



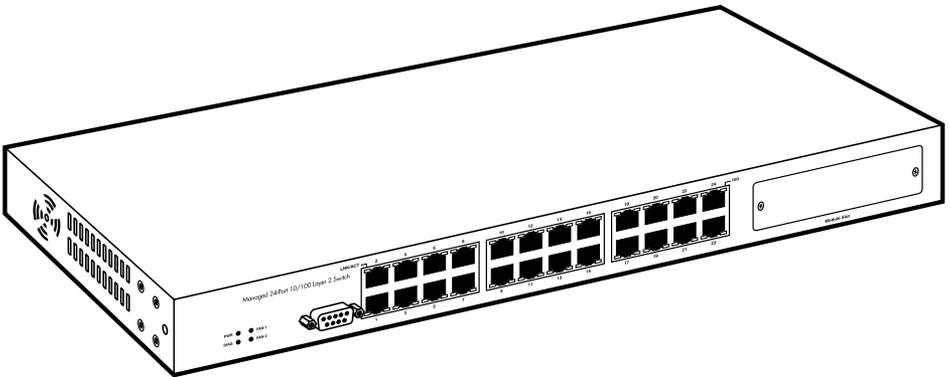
© Copyright 2005. Black Box Corporation. All rights reserved.

---

1000 Park Drive • Lawrence, PA 15055-1018 • 724-746-5500 • Fax 724-746-0746



# 24-Port 10/100 Managed Switch with Gigabit Uplink Port Multimode Gigabit Uplink Module Single-Mode Gigabit Uplink Module Installation Guide



**CUSTOMER  
SUPPORT  
INFORMATION**

Order toll-free in the U.S.: Call **877-877-BBOX** (outside U.S. call **724-746-5500**)  
FREE technical support 24 hours a day, 7 days a week: Call **724-746-5500** or fax **724-746-0746**  
Mailing address: **Black Box Corporation**, 1000 Park Drive, Lawrence, PA 15055-1018  
Web site: [www.blackbox.com](http://www.blackbox.com) • E-mail: [info@blackbox.com](mailto:info@blackbox.com)



**FEDERAL COMMUNICATIONS COMMISSION  
AND  
INDUSTRY CANADA  
RADIO FREQUENCY INTERFERENCE STATEMENTS**

This equipment generates, uses, and can radiate radio-frequency energy, and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio communication. It has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart B of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be necessary to correct the interference.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

*This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of Industry Canada.*

*Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par Industrie Canada.*

**EUROPEAN UNION DECLARATION OF CONFORMITY**

This equipment complies with the requirements of the European EMC Directive 89/336/EEC.



**NORMAS OFICIALES MEXICANAS (NOM)  
ELECTRICAL SAFETY STATEMENT**

**INSTRUCCIONES DE SEGURIDAD**

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.
2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.
3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.
4. Todas las instrucciones de operación y uso deben ser seguidas.
5. El aparato eléctrico no deberá ser usado cerca del agua—por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc..
6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.
7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.
8. Servicio—El usuario no debe intentar dar servicio al equipo eléctrico más allá a lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.
9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.
10. El equipo eléctrico deber ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.
11. El aparato eléctrico deberá ser conectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.

12. Precaución debe ser tomada de tal manera que la tierra física y la polarización del equipo no sea eliminada.
13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.
14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.
15. En caso de existir, una antena externa deberá ser localizada lejos de las líneas de energía.
16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.
17. Cuidado debe ser tomado de tal manera que objetos líquidos no sean derramados sobre la cubierta u orificios de ventilación.
18. Servicio por personal calificado deberá ser provisto cuando:
  - A: El cable de poder o el contacto ha sido dañado; u
  - B: Objetos han caído o líquido ha sido derramado dentro del aparato; o
  - C: El aparato ha sido expuesto a la lluvia; o
  - D: El aparato parece no operar normalmente o muestra un cambio en su desempeño; o
  - E: El aparato ha sido tirado o su cubierta ha sido dañada.

### TRADEMARKS USED IN THIS MANUAL

AppleTalk and EtherTalk are registered trademarks of Apple Computer, Inc.

IPX is a trademark, and Novell is a registered trademark, of Novell, Inc.

Telnet is a trademark of Telnet Communications, Inc.

*Any other trademarks mentioned in this manual are acknowledged to be the property of the trademark owners.*

# Contents

Chapter	Page
1. Specifications .....	8
2. Overview .....	10
2.1 Introduction .....	10
2.2 What's Included .....	10
2.3 Typical Applications .....	11
2.3.1 Building-to-Building (Small Campus) .....	11
2.3.2 Enterprise Server Aggregation .....	12
2.3.3 LAN Switch .....	12
3. About the Technology .....	13
3.1 Gigabit Ethernet .....	13
3.2 Fast Ethernet .....	13
3.3 Switching .....	14
3.4 VLAN (Virtual Local Area Network) .....	14
4. Installation .....	15
4.1 Rackmounting .....	15
4.2 Install the Gigabit Uplink Module (Optional) .....	15
4.3 Connecting Network Cable .....	15
4.4 Applying AC Power .....	16
5. Operation .....	17
5.1 Front-Panel Components .....	17
5.2 Rear-Panel Components .....	19
6. Web Management .....	20
6.1 Overview .....	20
6.2 Home Page .....	21
6.2.1 Basic .....	21
6.2.2 Advanced .....	22
6.2.3 Misc .....	25
6.3 Main Menu .....	25
6.4 System Details .....	26
6.4.1 System Information .....	26
6.4.2 Console Information .....	26
6.4.3 IP Address .....	27
6.5 Port Management .....	28

# Contents (continued)

<b>Chapter</b>	<b>Page</b>
6.5.1	Port Configuration . . . . . 28
6.5.2	Port Trunking . . . . . 31
6.5.3	Port Mirroring . . . . . 35
6.5.4	Port Status . . . . . 38
6.5.5	Port Statistics . . . . . 40
6.6	Bridge Management . . . . . 41
6.6.1	Filtering . . . . . 41
6.6.2	Spanning Tree . . . . . 45
6.6.3	VLAN Configuration . . . . . 50
6.6.4	802.1x Configuration . . . . . 58
6.6.5	SNMP Configuration . . . . . 63
6.7	User Management . . . . . 64
6.8	System Restart . . . . . 65
6.8.1	Reset to Default . . . . . 65
6.8.2	System Reboot . . . . . 66
6.8.3	Firmware Management . . . . . 66
6.9	Network Tree . . . . . 68
7.	Console 1K Xmodem Update Firmware . . . . . 69
8.	Console Menu Line . . . . . 72
8.1	Main Menu . . . . . 74
8.2	Switch Static Configuration . . . . . 74
8.2.1	Port Configuration . . . . . 75
8.2.2	Trunk Configuration . . . . . 77
8.2.3	VLAN Configuration . . . . . 78
8.2.4	Misc Configuration . . . . . 86
8.2.5	Administration Configuration . . . . . 92
8.2.6	Port Mirroring Configuration . . . . . 100
8.2.7	Priority Configuration . . . . . 101
8.2.8	MAC Address Configuration . . . . . 104
8.3	Protocol Related Configuration . . . . . 111
8.3.1	Spanning Tree Protocol (STP) . . . . . 112
8.3.2	SNMP . . . . . 115
8.3.3	GVRP . . . . . 119
8.3.4	IGMP . . . . . 120
8.3.5	LACP . . . . . 121
8.3.6	802.1x Protocol . . . . . 124

Chapter	Page
8.4	Status and Counters . . . . . 128
8.4.1	Port Status . . . . . 129
8.4.2	Port Counters. . . . . 130
8.4.3	System Information. . . . . 131
8.4.4	Network Information . . . . . 132
8.5	Reboot Switch . . . . . 133
8.5.1	Default . . . . . 133
8.5.2	Restart. . . . . 133
8.6	TFTP Update Firmware . . . . . 134
8.6.1	TFTP Update Firmware . . . . . 135
8.6.2	TFTP Restore Configuration . . . . . 136
8.6.3	TFTP Backup Configuration . . . . . 137
8.6.4	TFTP Import Text Configuration File. . . . . 138
8.6.5	TFTP Export Text Configuration File . . . . . 139
8.7	Logout . . . . . 140
9.	Menu-Driven Interface via Telnet . . . . . 141
10.	Troubleshooting . . . . . 142
10.1	Symptoms/Causes/Solutions. . . . . 142
10.2	Calling Black Box . . . . . 143
10.3	Shipping and Packaging. . . . . 143

# 1. Specifications

**Standards:** IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX, IEEE 802.3x full duplex on 10BASE-T and 100BASE-TX ports, IEEE 802.3z 1000BASE-SX, IEEE 802.1d spanning tree protocol, IEEE 802.1p priority queues, IEEE 802.1q VLAN tagging, RFC 1350 TFTP

**Data Transfer Rate:** Ethernet: 10 Mbps (half-duplex), 20 Mbps (full duplex);  
Fast Ethernet: 100 Mbps (half-duplex), 200 Mbps (full duplex);  
Gigabit Ethernet: 2000 Mbps (full duplex)

**Filtering Address Table:** 14K entries per device

**Packet Filtering/Forwarding Rate:** 10-Mbps Ethernet: 14,880 pps;  
100-Mbps Fast Ethernet: 148,800 pps;  
1000-Mbps Gigabit Ethernet: 1,488,000 pps

