter** key to continue.
12. Change the baud rate of your HyperTerminal session and press the **Enter** key.

    After the switch module is in the download mode and the baud rates are configured properly, a connection-established message is displayed.

IMPORTANT: If the following screen displays nonsense characters, then a mismatched baud rate configuration has occurred. Check HyperTerminal to see if the baud rate setting on the switch module console interface and the HyperTerminal are mismatched.


Interconnect Switch - HyperTerminal
File Edit View Call Transfer Help
Connected 0:19:37
VT100
115200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
  Boot Procedure                                                0.00.003
-------------------------------------------------------------------------
  Power On Self Test .....................................  60 %

  Please change your baud rate to 115200 for Z modem download or
  press CTRL-C go to BOOT MENU.


  Z-Modem: baud rate - 115200
  Z-Modem: Establishing Connection with Sender.

**B0000000027fed4
**B0000000027fed4
**B0000000027fed4
**B0000000027fed4
**B0000000027fed4
**B0000000027fed4
**B0000000027fed4
**B0000000027fed4
```

Figure F-4: Connection-established message

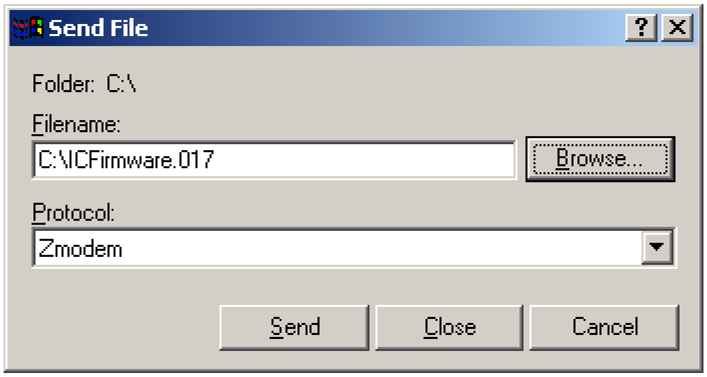
13. Before beginning the ZModem transfer, disable the Integrated Administrator escape character to ensure a transparent connection for the file transfer. To disable this character, press the following keys:

    Ctrl+_ C L D

    Your screen displays the following lines:

    ```
    ----------------------------------------------------------------
    Command: D)isconnect, C)hange settings, R)eboot Switch, E)xit
    command mode > C
    Change settings for: L)ocal Session, R)emote Port [Switch B],
    E)xit >L
    Change Local: C)ommunication Settings, D)isable Escape Character,
    E)xit > D

    The Escape Character <Ctrl>_ is now disabled.  To re-enable it,
    you must
    press <Ctrl>_ twelve times in sequence.

    Press [Enter] to continue:

    ----------------------------------------------------------------
    ```

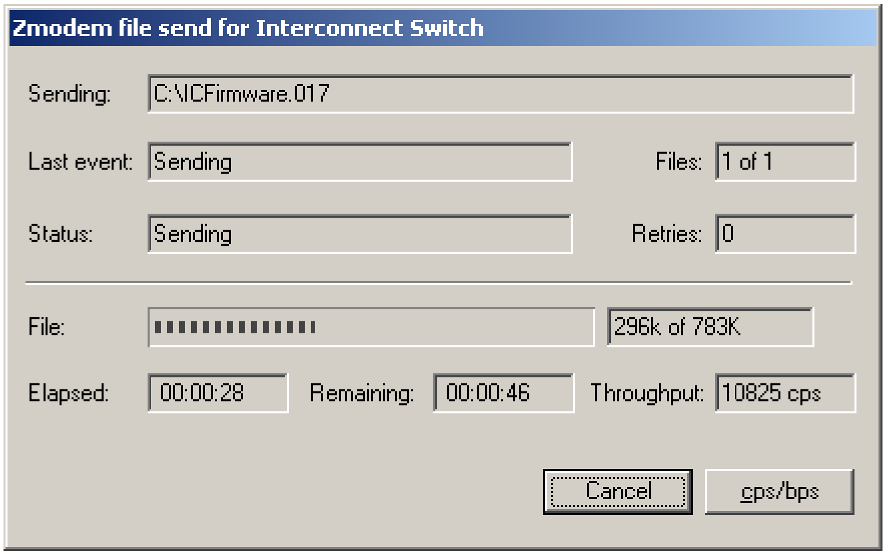
14. Press the **Enter** key to continue.
15. From the **Interconnect Switch HyperTerminal** window menu, select **Transfer,** then **Send File.** The following window is displayed.



Folder: C:\
Filename: C:\ICFirmware.017
Protocol: Zmodem

Figure F-5: Send File window

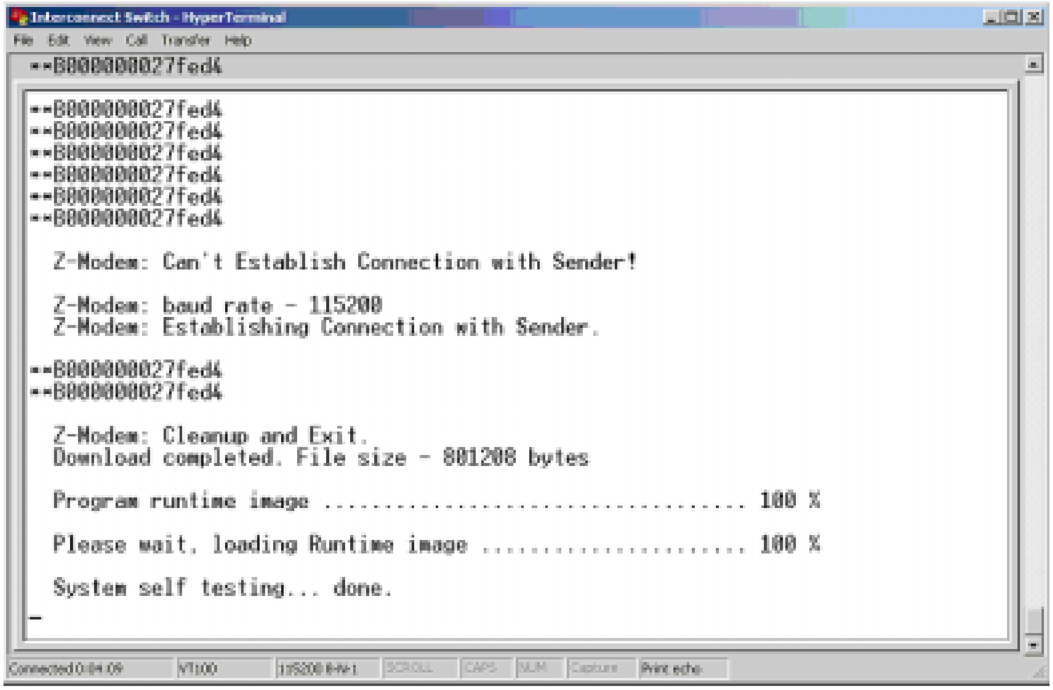
16. Click **Browse** and select the firmware file to be downloaded to the switch module.
17. Select the download protocol from the drop-down menu.
18. Click **Send** to start the download process. The following screen is displayed.



Sending: C:\ICFirmware.017
Last event: Sending
Files: 1 of 1
Status: Sending
Retries: 0
File: 296k of 783K
Elapsed: 00:00:28
Remaining: 00:00:46
Throughput: 10825 cps

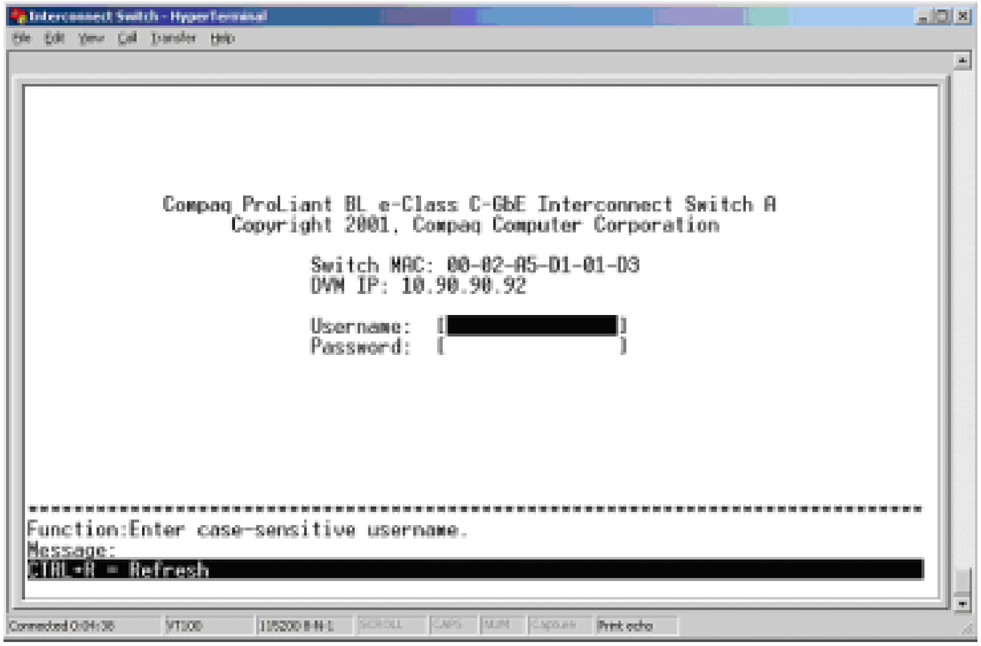
Figure F-6: ZModem file send for Interconnect Switch window

After the firmware file transfer is complete, a download-completed message is displayed and then the interconnect login screen is displayed.


Interconnect Switch - HyperTerminal
File Edit View Call Transfer Help
Connected 0:04:09
VT100
115200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
**B000000027fed4

**B000000027fed4
**B000000027fed4
**B000000027fed4
**B000000027fed4
**B000000027fed4
**B000000027fed4

  Z-Modem: Can't Establish Connection with Sender!

  Z-Modem: baud rate - 115200
  Z-Modem: Establishing Connection with Sender.

**B000000027fed4
**B000000027fed4

  Z-Modem: Cleanup and Exit.
  Download completed. File size - 801208 bytes

  Program runtime image ................................... 100 %

  Please wait, loading Runtime image ...................... 100 %

  System self testing... done.
_
```