**MAC Address Learning:** Automatic update

**RAM Buffer:** 3 Mb

**Network Management:** System Configuration: Console port, Telnet™;  
Spanning Tree Algorithm: IEEE 802.1d provides redundant link support;  
Port-based, Protocol-based, or 802.1q VLANs: Up to 256 VLANs with GVRP for dynamic VLAN registration;  
Link Aggregation: Up to 4 ports can be combined into a fat pipe, 7 trunks

**Maximum Distance:** UTP: 328 ft. (100 m) over Category 5e or better cable;  
Fiber: LGB2004C-MMSX: 721.6 ft. (219.9 m) (62.5/125-micron multimode fiber via SC connectors);  
LGB2004C-SMLX: 6.2 mi. (10 km) (9/125-micron single-mode fiber cabling via SC connectors)

**Connectors:** LGB2004A: (24) 10/100 Ethernet ports, (1) card slot (for 1-port multimode fiber [LGB2004C-MMSX] or single-mode fiber [LGB2004C-SMLX] Gigabit module), (1) DB9 console port (DCE);  
LGB2004C-MMSX: (2) SC multimode ports;  
LGB2004C-SMLX: (2) SC single-mode ports

**Indicators:** LGB2004A: (52) LEDs: (1) Power, (1) Diag, (1) Fan 1, (1) Fan 2, (24) Twisted-Pair Link Activity, (24) 100 Mbps

**Temperature Tolerance:** Operating: 41 to 104°F (5 to 40°C);  
Storage: -4 to +158°F (-20 to +70°C)

**Humidity Tolerance:** Operating: 10 to 90%, noncondensing;  
Storage: 5 to 90%, noncondensing

**Power:** Input: 100 to 240 VAC (auto-ranging), 50 to 60 Hz;  
Output: 3.3 VDC, 20 amps and 5 VDC, 35 watts;  
(2) power supplies ([1] primary, [1] redundant)

**Size:** LGB2004A: 1.7"H (1U) x 17.3"W x 11.2"D (4.3 x 43.9 x 28.4 cm)

**Weight:** LGB2004A: 5.1 lb. (2.3 kg), fully loaded

## 2. Overview

### 2.1 Introduction

The Managed 24-Port 10/100 Switch with Gigabit Uplink Port incorporates leading switching technology and high-port density within a slim one-rack-unit (1U) chassis that fits in a standard 19" rack. It integrates 100-Mbps Fast Ethernet and 10-Mbps Ethernet network capabilities in a highly flexible package.

24 10/100 ports connect to each Ethernet device via up to 328 feet (100 m) of either 10BASE-T 2-pair UTP Category 3, 4, or 5 cable or 100BASE-TX 2-pair UTP Category 5 cable. These ports automatically detect whether the connected device is running at 10 or 100 Mbps.

An optional one-port Gigabit fiberoptic module (LGB2004C-MMSX or LGB2004C-SMLX) fits in the switch's front panel for length extension up to 721.6 feet (219.9 m) over multimode fiber or up to 6.2 miles (10 km) over single-mode fiber.

The switch works in half-duplex or full duplex transfer mode for 10- and 100-Mbps connection speeds. Furthermore, it receives and transmits data at wire speed.

A store-and-forward switching scheme enables the switch to support rate adaptation. This also ensures data integrity.

Up to 14K unicast address entities are supported per device. Plus, the switch features self-learning, table aging, and has a 3-Mb RAM buffer. It supports 802.3x flow control for the full duplex mode ports. Other functions include port-based VLAN, port-based QoS (Quality of Service), trunking, port mirroring, port setting for speed/disable, and flow control.

Configuration is easy via a Web browser or console port interface.

### 2.2 What's Included

Your package should contain the following items. If anything is missing or damaged, please contact Black Box at 724-746-5500.

LGB2004A:

- (1) 24-Port 10/100 Managed Switch with Gigabit Uplink Port
- (1) AC power cord

- (2) rackmount brackets
- (8) screws
- (1) CD-ROM containing this installation manual and a quick start guide

LGB2004C-MMSX or LGB2004C-SMLX:

- (1) Multimode SX Gigabit Uplink Module or
- (1) Single-Mode LX Gigabit Uplink Module

## 2.3 Typical Applications

Three application examples appear in Figures 2-1 through 2-3. They're described in the corresponding sub-sections (**Section 2.3.1** through **2.3.3**).

### 2.3.1 BUILDING-TO-BUILDING (SMALL CAMPUS)

Figure 2-1 shows the switch functioning as a backbone for a small campus network. It provides a 200-Mbps full duplex link to a remote stack of 10-/100-Mbps switches.

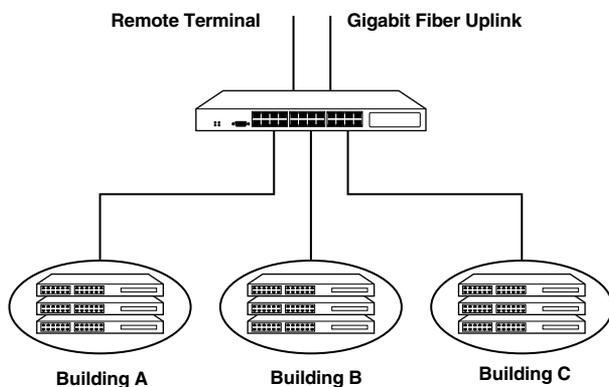
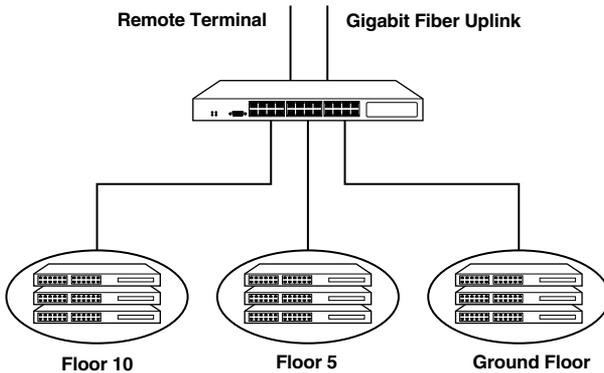


Figure 2-1. Interbuilding example.

## 2.3.2 ENTERPRISE SERVER AGGREGATION

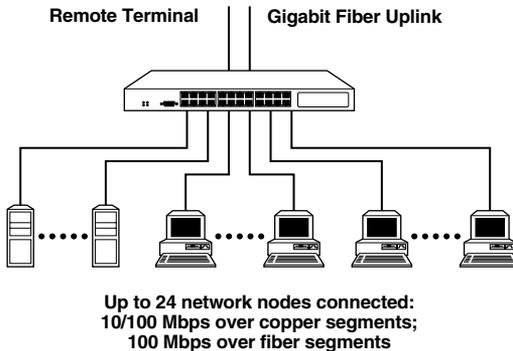
Figure 2-2 shows the switch functioning as a server aggregation for an enterprise or LAN configuration. It provides a 200-Mbps full duplex link to workgroups of 10/100 switches located on separate floors within a single building.



**Figure 2-2. Intrabuilding example.**

## 2.3.3 LAN SWITCH

Figure 2-3 shows the switch functioning as a high-speed bridge between segments, creating increased capacity for each user (node) on the local area network. It provides a 200-Mbps full duplex link to a variety of Ethernet/Fast Ethernet devices within a LAN.



**Figure 2-3. LAN switch example.**

## 3. About the Technology

### 3.1 Gigabit Ethernet

Gigabit Ethernet is an extension of IEEE 802.3 Ethernet using the same packet structure, format, and support for CSMA/CD protocol, full duplex, flow control, and management objects, but with a tenfold increase in theoretical throughput over 100-Mbps Fast Ethernet and a hundredfold increase over 10-Mbps Ethernet. Since it's compatible with all 10- and 100-Mbps Ethernet environments, Gigabit Ethernet provides a straightforward upgrade without wasting a company's existing investment in hardware, software, and trained personnel.

The increased speed and extra bandwidth offered by Gigabit Ethernet is essential for coping with the network bottlenecks that frequently develop as computers and their buses get faster and more users use applications that generate more traffic. Upgrading key components—such as your backbone and servers—to Gigabit Ethernet can greatly improve network response times as well as significantly speed up the traffic between your subnets.

Gigabit Ethernet enables fast optical fiber connections to support videoconferencing, complex imaging, and similar data-intensive applications. Likewise, since data transfers occur 10 times faster than Fast Ethernet, servers outfitted with Gigabit Ethernet NICs can perform 10 times the number of operations in the same amount of time.

In addition, the phenomenal bandwidth delivered by Gigabit Ethernet is the most cost-effective method to take advantage of today and tomorrow's rapidly improving switching and routing internetworking technologies. And with expected advances in the coming years in silicon technology and digital signal processing that will enable Gigabit Ethernet to eventually operate over UTP cabling, outfitting your network with a powerful 1000-Mbps-capable backbone/server connection creates a flexible foundation for the next generation of network technology products.

### 3.2 Fast Ethernet

LAN's growing importance and desktop computing applications' increasing complexity are fueling the need for high-performance networks. A number of high-speed LAN technologies have been proposed to provide greater bandwidth and improve client/server response times. Among them, 100BASE-T (Fast Ethernet) provides a smooth evolution from the current 10BASE-T technology. Its non-disruptive nature, plus the dominating potential market base, virtually guarantees cost-effective and high-performance Fast Ethernet solutions.