Figure F-7: Download-completed message


Interconnect Switch - HyperTerminal
File Edit View Call Transfer Help
Connected 0:04:38
VT100
115200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
          Compaq ProLiant BL e-Class C-GbE Interconnect Switch A
               Copyright 2001, Compaq Computer Corporation

                           Switch MAC: 00-02-A5-D1-01-D3
                           DVM IP: 10.90.90.92

                           Username:  [               ]
                           Password:  [               ]



*******************************************************************************
Function:Enter case-sensitive username.
Message:
CTRL+R = Refresh
```

Figure F-8: ProLiant BL e-Class C-GbE Interconnect Switch login screen

19. Close your connection with the Integrated Administrator, which will reset the Integrated Administrator console port to 9600 baud (if you changed the speed previously).

20. Press the **Ctrl+_** keys twelve times in sequence to re-enable the escape character. The following text is displayed:

```
-----------------------------------------------------------------
Command: D)isconnect, C)hange settings, R)eboot Switch, E)xit
command mode
-----------------------------------------------------------------
```

21. Press the **D** key to disconnect your session. If you changed the speed previously, you must reset your terminal to 9600 baud to continue. The following text is displayed:

```
-----------------------------------------------------------------
Command: D)isconnect, C)hange settings, R)eboot Switch, E)xit
command mode > D
The console speed is being set back to 9600 bps.
Change your local speed back to 9600 and press [Enter] to continue

-----------------------------------------------------------------
```

22. Press the **Enter** key to close your connection to the switch module.

G

Troubleshooting

This section provides information on solutions to problems that may occur during the configuration and operation of Proliant BL e-Class C-GbE Interconnect Switch. The following table lists steps you should take before calling your service representative.

Following are four tables with basic troubleshooting information:

- **Setting Up and Accessing**—Table G-1 contains general troubleshooting information about setting up and accessing the interconnect switch. Topics covered include LEDs, cables, failure of the interconnect switch to get IP settings, failure to connect to the interconnect switch remotely, and what to do if you forget your administrator user name and password.
- **Configuring**—Table G-2 contains general troubleshooting information about configuring the interconnect switch. Topics covered include configuring VLANs and XConnect ports.
- **Using the TFTP Server**—Table G-3 contains general troubleshooting information about using a TFTP server to backup interconnect switch configuration or to configure multiple interconnect switches.
- **Upgrading Firmware using the Serial Port**—Table G-4 contains general troubleshooting information about upgrading system firmware using the serial console port.

For additional troubleshooting information:

- See Appendix D, Spanning Tree Protocol
- Visit the Compaq website:

  www.compaq.com/support/

Table G-1: Troubleshooting: Setting Up and Accessing

Problem	Possible Cause	Possible Solution
Forgot the administrator user name and password that you configured on the interconnect switch.	• Unknown	• Call Compaq technical support at 1-800-OKCOMPAQ or your service representative and provide your interconnect switch MAC address (available on the MAC address label attached to your interconnect switch) to get a unique switch password. This password gives you Root privileges. After receiving the password, do the following: 1. Reboot the switch module. 2. Access the console interface. 3. Within 60 seconds of when the Logon screen displays, type the password in the **Password** field. 4. Leave the **Username** field blank. 5. Press the **Enter** key. The main menu will be displayed. 6. Access the **User Accounts Management** option and set a new Administrator password. (See Chapter 3.)
		• Interconnect Switch configuration, you can reload the factory default settings: 1. Power off the system. 2. Power on the system. The console interface logon screen is displayed. 3. In the **Username** field, do the following very quickly: Press the **Esc** key and type `D L K s` 4. At the **>** prompt, type `FactoryReset` A message is displayed indicating the system is rebooting. The factory defaults reload and the switch module reboots. 5. Follow the directions to log on to the switch module for the first time. See “Logging on to the Switch Module” in Chapter 3.

continued

Table G-1: Troubleshooting: Setting Up and Accessing *continued*

Problem	Possible Cause	Possible Solution
Power LED on the interconnect switch is not on.	• Interconnect switch is not seated properly.	• Make sure interconnect switch is inserted completely and seated properly.
	• Server blade enclosure is not powered up.	• Make sure the server blade enclosure is powered up and all the power connections are intact.
No link LED displays, even after you plug in the Category 5 cable in the external port's RJ-45 connector.	• The cable is not properly plugged in.	• Check if the cable is plugged in and seated properly.
	• The cable or connector heads are faulty.	• Replace with another tested cable.
	• The RJ-45 connector on the switch or LED is faulty.	• After checking all the above, if no link LED displays, check whether the port is transferring data. If yes, the LED is faulty. If no, it could be a faulty RJ-45 connector. Call your service representative.
Cannot access the interconnect switch serial console interface via the Integrated Administrator using null modem connection from a PC Terminal Emulation Program.	• Null modem cable has a problem.	• Make sure you use the null modem cable provide by Compaq Computer Corporation with this hardware.
	• Connection settings do not match the Integrated Administrator serial settings.	• Make sure the PC Terminal Emulation session settings match the Integrated Administrator serial settings. **NOTE:** Refer to Chapter 3 for default serial settings if you are connecting to the interconnect switch via the Integrated Administrator serial port for the first time.
Error message that the interconnect switch failed to complete the system self-testing is displayed on the serial console screen.	• System diagnostic tests failed.	• Note the reason for failure from the serial console screen message and call your service representative.
Keyboard locks up when using HyperTerminal to logon to the switch module through the console interface.	• Scroll lock is set on.	• Press the Scroll Lock key on the keyboard and make sure that scroll lock is off.

continued

Table G-1: Troubleshooting: Setting Up and Accessing *continued*

Problem	Possible Cause	Possible Solution