100-Mbps Fast Ethernet is a standard specified by the IEEE 802.3 LAN committee. It is an extension of the 10-Mbps Ethernet standard with the ability to transmit and receive data at 100 Mbps while maintaining the CSMA/CD Ethernet protocol. Since 100-Mbps Fast Ethernet is compatible with all other 10-Mbps Ethernet environments, it provides a straightforward upgrade and takes advantage of the existing investment in hardware, software, and personnel training.

### 3.3 Switching

Another approach to pushing beyond Ethernet technology's limits is switching technology's development. A switch bridges Ethernet packets at the Ethernet protocol's MAC address level, transmitting among connected Ethernet or Fast Ethernet LAN segments.

Switching is a cost-effective way to increase the total network capacity available for users on a local area network. A switch increases capacity and decreases network loading by dividing a local area network into different segments that don't compete with each other for network transmission capacity.

The switch acts as a high-speed selective bridge between the individual segments. The switch, without interfering with any other segments, automatically forwards traffic that needs to go from one segment to another. By doing this, the total network capacity is multiplied while still maintaining the same network cabling and adapter cards.

Switching LAN technology is a marked improvement over the previous network bridges generation; they were characterized by higher latencies. Routers have also been used to segment local area networks, but a router's cost—and the setup and maintenance required—make routers relatively impractical. Today, switches are an ideal solution to most local area network congestion problems.

### 3.4 VLAN (Virtual Local Area Network)

A VLAN is a group of end stations that are not constrained by their physical location and can communicate as if they are part of a common broadcast domain (a LAN). The primary VLAN use is to reduce latency and the need for routers, using faster switching instead.

Other VLAN utility features include security, cost reduction, and port-based VLAN. Since data switches only to confidential users within a VLAN, security increases. Because VLANs create multiple broadcast domains, you don't need expensive routers. The switch supports a common VLAN implementation—port-based (or port-group).

# 4. Installation

Before you install the switch, refer to **Section 2.2** and make sure your package includes everything listed.

The site where you install the switch may greatly affect its performance. When installing, consider the following:

- Install the switch in a fairly cool and dry place. See **Chapter 1** for the acceptable temperature and humidity operating ranges.
- Install the switch in a site free from strong electromagnetic field generators (such as motors), vibration, dust, and direct exposure to sunlight.
- Leave at least 4" (10.2 cm) of space at the switch's front and rear for ventilation.
- Install the switch in an EIA standard-size equipment rack. For information on rack installation, see **Section 4.1**.

## 4.1 Rackmounting

The switch can be mounted in an EIA standard-size 19" rack that can be placed in a wiring closet with other equipment. Attach the mounting brackets at the switch's front panel (one on each side) and secure them with the eight provided screws.

Next, install the switch in the rack.

### NOTE

**The four screws used to connect the switch to the rack are *not* included; you must supply them.**

## 4.2 Install the Gigabit Uplink Module (Optional)

To connect to a Gigabit fiber link, slide the Gigabit Uplink Module (LGB2004C-MMSX or LGB2004C-SMLX) into the slot on the switch's front panel. See Figure 5-1 for the fiber module slot's location.

## 4.3 Connecting Network Cable

The switch supports 10-Mbps Ethernet or 100-Mbps Fast Ethernet that runs both in half- and full duplex mode.

## 24-PORT 10/100 MANAGED SWITCH WITH GIGABIT UPLINK PORT

These RJ-45 ports are auto-MDI. The switch can auto transform to MDI-II or MDI-X, so you can make an easy connection without worrying if you are using a standard or crossover RJ-45 cable.

If you installed an optional Gigabit uplink module (LGB2004C-MMSX or LGB2004C-SMLX) in the switch's Gigabit uplink module slot, you will need to connect the fiber cable for this link. Use 1310-nm multimode or single-mode fiberoptic cable.

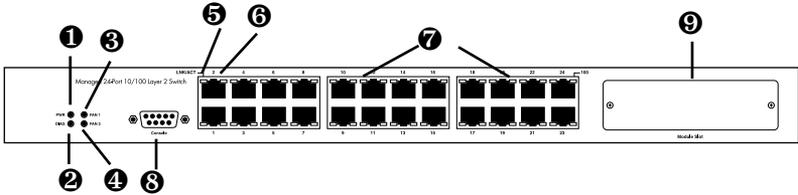
### 4.4 Applying AC Power

The 24-Port 10/100 Managed Switch with Uplink Port uses a 100–240-VAC, 50–60-Hz power supply. Its power switch is located on the unit's rear panel, next to the AC power connector. The power supply automatically adjusts to the local power source. Power on the unit without having LAN segment cables connected.

# 5. Operation

## 5.1 Front-Panel Components

The front panel is shown in Figure 5-1 below.



**Figure 5-1. Front panel.**

Comprehensive indicators display the switch's and the network's status. Table 5-1 describes the switch's front-panel indicators and connectors.

**Table 5-1. Front-panel indicators and connectors.**

Component	Function
① Power LED	This LED lights when the switch is receiving power.
	When the power is off or the power cord has improper connection, this LED is off.
② Diag LED	This LED flashes while the switch is performing self-system diagnostics upon startup. The LED lights solid to indicate normal operation.
③ Fan 1 LED	This LED lights when the fan is operating properly.
④ Fan 2 LED	This LED lights when the fan is operating properly.

## 24-PORT 10/100 MANAGED SWITCH WITH GIGABIT UPLINK PORT

Table 5-1 (continued). Front-panel indicators and connectors.

Component	Function
⑤ LNK/ACT LED (left side of port)	<p>When this LED is on, the switch's respective twisted-pair port is successfully connected to a network.</p> <p>When this LED is blinking, the port is transmitting or receiving data on the Ethernet network.</p> <p>When this LED is off, no link is connected.</p>
⑥ 10/100 Mbps LED (right side of port)	<p>When this LED is on, the switch's respective twisted-pair port is connected to a Fast Ethernet network.</p> <p>When this LED is off, the switch's respective port is connected to a 10-Mbps Ethernet port.</p>
⑦ 10-/100-Mbps Ethernet ports (1–24)	<p>The switch's 24 twisted-pair ports support autonegotiable 10/100 Mbps and auto-MDI/MDI-X crossover detection. Simply plug the network cable directly into the switch. It doesn't matter whether the end node is a NIC (network interface card), switch, or hub. These ports operate in half- or full duplex mode.</p>
⑧ Console port	<p>This DB9 connector is used for a terminal connection for remote management.</p>
⑨ Fiber module slot	<p>This slot holds an optional Gigabit Uplink Module (LGB2004C-MMSX or LGB2004C-SMLX) that connects to a fiber link.</p>

## 5.2 Rear-Panel Components

Figure 5-2 shows the switch's rear-panel button and connector. Table 5-2 describes these components.



Figure 5-2. Rear panel.

Table 5-2. Rear-panel button and connector.

Component	Function
Power button	Set the button to the On position to power on the switch. Set it to the Off position to power off the switch.
AC power connector	This three-pronged connector supports the power cord. Plug the provided power cord's female connector into this connector, and plug the cord's male connector into a power outlet. Supported input voltages range from 100–240 VAC at 50–60 Hz.

## 6. Web Management

### 6.1 Overview

The switch management agent can be accessed via a Web browser.

If you need to change the IP or other default address for the first time, we recommend that you go to **Section 8.2.5** and use console mode to secure a direct connection and to modify them.

Default Address:

MAC Address:	(Factory set and unique for each device)
IP Address:	192.168.0.254
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.0.1
User Name:	admin
Password:	(no default password)

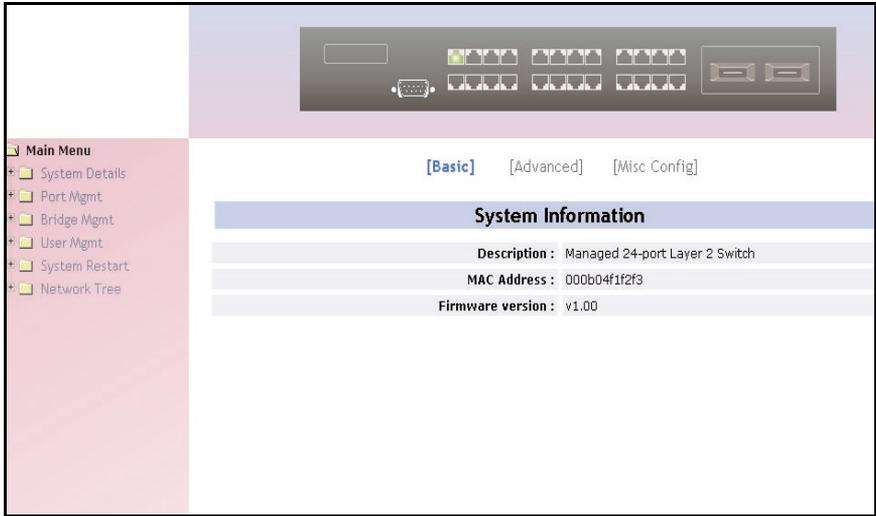
To access the switch, open a Web browser and type in the switch's IP address. Type in the user name and password (the default is no password), then check or uncheck the **Remember my password** box. See Figure 6-1. To cancel the login, click on the **Cancel** button. To complete the login, click on the **OK** button.



**Figure 6-1. Login screen.**

## 6.2 Home Page

Figure 6-2 shows the Home page. This screen appears when you click on **OK** in the Login screen (Figure 6-1). The Main Menu is located vertically on the left side of the screen. Three configuration options—Basic, Advanced, and Misc Config—are listed horizontally near the top of the screen. These options are described in Sections 6.2.1 through 6.2.3.



**Figure 6-2. The Home page.**

### 6.2.1 BASIC

When you click on **Basic** in the Home page, the parameters described in Table 6-1 and displayed in Figure 6-2 are shown.

**Table 6-1. Basic configuration parameters.**

Parameter	Description
Description	Display the device type name.
MAC Address	The unique hardware address assigned by the manufacturer (default).
Firmware Version	Display the switch's firmware version.

## 6.2.2 ADVANCED

When you click on **Advanced** in the Home page, the parameters listed in Figure 6-3 and described in Table 6-2 are displayed.



**Figure 6-3. Advanced configuration option selected.**

**Table 6-2. Advanced configuration parameters.**

Parameter	Description
MAC Table Address Entry	Check this box to enable or disable an address.
Age-Out Time	Type in the number of seconds that an inactive MAC address remains in the switch's address table. The valid range is 300–765 seconds. The default is 300 seconds.
Max. bridge transmit delay bound control	Limit the packets' queueing time in the switch. If enabled, the packets queued that exceed this time will be dropped. Select 1 sec, 2 sec, 4 sec, or off from the drop-down menu.

**Table 6-2 (continued). Advanced configuration parameters.**

<b>Parameter</b>	<b>Description</b>
Enable Low Queue Delay Bound	Check this box to limit the low-priority packets' queueing time in the switch. If the low-priority packets' stay in the switch exceeds the Max. Delay Time, the packet will be sent. The valid range is 1–255 ms.
Max. Delay Time	Type in a number between 1 and 255. This represents the number of milliseconds.
Broadcast Storm Filter Mode	To configure broadcast storm control, enable it and set the upper threshold for individual ports. The threshold is the percentage of the port's total bandwidth used by broadcast traffic. When broadcast traffic for a port rises above this threshold, broadcast storm control will be activated. The valid threshold values are 5%, 10%, 15%, 20%, 25%, and Off.
<b>Priority Queue Service</b>	
First Come First Service	The sequence of packets sent depends on the order they arrive. Click on this button to enable, or unclick to disable.
802.1p Priority	AHBL (All High Before Low): The high-priority packets are sent before low-priority packets. Click on this button to enable, or unclick to disable.

**Table 6-2 (continued). Advanced configuration parameters.**

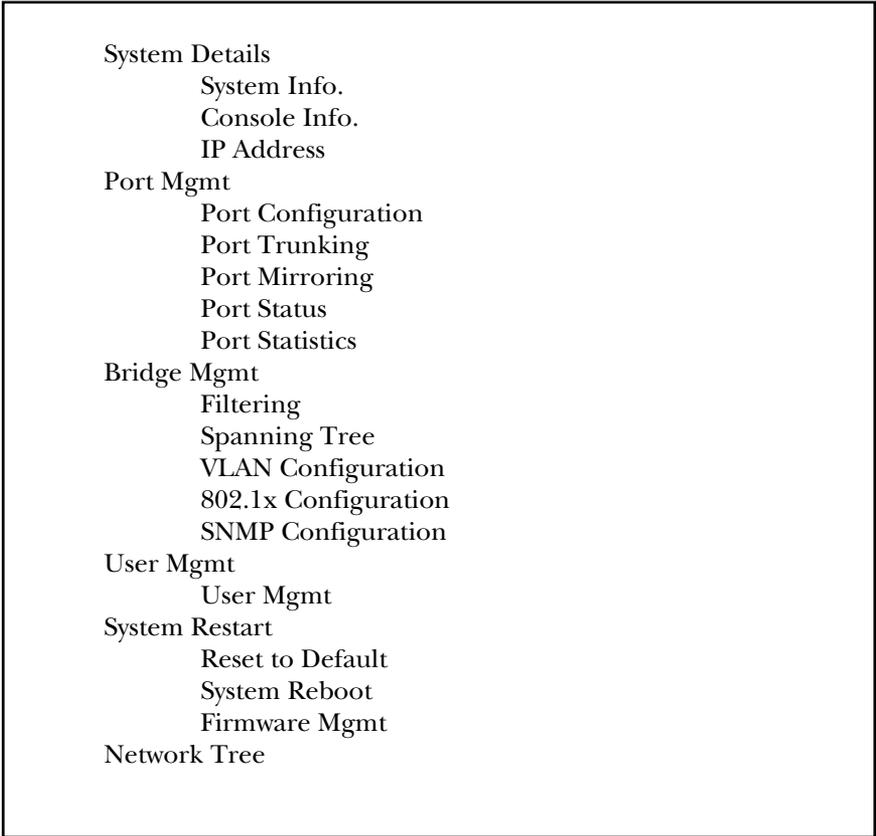
<b>Parameter</b>	<b>Description</b>
WRR (Weighted Round Robin)	Click on this button to enable, then type in the preferred ratio of high- and low-priority packets sent by the switch in its priority queue. These options represent the number of high-priority packets sent before one low-priority packet is sent. For example, 5 High: 2 Low means that the switch sends 5 high-priority packets before sending 2 low-priority packets.
QoS Policy: High Priority Levels	8 QoS levels (0 to 7) can be assigned to designated high or low priority. Check the appropriate boxes to enable, or uncheck to disable.
Apply button	Click on this button to apply the settings.
Default button	Click on this button to restore the default settings.
Help button	Click on this button for help.

### 6.2.3 Misc

Click on this button in the Home page to display a combination of Basic (**Section 6.2.1**) and Advanced (**Section 6.2.2**) configuration fields. (The resulting screen is not pictured in this manual.)

## 6.3 Main Menu

The Main Menu appears vertically on the left side of the Home page (Figure 6-2). Main Menu options are shown below (Figure 6-4) and are described in **Sections 6.4** through **6.9**.



- System Details
  - System Info.
  - Console Info.
  - IP Address
- Port Mgmt
  - Port Configuration
  - Port Trunking
  - Port Mirroring
  - Port Status
  - Port Statistics
- Bridge Mgmt
  - Filtering
  - Spanning Tree
  - VLAN Configuration
  - 802.1x Configuration
  - SNMP Configuration
- User Mgmt
  - User Mgmt
- System Restart
  - Reset to Default
  - System Reboot
  - Firmware Mgmt
- Network Tree

**Figure 6-4. Main Menu.**

## 6.4 System Details

The System Details menu is the first option on the Main Menu. It appears when you log in as described in **Section 6.1**. Options include System Info., Console Info., and IP Address.

### 6.4.1 SYSTEM INFORMATION

See **Sections 6.2.1** through **6.2.3**.

### 6.4.2 CONSOLE INFORMATION

Console provides a standard UART interface to communicate with the serial port. You can launch the HyperTerminal program to link with the switch. See **Chapter 8** for how to configure the switch using the console interface.

Console information settings are listed in Figure 6-5 and described in Table 6-3. To get to this screen, click on **Console Info.** in the System Details menu (see Figure 6-4).



**Figure 6-5. Console Information screen.**

**Table 6-3. Console Information screen parameters.**

Parameter	Description
Baud rate (bits/sec)	The baud rate is fixed at 38,400 bps.

**Table 6-3 (continued). Console Information screen parameters.**

<b>Parameter</b>	<b>Description</b>
Data Bits	The default is 8 data bits; this cannot be changed.
Parity Check	The parity check is fixed at None.
Stop Bits	The default is 1; this can't be changed.
Flow Control	The default is fixed at None.

**6.4.3 IP ADDRESS**

When you click on IP Address in the System Details menu, Figure 6-6 appears.

**IP Address Configuration**

DHCP :

IP Address :

Subnet\_Mask :

Gateway :

**Figure 6-6. IP Address Configuration screen.**

**Table 6-4. IP Address Configuration settings.**

<b>Parameter</b>	<b>Description</b>
DHCP	Use the drop-down menu to select Disable or Enable.
IP Address	Type in the IP address.
Subnet Mask	Type in the subnet mask.

Table 6-4. (continued) IP Address Configuration settings.

Parameter	Description
Gateway	Type in the gateway address.
Apply button	Click on this button to save the settings.
Help button	Click on this button for help.

## 6.5 Port Management

### 6.5.1 PORT CONFIGURATION

Use this page (Figure 6-7) to change the status of each port. To get to this page, click on **Port Configuration** in the Port Mgmt menu.

### Port Configuration

Port	State	Negotiation	Speed	Duplex	Flow Control		Rate Control (100K)		Priority	Security	Broadcast Filtering
					Full	Half	Ingress	Egress			
<div style="border: 1px solid #ccc; padding: 2px;">                     PORT1 ▲                      PORT2                      PORT3                      PORT4 ▼                 </div>	Enable ▼	Auto ▼	100 ▼	Full ▼	Enable ▼	Enable ▼	0	0	Disable ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="button" value="Apply"/>											

Port	State		Link		Negotiation		Speed		Duplex		Flow Control			Rate Control (100K)		Priority	Security	Broadcast Filtering
	Config	Actual	Config	Actual	Config	Actual	Config	Actual	Config	Actual	Config	Actual	Actual	Actual				
	Full	Half	Ingr	Egr														
2	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off	
3	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off	
4	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off	

Figure 6-7. Port Configuration screen.

Table 6-5 describes the parameters shown in Figure 6-7.