The interconnect switch fails to get its IP settings from DHCP server, even though by default it is configured for DHCP. **NOTE:** If you are running in spanning tree mode, it can take 60-90 seconds for the switch module to get its IP settings.	• The interconnect switch is not connected properly to the network.	• Check the cable and connections and make sure there is network connectivity between the interconnect switch and the DHCP server.
	• The DHCP server is not available on the network or VLAN that is attached to the switch management port.	• Make sure DHCP server is present on the network or VLAN attached to the interconnect switch.
	• The DHCP server is not able to offer IP settings to the interconnect switch as it is out of available IP addresses.	• Make sure the IP addresses are available.
	• The interconnect switch timed out its request for IP settings.	• Go to the **Switch IP Settings** screen and click **Apply,** to make the interconnect switch retry DHCP. • Reset/reboot the interconnect switch.
Cannot connect to the interconnect switch console interface remotely using Telnet.	• The interconnect switch IP address may not be configured or correct.	• From the serial console interface, on the **Switch IP Settings** screen, make sure that the interconnect switch IP address is configured and valid on your network. • Use the correct IP address to establish the Telnet connection with the interconnect switch.
	• The setting allowing access to the interconnect switch using the Telnet interface is disabled.	• From the serial console interface, on the **Advanced Switch Settings** screen, make sure the Telnet interface is enabled.
	• The Security IP list (if used) does not contain the IP address of your management station.	• From the **SNMP Manager Configuration** screen, make sure that security IP list or Management IP Station list has the IP address of your management station.

continued

Table G-1: Troubleshooting: Setting Up and Accessing *continued*

Problem	Possible Cause	Possible Solution
Cannot connect to the interconnect switch remotely using the Web interface.	• The interconnect switch IP address may not be configured or correct.	• From the serial console interface, on the **Switch IP Settings** screen, make sure that the interconnect switch IP address is configured and valid on your network. • Use the correct IP address to establish the Web connection with the interconnect switch.
	• Accessing the interconnect switch using Web interface is disabled.	• From the serial console interface, on the **Advanced Switch Settings** screen, make sure the Web interface is enabled.
	• The Proxy server settings are configured on your Internet browser and your proxy server does not know the interconnect switch IP address.	• Disable the manual proxy settings on your Internet browser and let it automatically find Web servers using the IP address.
	• The Security IP list (if used) does not contain the IP address of your management station.	• From the **Security IP settings** screen, make sure that security IP list or Management IP Station list has the IP address of your management station.
Cannot connect to the interconnect switch SNMP interface.	• The interconnect switch IP address may not be configured or correct.	• From the serial console interface, on the **Switch IP Settings** screen, make sure that the interconnect switch IP address is configured and valid on your network. • Use the correct IP address to establish the SNMP connection with the interconnect switch.
	• The Security IP list (if used) does not contain the IP address of your management station.	• From the **Security IP settings** screen, make sure that security IP list or Management IP Station list has the IP address of your management station.
Cannot connect to the interconnect switch management interface via the Telnet, Web, or SNMP interfaces. The IP configuration, including address settings, is valid and the VLANs are configured correctly.	• The internal switch CPU port (meant for supporting switch management interfaces) and the port you have connected to access the switch from the Telnet, Web, or SNMP interfaces are not in the same VLAN.	• Check and make sure that the Management VLAN ID on the **Switch IP Settings** screen is the same as the VLAN ID of the port that is trying to make the Telnet, Web, or SNMP connection. If not, change it to match.

Table G-2: Troubleshooting: Configuring

Problem	Possible Cause	Possible Solution
After connecting more than one port to another switch or destination device, the port activity LEDs continuously indicate activity.	• Since there are multiple links across this device and the destination device, they form loops, which cause broadcast storms.	• From the **Configure Spanning Tree settings** screen, enable STP at switch level. From the **Port Spanning Tree settings** screen, enable STP at port level, if you want multiple links. Make sure that the Bypass setting is disabled. This will avoid loops and maintain standby links for resilience in case the primary links go down.
While configuring VLANs, you cannot enable a port in multiple VLANs.	• A port can be part of only one VLAN unless the port is a tagged port.	• Make sure that your VLANs are 802.1Q VLANs and enable the port as a tagged port from the **802.1Q Static VLAN Settings** screen on console interface, or the **VLAN settings** screen on Web-based interface.