**Table 6-5. Port Configuration screen parameters.**

<b>Parameter</b>	<b>Description</b>
Port	Use the scroll-down menu to select the desired port. Options are 1–24 and M1–M2.
State	From the drop-down menu, disable or enable this port control.
Negotiation	From the drop-down menu, select the auto-negotiation mode, either Force or Auto. Force specifies the speed/duplex on this port with auto-negotiation enable. Auto automatically determines the highest speed and duplex mode possible.
Speed	Using the drop-down menu, set speeds of 100 Mbps or 10 Mbps on Ports 1–24, or a speed of 1000 Mbps on Ports 25–26.
Duplex	From the drop-down menu, select full or half-duplex mode for each port.
Flow Control	<p>Full: Selecting Enable sets full flow control function (pause). Selecting Disable cancels full flow control.</p> <p>Half: Selecting Enable sets half flow control (backpressure). Selecting Disable cancels half flow control.</p>
Rate Control	Ports 1–24 support by-port ingress and egress rate control. For example, assume port 1 is 10 Mbps. You can set the effective egress rate to 1 Mbps. The ingress rate is 500 kbps. The switch will perform flow control or backpressure to adapt the ingress rate to meet the specified rate.

**Table 6-5 (continued). Port Configuration screen parameters.**

<b>Parameter</b>	<b>Description</b>
Rate Control (continued)	<p>Ingress: Type in the port's effective ingress rate. The valid range is 0–1000.</p> <p>Egress: Type in the port's effective egress rate. The valid range is 0–1000.</p> <p>0: Disable rate control.</p> <p>1–1000: Valid rate value.</p>
Priority	<p>If you set the port to high priority, the priority of incoming frames to this port will always be high. Enable or disable it from the drop-down menu.</p>
Security	<p>A port in security mode will be locked without permission of address learning. Only the incoming packets with SMAC already existing in the address table can be forwarded. You can disable the port from learning any new MAC addresses, and then use the static MAC addresses screen to define a list of MAC addresses that can use the secure port. Enter the settings, then click on <b>Apply</b> to set the switch.</p>
Broadcast Filtering	<p>In a regular wired LAN network, there is a lot of broadcasting traffic. In order to filter the broadcast traffic, you can disable or enable this function for each port.</p>

### 6.5.2 PORT TRUNKING

The Link Aggregation Control Protocol (LACP) that's defined in IEEE 802.3ad allows ports with similar characteristics to form a channel through dynamic negotiation with adjoining switches. It provides a means for exchanging information on a link, allowing their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs. LACP allows you to move the link to an Aggregation Group and enable its transmission and reception functions in an orderly manner.

#### *Aggregator Setting*

Figure 6-8 shows the Port Trunking screen that appears when you click on Aggregator Setting at the top of the screen. To initially get to this screen, click on Port Trunking in the Port Mgmt menu (see Figure 6-4).

Link Aggregation lets you group up to four ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. LACP operation requires full duplex mode. More detailed information about LACP can be found in IEEE 802.3ad.

The screenshot shows the 'Port Trunking' configuration interface. At the top, there are three tabs: '[Aggregator Setting]' (active), '[Aggregator information]', and '[State Activity]'. The main content area is titled 'Port Trunking' and contains the following elements:

- System Priority:** A text input field.
- Group ID:** A dropdown menu currently set to 'Group1', with a '<< Get' button to its right.
- Lacp:** A dropdown menu currently set to 'Disable'.
- Work Ports:** A text input field containing the number '0'.
- Port Selection:** A list of ports from PORT1 to PORT9. To the left of the list are two buttons: '<< Add <<' and 'Remove >>'.
- Footer:** Three buttons: 'Apply', 'Delete', and 'Help'.

**Figure 6-8. Port Trunking screen.**

Table 6-6 describes the parameters shown in Figure 6-8.

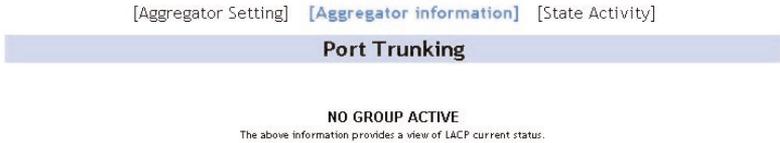
**Table 6-6. Port Trunking screen parameters.**

<b>Parameter</b>	<b>Description</b>
System Priority	Type in a value used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP.
Group ID	There are up to seven trunk groups that can be configured. Choose the Group ID from the drop-down menu and click on the <b>Get</b> button.
LACP	Enable or disable LACP from the drop-down menu. If enabled, the group is an LACP static trunking group. If disabled, the group is a local static trunking group. All ports support LACP dynamic trunking groups. If connecting to the device that also supports LACP, the LACP dynamic trunking group will be created automatically.
Work Ports	Type in the number of ports (1–4) that can be aggregated at the same time. In an LACP static trunking group, the excess ports are in standby mode and are able to aggregate if work ports fail. In a local static trunking group, the number must be the same as the group member ports.
Add and Remove buttons	Click on these buttons to select the ports to join the trunking group. Allow a maximum of four ports that can be aggregated at the same time.  If LACP is enabled, you can configure LACP Active/Passive status in each port on the State Activity page (see Figure 6-11).
Apply button	Click on this button to save your selections.
Delete button	Click on this button to delete the selections.
Help button	Click on this button for help.

### Aggregator Information

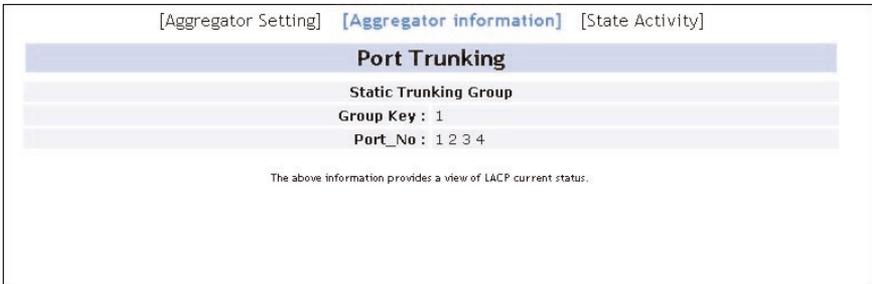
When setting the LACP aggregator, you can view related information as follows.

If no groups are active, this page (Figure 6-9) provides LACP current status. To get to this screen, click on **Aggregator Information** at the top of Figure 6-8. In this case, no group is active since LACP is not enabled.



**Figure 6-9. Port Trunking, Aggregator Information screen.**

If groups are active, this page (Figure 6-10) displays Static Trunking groups, identified by Group Key and Port Number. To get to this screen, click on **Aggregator Information** at the top of Figure 6-8.



**Figure 6-10. Static Trunking Group screen.**

## State Activity

The screen shown in Figure 6-11 shows the port trunking activity. To get to this screen, click on **State Activity** at the top of Figure 6-8.

[\[Aggregator Setting\]](#)   [\[Aggregator information\]](#)   **[\[State Activity\]](#)**

Port Trunking							
Port	LACP State Activity	Port	LACP State Activity	Port	LACP State Activity	Port	LACP State Activity
1	<input checked="" type="checkbox"/> Active	2	<input checked="" type="checkbox"/> Active	3	<input checked="" type="checkbox"/> Active	4	<input checked="" type="checkbox"/> Active
5	N/A	6	N/A	7	N/A	8	N/A
9	N/A	10	N/A	11	N/A	12	N/A
13	N/A	14	N/A	15	N/A	16	N/A
17	N/A	18	N/A	19	N/A	20	N/A
21	N/A	22	N/A	23	N/A	24	N/A
MOD_1	N/A	MOD_2	N/A				

**Figure 6-11. Port Trunking, State Activity screen.**

Table 6-7 describes the options shown in Figure 6-11.

**Table 6-7. State Activity parameters.**

Parameter	Description
Port	Identifies a port numbered 1–24 or MOD_1–MOD_2.
LACP State Activity	<p>A link that has either two active LACP ports or one active port can perform dynamic LACP trunking. A link that has two passive LACP ports will not perform LACP trunking because both ports are waiting for LACP packets from another networking device.</p> <p>When you select the trunking port for an active LACP, the active status will be created automatically.</p>

Table 6-7 (continued). State Activity parameters.

Parameter	Description
LACP State Activity (continued)	When the Active box is checked, the port automatically sends LACP packets.  When the Active box isn't checked, the port does not automatically send LACP packets, and it responds only if it receives LACP packets from another networking device.
Apply button	Click on this button to save the selections.
Help button	Click on this button for help.

### 6.5.3 PORT MIRRORING

Port Mirroring is a method used to monitor traffic in switched networks. Traffic through ports can be monitored by one specific port. That is, traffic going in or out monitored ports will be duplicated to a mirror port. Figure 6-12 shows this screen. To get to this screen, click on **Port Mirroring** in the Port Mgmt menu (see Figure 6-4).

Port Mirroring							
Roving Analysis State:		DISABLE					
Analysis Port:		None					
Port	Monitor	Port	Monitor	Port	Monitor	Port	Monitor
PORT1	<input type="checkbox"/>	PORT2	<input type="checkbox"/>	PORT3	<input type="checkbox"/>	PORT4	<input type="checkbox"/>
PORT5	<input type="checkbox"/>	PORT6	<input type="checkbox"/>	PORT7	<input type="checkbox"/>	PORT8	<input type="checkbox"/>
PORT9	<input type="checkbox"/>	PORT10	<input type="checkbox"/>	PORT11	<input type="checkbox"/>	PORT12	<input type="checkbox"/>
PORT13	<input type="checkbox"/>	PORT14	<input type="checkbox"/>	PORT15	<input type="checkbox"/>	PORT16	<input type="checkbox"/>
PORT17	<input type="checkbox"/>	PORT18	<input type="checkbox"/>	PORT19	<input type="checkbox"/>	PORT20	<input type="checkbox"/>
PORT21	<input type="checkbox"/>	PORT22	<input type="checkbox"/>	PORT23	<input type="checkbox"/>	PORT24	<input type="checkbox"/>

Apply Default Help

Figure 6-12. Port Mirroring screen.