After assigning a port to multiple 802.1Q VLANs by configuring it as tagged port, you check the PVID. It is equal to the first VLAN ID.	• For port-based VLANs, ports belong to only one VLAN and only one PVID can be assigned. Port-based VLANs can be extended to other switches by cross connecting ports that have the same PVID (the same Port based VLAN).	• By default, all the ports have PVID 1. The switch assigns to the port a PVID that is equal to the VLAN ID of the first VLAN that the port was enabled in. To manually configure a Port VLAN, see “Configuring a Port VLAN” in Chapter 3 (console management interface) and Chapter 4 (Web-based management interface.)
Changing the first XConnect port settings changes the next XConnect port settings. But changes to the second XConnect port settings cannot be applied or saved.	• By default, XConnect ports are bundled into a Multilink Trunk.	• Since they are bundled into a trunk, the settings of the first port are referenced and applied to the reset of the ports. So in a trunk, only the first port (reference port) is configurable and defines the characteristics of the other ports in the trunk.
While assigning the ports to VLANs, the interconnect switch does not let the user enable two adjacent ports into two different VLANs.	• The ports could be two adjacent ports that are bundled in a multilink trunk.	• Two ports that are assigned to a multilink trunk cannot be assigned to two different VLANs. Either break the trunk to assign it two different VLANs or assign the ports to one VLAN.
After forcing the speed, duplex, and flow control on the port, the link does not come up and transfer data properly.	• Both sides need to be forced to the same settings. In case of auto-negotiation, both sides will negotiate and match the setting to make the correct link.	• From the **Configure Ports** screen, make sure the ports are forced to the same setting as the setting on the other end of the link.

Table G-3: Troubleshooting: Using a TFTP Server

Problem	Possible Cause	Possible Solution
While using TFTP to download firmware, the interconnect switch fails to connect to the TFTP server or after connection the download fails.	• The TFTP server is not available to connect or there is connectivity failure between the switch and TFTP server.	• Make sure the IP address of the TFTP server is correct. • Make sure that the TFTP server exists on the same network or VLAN as the interconnect switch. • Make sure that you can ping the TFTP server from the interconnect switch and vice versa.
	• The firmware file is not found on the TFTP server. The file name could be wrong and is mismatching.	• Make sure that a valid firmware file exists on the TFTP server to download to the interconnect switch. • On the interconnect switch, check the file name you configured to download.
While using TFTP to download or upload a configuration file, the interconnect switch fails to connect to the TFTP server, or after connection the download or upload fails.	• The TFTP server is not available to connect or there is a connectivity failure between the interconnect switch and the TFTP server.	• Make sure that TFTP server exists on the same network or VLAN as that of the switch. • Make sure that you can ping TFTP server from the switch and vice versa. • Make sure the IP address of the TFTP server is correct.
	• The configuration file is not found on the TFTP server. The file name could be wrong and is mismatching.	• Make sure that a valid configuration file exists on the TFTP server to download to the interconnect switch. • On the interconnect switch, check the file name you configured to download or upload.
While using TFTP to save the history log, the interconnect switch fails to connect to the TFTP server or after connection the download fails	• The TFTP server is not available to connect or there is connectivity failure between the interconnect switch and the TFTP server.	• Make sure the IP address of the TFTP server is correct. • Make sure that the TFTP server and the interconnect switch are on the same network or VLAN. • Make sure that you can ping the TFTP server from the interconnect switch and vice versa.

Table G-4: Troubleshooting: Upgrading Firmware using the Serial Port

Problem	Possible Cause	Possible Solution
On the serial console screen, a message that interconnect switch failed to load runtime image (firmware) is displayed.	• Runtime image (firmware file) got corrupted.	• Download the new runtime image (firmware file) using the procedure in Appendix F.
	• Flash file system went bad partially.	• Call your service representative.
From the serial console, pressing the pound (#) key during boot procedure does not force the interconnect switch into the download mode.	• You did not press the pound (#) key during the time the boot procedure responds to this special key.	• Make sure to press the pound (#) key immediately when you see the boot procedure starting POST. Pressing the pound (#) key in the middle of POST puts the interconnect switch into the download mode instead of the runtime mode.