Table 6-8 describes the options shown in Figure 6-12.

**Table 6-8. Port Mirroring screen parameters.**

<b>Parameter</b>	<b>Description</b>
Roving Analysis State	<p>Roving analysis is the mirroring of Fast Ethernet port traffic to another port of the same media type within a system that has an RMON probe or analyzer attached. This port allows external RMON probes (network analyzers) to monitor traffic on any switched segment.</p> <p>You can monitor a designated roving analysis port to: analyze traffic loads on each segment so that you can continually optimize your network loads by moving network segments, or troubleshoot switched network problems (for example, to find out why a particular segment has so much traffic).</p> <p>From the drop-down menu, select Enable to enable roving analysis state, or Disable to disable it.</p>
Analysis Port	<p>You can have as many as 16 network analyzers connected to a system. For more accurate analysis, attach the analyzer to a dedicated port instead of through a repeater. When the analyzer port is set, it cannot receive or transmit any other data. Instead, it receives only the data from the ports to be monitored.</p> <p>Select a port number between 1–24 or None from the drop-down menu.</p>

**Table 6-8 (continued). Port Mirroring screen parameters.**

<b>Parameter</b>	<b>Description</b>
Port	The ports that can be monitored. All monitor port traffic will be copied to a mirror port. You can select a maximum of 24 monitor ports in the switch. Choose which port to monitor in only one mirror mode.
Monitor	For each port you want to monitor, click on the check box next to that port.
Apply button	Click on this button to save your selections.
Default button	Click on this button to return to the default settings.
Help button	Click on this button for help.

# 24-PORT 10/100 MANAGED SWITCH WITH GIGABIT UPLINK PORT

## 6.5.4 PORT STATUS

This page (Figure 6-13) displays every port status that depends on a user setting and the negotiation result. To get to this screen, click on **Port Status** in the Port Mgmt menu (see Figure 6-4).

Port Status																	
Port	State		Link	Negotiation		Speed		Duplex		Flow Control			Rate Control (100K)		Priority	Security	Broadcast Filtering
	Config	Actual		Config	Actual	Config	Actual	Config	Actual	Config	Full	Half	Actual	Ingr			
1	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
2	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
3	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
4	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
5	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
6	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
7	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
8	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
9	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
10	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
11	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
12	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
13	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
14	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
15	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
16	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
17	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
18	On	On	Up	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
19	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
20	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
21	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
22	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
23	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
24	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
MOD_1	On	On	Down	Auto	Auto	1000	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
MOD_2	On	On	Down	Force	Force	1000	100	Full	Full	On	---	On	Off	Off	Disable	Off	Off

Figure 6-13. Port Status screen.

Table 6-9 describes the parameters shown in Figure 6-13.

Table 6-9. Port Status screen parameters.

Parameter	Description
Port	Lists the port number 1–24, or MOD_1–MOD_2.
State	Display Config and Actual port status as On or Off.

**Table 6-9 (continued). Port Status screen parameters.**

<b>Parameter</b>	<b>Description</b>
Link	Down is No Link, and Up is Link.
Negotiation	Display the Config and Actual values for auto-negotiation mode: Auto, Force, or NWay.
Speed	Display the Config and Actual: 1000 Mbps, 100 Mbps, or 10 Mbps speed. Ports 1–24 are 10-/100-Mbps, Ports 25–26 are 10-/100-/1000-Mbps (depending on the modular card used).
Duplex	Display Config and Actual full duplex or half-duplex mode.
Flow Control	<p>Full: Display the flow control status as On or Off in full duplex mode.</p> <p>Half: Display the backpressure as On or Off in half-duplex mode.</p> <p>Actual: Display the actual flow control setting: On or Off.</p>
Rate Control	<p>Display the actual rate control setting.</p> <p>Ingr: Display the port effective ingress rate of the user setting.</p> <p>Egr: Display the port effective egress rate of the user setting.</p>
Priority	Display the port static priority status of High, Low, or Disabled.

Table 6-9 (continued). Port Status screen parameters.

Parameter	Description
Security	Display the port security as On or Off.
Broadcast Filtering	The broadcast filtering setting is either On or Off.

### 6.5.5 PORT STATISTICS

The Port Statistic screen provides a summary of the current switch’s status. See Figure 6-14. To get to this screen, click on **Port Statistics** in the Port Mgmt menu (see Figure 6-4).

Port Statistic										
Port	State	Link	TxGoodPkt	TxBadPkt	RxGoodPkt	RxBadPkt	TxAbort	Collision	DropPkt	
1	On	Down	0	0	0	0	0	0	0	0
2	On	Down	0	0	0	0	0	0	0	0
3	On	Down	0	0	0	0	0	0	0	0
4	On	Down	0	0	0	0	0	0	0	0
5	On	Down	0	0	0	0	0	0	0	0
6	On	Down	0	0	0	0	0	0	0	0
7	On	Down	0	0	0	0	0	0	0	0
8	On	Down	0	0	0	0	0	0	0	0
9	On	Down	0	0	0	0	0	0	0	0
10	On	Down	0	0	0	0	0	0	0	0
11	On	Down	0	0	0	0	0	0	0	0
12	On	Down	0	0	0	0	0	0	0	0
13	On	Down	0	0	0	0	0	0	0	0
14	On	Down	0	0	0	0	0	0	0	0
15	On	Down	0	0	0	0	0	0	0	0
16	On	Down	0	0	0	0	0	0	0	0
17	On	Down	0	0	0	0	0	0	0	0
18	On	Up	7210	0	16773	0	0	0	9244	0
19	On	Down	0	0	0	0	0	0	0	0
20	On	Down	0	0	0	0	0	0	0	0
21	On	Down	0	0	0	0	0	0	0	0

Figure 6-14. Port Statistic screen.

Table 6-10 describes the fields shown in Figure 6-14.

Table 6-10. Port Statistic screen parameters.

Parameter	Description
Port	Displays the port number (1–24).
State	Displays the port's state (On or Off).
Link	Displays the link's state (Up or Down).
TxGoodPkt	Lists the number of good packets transmitted.
TxBadPkt	Lists the number of bad packets transmitted.
RxGoodPkt	Lists the number of good packets received.
RxBadPkt	Lists the number of bad packets received.
TxAabort	Lists the number of data packets aborted.
Collision	Lists the number of collisions on the network.
DropPkt	Lists the number of packets dropped.
Reset button	Click on this button to reset the settings.

## 6.6 Bridge Management

### 6.6.1 FILTERING

#### *IGMP Snooping*

The switch supports IP multicast. You can enable IGMP on the Web management's switch setting advanced page (see Figure 6-15), then display the IGMP snooping information in this page. To get to this page, click on **Filtering** in the Bridge Mgmt menu (see Figure 6-4). You can view different multicast group, VID, and member ports here. IP multicast addresses range from 224.0.0.0 to 239.255.255.255.

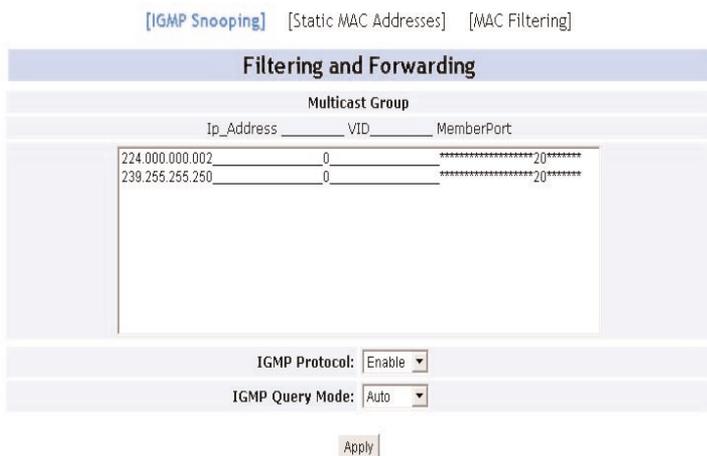
The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, routers, and hosts that support IGMP. Enabling IGMP allows the ports to detect IGMP

queries, report packets, and manage IP multicast traffic through the switch. IGMP has three fundamental types of messages: query, report, and leave group.

**Query:** A message sent from the querier (IGMP router or switch) asking for a response from each host belonging to the multicast group.

**Report:** A message sent by a host to this querier to indicate that the host wants to be or is a member of a given group indicated in the report message.

**Leave Group:** A message sent by a host to the querier to indicate that the host has quit to be a member of a specific multicast group.



**Figure 6-15. Filtering and Forwarding screen, IGMP Snooping.**

**Table 6-11. IGMP Snooping parameters.**

<b>Parameter</b>	<b>Description</b>
IGMP Protocol	Select Enable or Disable from the drop-down menu.
IGMP Query Mode	Select Auto, Enable, or Disable from the drop-down menu. Auto automatically determines if the IGMP query needs to be sent, Enable sends the IGMP query to members, and Disable sends no queries to members.
Apply	Click on this button to save your selections.

*Static MAC Address*

When you add a static MAC address, it is stored in the switch’s address table regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device’s MAC address when the device is disconnected or powered off and then activated on the network again. Figure 6-16 shows the Filtering and Forwarding screen with the Static MAC Addresses option selected. To get to this screen, select Filtering from the Bridge Mgmt menu (see Figure 6-4) and click on **Static MAC Addresses** at the top of the screen that appears in Figure 6-16.



Static addresses currently defined on the switch are listed below. Click Add to add a new static entry to the address table.

**Figure 6-16. Filtering and Forwarding screen, Static MAC Addresses.**

**Table 6-12. Static MAC Addresses screen parameters.**

Parameter	Description
MAC Address	In the MAC address box, type the MAC address to and from which the port should permanently forward traffic, regardless of the device’s network activity.
Port num.	In the drop-down menu, select a port number.

Table 6-12 (continued). Static MAC Addresses screen parameters.

Parameter	Description
VLAN ID	If tag-based (IEEE 802.1q) VLANs are set up on the switch, static addresses are associated with individual VLANs. Type the VID (tag-based VLAN) associated with the MAC address.
Add button	Click on this button to save the selections.
Delete button	Click on this button to delete the selections.
Help button	Click on this button for help.

### MAC Filtering

MAC address filtering allows a method to restrict unauthorized access by checking each MAC address before allowing it to connect to the network. This provides an additional layer of control in that only stations with registered MAC addresses can connect. This approach requires that the list of MAC addresses be configured. Traffic is filtered based on the destination address. To get to the screen shown in Figure 6-17, click on **Filtering** in the Bridge Mgmt menu (see Figure 6-4), then click on **MAC Filtering** at the top of the screen that appears.

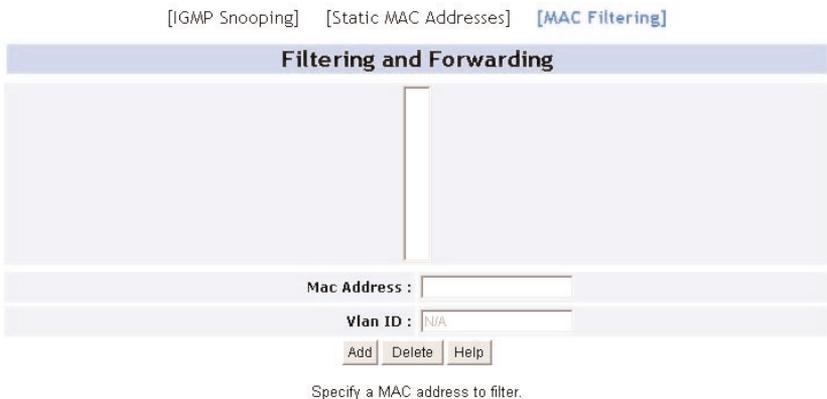


Figure 6-17. Filtering and Forwarding screen, MAC Filtering.

Table 6-13. MAC Filtering parameters.

Parameter	Description
MAC Address	In the MAC Address box, type in the MAC addresses that are to be filtered.
VLAN ID	If a tag-based (802.1q) VLAN is set up on the switch, type the VID associated with the MAC address in the VLAN ID box.
Add button	Click on this button to select a MAC address to filter.
Delete button	Choose the MAC address that you want to filter and then click on this button.
Help button	Click on this button for help.

### 6.6.2 SPANNING TREE

The Spanning Tree Protocol (STP) is a standardized method (IEEE 802.1d) for avoiding loops in switched networks. When STP is enabled, it ensures that only one path at a time is active between any two nodes in the network. We recommend that you enable STP on all switches to ensure that only a single active path in the network exists.

1. From the Spanning Tree Configuration menu (Figure 6-18), you can create a new value for the STP parameter and then click on the **Apply** button to set it. You can view spanning tree information for the root bridge from the same screen. To get to this screen, click on **Spanning Tree** in the Bridge Mgmt menu (see Figure 6-4), then click on System Configuration at the top of the screen that appears. The System Configuration parameters are described in Table 6-14.

[System Configuration] [PerPort Configuration]

**Spanning Tree Configuration**

Configure Spanning Tree Parameters

STP State

Priority (0-65535)

Max Age (6-40)

Hello Time (1-10)

Forward\_Delay\_Time(4-30)

---

**Spanning Tree Configuration**

Priority 32760

Mac Address 0050bf124ba0

Root\_Path\_Cost 10

Root Port PORT18

Max Age 10

Hello Time 2

Forward Delay 7

**Figure 6-18. Spanning Tree screen, System Configuration.**

**Table 6-14. System Configuration parameters.**

Parameter	Description
STP State	Check this box to enable, or uncheck it to disable, STP state.
Priority	Type in a number between 0 and 65535.
Max. Age	The Max. Age value is the number of seconds a bridge waits without receiving Spanning Tree Protocol configuration messages before attempting a reconfiguration. Type in a time in seconds from 6 to 40.
Hello Time	The Hello time value is the number of seconds between the transmissions of Spanning Tree Protocol configuration messages. Type in a time in seconds from 1 to 10.

**Table 6-14 (continued). System Configuration parameters.**

<b>Parameter</b>	<b>Description</b>
Forward Delay Time	The Forward Delay Time is the number of seconds a port waits before changing from its Spanning Tree Protocol learning and listening states to the forwarding status. Type in a time in seconds from 4 to 30.
Apply button	Click on this button to save the selections.

2. You can view a switch’s spanning tree status from the STP Port Status screen (Figure 6-19). This screen appears when you click on **Apply** in Figure 6-18.

<b>STP Port Status</b>			
<b>PortNum</b>	<b>PathCost</b>	<b>Priority</b>	<b>PortState</b>
PORT1	10	128	FORWARDING
PORT2	10	128	FORWARDING
PORT3	10	128	FORWARDING
PORT4	10	128	FORWARDING
PORT5	10	128	FORWARDING
PORT6	10	128	FORWARDING
PORT7	10	128	FORWARDING
PORT8	10	128	FORWARDING
PORT9	10	128	FORWARDING
PORT10	10	128	FORWARDING
PORT11	10	128	FORWARDING
PORT12	10	128	FORWARDING
PORT13	10	128	FORWARDING
PORT14	10	128	FORWARDING
PORT15	10	128	FORWARDING
PORT16	10	128	FORWARDING
PORT17	10	128	FORWARDING
PORT18	10	128	FORWARDING
PORT19	10	128	FORWARDING
PORT20	10	128	FORWARDING
PORT21	10	128	FORWARDING
PORT22	10	128	FORWARDING
PORT23	10	128	FORWARDING
PORT24	10	128	FORWARDING
MOD_1	4	128	FORWARDING
MOD_2	4	128	FORWARDING

**Figure 6-19. STP Port Status screen.**

Table 6-15. STP Port Status screen parameters.

Parameter	Description
PortNum	Displays the port number (1–24) or the module number (MOD_1–MOD_2).
PathCost	PathCost is used to determine which ports are the forwarding ports. The lowest numbers assigned are the forwarding ports, and the range is between 1 and 65535. Default PathCost values are: 50–600 for 10 Mbps, 10–60 for 100 Mbps, and 3–10 for 1000 Mbps.
Priority	The priority value is a value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root bridge. Enter any number from 1 to 65535.
PortState	When Spanning Tree is enabled and the port must choose between multiple paths to transmit the data to the destination, this setting blocks one port and allows data to be sent from a forwarding port.

- From the Spanning Tree Configuration menu (Figure 6-20), click on **PerPort Configuration** to configure STP parameters on each port, then click on the **Apply** button.

[\[System Configuration\]](#)    [\[PerPort Configuration\]](#)

**Spanning Tree Configuration**

Configure Spanning Tree Port Parameters

Port Number	Path Cost (1 - 65535; Default 10)	Priority (0 - 255; Default 128)
<div style="border: 1px solid #ccc; padding: 2px;">                     PORT1                      PORT2                      PORT3                      PORT4                      PORT5                 </div>	<input style="width: 50px;" type="text" value="10"/>	<input style="width: 50px;" type="text" value="128"/>

**STP Port Status**

PortNum	PathCost	Priority	PortState
PORT1	10	128	FORWARDING
PORT2	10	128	FORWARDING
PORT3	10	128	FORWARDING
PORT4	10	128	FORWARDING
PORT5	10	128	FORWARDING
PORT6	10	128	FORWARDING

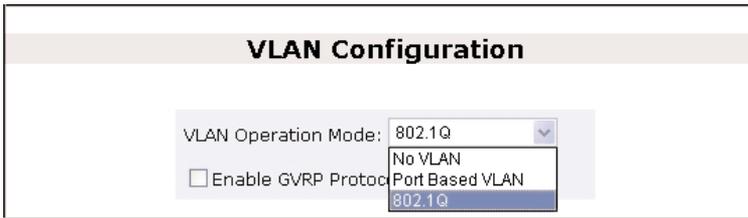
Figure 6-20. Spanning Tree Configuration, PerPort Configuration.