After forcing the interconnect switch into the download mode, the console screen displays a message to change your terminal emulation session's baud rate for ZModem transfer and also displays unusual characters.	• Your terminal emulation session baud rate does not match the interconnect switch serial console baud rate in the download mode.	• Change your terminal emulation session's baud rate to match the interconnect switch serial console baud rate in the download mode. **NOTE:** The baud rate for the interconnect switch serial console in the download mode and runtime mode are two separate settings.
After starting to download the firmware file, download fails.	• The firmware file is not the correct one or got corrupted.	• Make sure to get the latest firmware file that is meant for this interconnect switch. • Make sure the file size matches the original one on the media you received with this file.
Interconnect switch configuration is corrupted.	• An error was made when saving the interconnect switch configuration.	• Reboot the interconnect switch and reload the factory settings. This clears all settings and restores them to their initial values that were present when the interconnect switch was purchased. See "Rebooting the Switch Module" in Chapter 3 (console management interface) or "Resetting the Switch Module Configuration to Factory Defaults" in Chapter 4 (Web-based interface). **NOTE:** You will have the option to reset all settings except the IP address. After reloading the factory settings, reconfigure the switch settings.

H

Regulatory Compliance Notices

Federal Communications Commission Notice

Part 15 of the Federal Communications Commission (FCC) Rules and Regulations has established Radio Frequency (RF) emission limits to provide an interference-free radio frequency spectrum. Many electronic devices, including computers, generate RF energy incidental to their intended function and are, therefore, covered by these rules. These rules place computers and related peripheral devices into two classes, A and B, depending upon their intended installation. Class A devices are those that may reasonably be expected to be installed in a business or commercial environment. Class B devices are those that may reasonably be expected to be installed in a residential environment (for example, personal computers). The FCC requires devices in both classes to bear a label indicating the interference potential of the device as well as additional operating instructions for the user.

The rating label on the device shows which class (A or B) the equipment falls into. Class B devices have an FCC logo or FCC ID on the label. Class A devices do not have an FCC logo or FCC ID on the label. Once the class of the device is determined, refer to the following corresponding statement.

Class A Equipment

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at personal expense.

Class B Equipment

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio or television technician for help.

Modifications

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by Compaq Information Technologies Group, L.P., may void the user's authority to operate the equipment.

Cables

Connections to this device must be made with shielded cables with metallic RFI/EMI connector hoods in order to maintain compliance with FCC Rules and Regulations.

Declaration of Conformity for Products Marked with the FCC Logo—United States Only

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For questions regarding your product, contact:

Compaq Computer Compaq Information Technologies Group, L.P.
P. O. Box 692000, Mail Stop 530113
Houston, Texas 77269-2000

Or, call

1-800- 652-6672 (1-800-OK COMPAQ). For continuous quality improvement, calls may be recorded or monitored.

For questions regarding this FCC declaration, contact:

Compaq Information Technologies Group, L. P.
P. O. Box 692000, Mail Stop 510101
Houston, Texas 77269-2000

Or, call

(281) 514-3333

To identify this product, refer to the part, series, or model number found on the product.

Canadian Notice (Avis Canadien)

Class A Equipment

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Class B Equipment

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

European Union Notice

Products bearing the CE marking comply with the EMC Directive (89/336/EEC) and the Low Voltage Directive (73/23/EEC) issued by the Commission of the European Community and if this product has telecommunication functionality, the R&TTE Directive (1999/5/EC).

Compliance with these directives implies conformity to the following European Norms (in parentheses are the equivalent international standards and regulations):

- EN 55022 (CISPR 22)—Electromagnetic Interference
- EN55024 (IEC61000-4-2, 3, 4, 5, 6, 8, 11)—Electromagnetic Immunity
- EN61000-3-2 (IEC61000-3-2)—Power Line Harmonics
- EN61000-3-3 (IEC61000-3-3)—Power Line Flicker
- EN 60950 (IEC 60950)—Product Safety

Taiwanese Notice

警告使用者：

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Japanese Notice

ご使用になっている装置にVCCIマークが付いていましたら、次の説明文をお読み下さい。

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

VCCIマークが付いていない場合には、次の点にご注意下さい。

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です　この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Index