**Table 6-16. PerPort Configuration parameters.**

<b>Parameter</b>	<b>Description</b>
Port Number	Select PORT1–PORT24 from the drop-down menu.
Path Cost	Type in a number (1–65535) for the port's path cost. The switch then determines which ports are the forwarding ports. The default values based on IEEE 802.1d are: 10 Mbps: 50–600 100 Mbps: 10–60 1000 Mbps: 3–10
Priority	You can make the port more or less likely to become the root port. The range is between 0–255. Its default setting is 128. The lower the number, the higher the priority.
Port State	When Spanning Tree is enabled (STP State is checked in Figure 6-18) and the port has multiple choices of paths to transmit the data to the destination, this setting blocks one port and allows data to be sent from a forwarding port.
Apply button	Click on this button to save the settings.
Help button	Click on this button for help.

**6.6.3 VLAN CONFIGURATION**

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain. It allows you to isolate network traffic so that members of a VLAN receive traffic only from members of the same VLAN. Basically, creating a VLAN in a switch is logically equivalent to reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still physically plugged into the same switch. The switch supports no VLAN, port-based VLAN, or 802.1q (protocol-based) VLAN in the Web management page. In the default configuration, VLAN support is disabled. To get to the VLAN Configuration screen shown in Figure 6-21, click on **VLAN Configuration** in the Bridge Mgmt menu (see Figure 6-4).



**Figure 6-21. VLAN Configuration screen.**

**NOTE**

Each time you change the VLAN mode, you'll need to reboot the switch for the changes to take effect.

**Table 6-17. VLAN Configuration parameters.**

<b>Parameter</b>	<b>Description</b>
VLAN Operation Mode	From the drop-down menu, select No VLAN, Port Based VLAN, or 802.1Q.
Enable GVRP Protocol	Check this box to enable the protocol, or uncheck the box to disable it.

The VLAN Configuration screen has three options in the VLAN Operation Mode field: No VLAN, Port Based VLAN, and 802.1Q. It also has a checkbox for GVRP Protocol. No VLAN and Port Based VLAN are described next. If you want to use Protocol Based VLAN (IEEE 802.1v), you must enable the IEEE 802.1Q standard first by selecting it from the drop-down menu in Figure 6-21 *and* checking the **Enable GVRP Protocol** box in this screen. When you select IEEE 802.1Q, you have a choice of either Basic (Figure 6-23) or Port VID (Figure 6-24) screens.

**No VLAN**

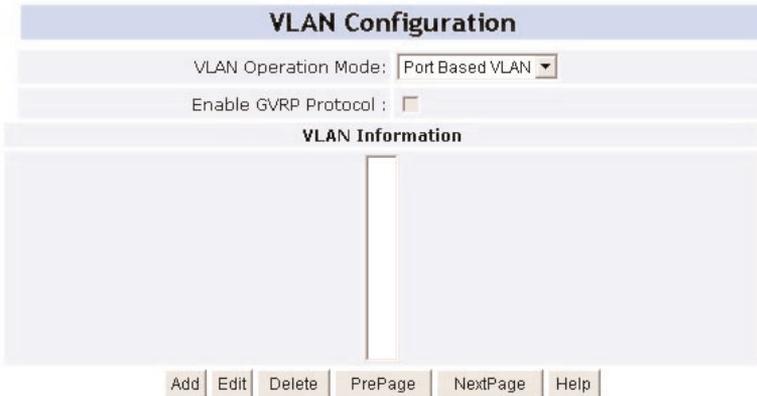
When you select No VLAN in Figure 6-21, no VLANs are active.

**Port Based VLAN**

When you select Port Based VLAN from the drop-down menu in Figure 6-21, Figure 6-22 appears. Packets can go only among members of the same VLAN group.

**NOTE**

**All unselected ports are treated as belonging to another single VLAN. If the port-based VLAN is enabled, the VLAN tagging is ignored.**



**Figure 6-22. Port Based VLAN screen.**

Table 6-18 described the port based VLAN parameters.

**Table 6-18. Port Based VLAN parameters.**

<b>Parameter</b>	<b>Description</b>
VLAN Operation Mode	Port Based VLAN is selected.
Enable GVRP Protocol	Check this box to enable the protocol, or uncheck the box to disable it.
VLAN Information	Type in the VLAN name, Group ID, and select the members for the new VLAN.
Add button	Click on this button to create a new VLAN group.
Edit button	Click on this button to edit the selections.
Delete button	Click on this button to delete the selections.
PrePage	Click on this button to go back to the previous page.
NextPage	Click on this button to go to the next page.
Help button	Click on this button for help.

**NOTE**

If trunk groups exist, they are displayed as: TRK1, TRK2, etc. Trunk groups can also be a member of a VLAN through use of the VLAN Configuration menu.

*IEEE 802.1Q Tag-Based VLAN (Protocol Based VLAN)*

Selecting 802.1Q from the drop-down menu in Figure 6-21 enables you to create a VLAN across devices from different switch vendors. IEEE 802.1q VLAN requires a standard methodology to insert and process the “tag” in the Ethernet frames. Tags contain a VLAN Identifier (VID) that indicates the VLAN numbers.

Use this page (Figure 6-23) to create tag-based VLANs, and to enable or disable GVRP protocol. To get to this page, select 802.1Q from the drop-down menu in Figure 6-21 and check the **Enable GVRP Protocol** box. There are 256 VLAN groups provided in the switch. When you enable 802.1q VLAN, all ports on the switch belong to a default VLAN. Its VID is 1. The Default\_\_1 VLAN cannot be deleted.

*Basic*

Figure 6-23 lists a Basic and a Port VID option near the top of the page. If you click on **Basic**, the screen appears as shown in Figure 6-23. If you click on **Port VID**, the screen appears as shown in Figure 6-24. Basic parameters are described in Table 6-19, and Port VID parameters are described in the text following Figure 6-24.

**Figure 6-23. VLAN Configuration, 802.1Q, Basic selected.**

**Table 6-19. 802.1Q VLAN parameters.**

<b>Parameter</b>	<b>Description</b>
VLAN Operation Mode	802.1Q is selected.
Enable GVRP Protocol	Check this box to enable GVRP Protocol. Uncheck the box to disable this protocol. GVRP (GARP [Generic Attribute Registration Protocol] VLAN Registration Protocol) allows automatic VLAN configuration between the switch and its nodes. If the switch is connected to a device with GVRP enabled, you can send a GVRP request using the VLAN ID (VID) of a VLAN defined on the switch. The switch will automatically add that device to the existing VLAN.
VLAN Information	DEFAULT_1 cannot be deleted. It's a VLAN with a VLAN ID of 1. Up to 256 different VLAN groups are possible.
Add button	Click on this button to create a new VLAN group.
Edit button	Click on this button to edit the selections.
Delete button	Click on this button to delete the selections.
PrePage button	Click on this button to go back to the previous page.
NextPage button	Click on this button to go to the next page.
Help button	Click on this button for help.

*Port VID*

Basic (described in the previous section) is the first option for a protocol based VLAN. The second option, Port VID, is described here.

Choose Port VID when you want to accommodate devices that will participate in the VLAN, but don't support tagging. The system can add VLAN tags to untagged frames that are based on PVID or on different protocols.

The switch will support protocol-based VLAN classification by means of both built-in knowledge of Layer 2 packet formats used by selected popular protocols, such as Novell® IPX™ and AppleTalk® EtherTalk®, and some degree of programmable protocol matching capability. A port can join more than one different protocol based VLAN, but a port can't apply the same protocol twice for the VLAN configuration purpose. Otherwise you will see the error message: "Save fail for ethertype conflict" when trying to configure VLANs.

1. From the Main Menu (Figure 6-4), click on **Bridge Mgmt**, then **VLAN Configuration**, and click on **Add**. You will see the page shown in Figure 6-24, with Port VID highlighted.

The screenshot shows the 'VLAN Configuration' web interface. At the top, there is a header 'VLAN Configuration'. Below it, there are two input fields: 'VLAN Operation Mode:' with a dropdown menu set to '802.1Q', and 'Enable GVRP Protocol:' with an unchecked checkbox. Below these are two tabs: '[Basic]' and '[Port VID]', with the latter being highlighted. The main configuration area contains:
 

- 'VLAN Name:' with an empty text input field.
- 'VID:' with a text input field containing the number '1'.
- 'Protocol Vlan:' with a dropdown menu set to 'NONE'.
- A list of ports from PORT1 to PORT12 on the left, with a scroll bar.
- An 'Add >>' button in the center.
- A '<< Remove' button in the center.
- A vertical text input field on the right side.

 At the bottom of the form are two buttons: 'Next' and 'Help'.

**Figure 6-24. The main tag-based VLAN page, Port VID selected.**

2. Type a name for the new VLAN in the VLAN Name area.

3. Type a VID number (between 1 and 4094). The default is 1 (in total, 255 VLANs that can be configured).
4. Choose the protocol type from the drop-down menu. If you are not applying protocol VLAN, you must set the value to NONE.

### NOTE

**You can't set a port to join more than one VLAN/VID with the same protocol.**

5. For each port you wish to add to the VLAN, select the port name (PORT1–PORT24) from the scroll-down box in Figure 6-24 and click on **Add**. If the trunk groups exist, you can see them displayed as TRK1, TRK2, etc. Later, you'll have the option of configuring it to be a member of the VLAN.
6. Click on **Next**. Figure 6-25 will appear. Or, click on **Remove** to remove the highlighted port from the list or click on **Help** for help.

The screenshot shows the 'VLAN Configuration' window. At the top, 'VLAN Operation Mode' is set to '802.1Q'. Below it, 'Enable GVRP Protocol' is unchecked. The 'VLAN Name' is 'RD3' and the 'VLAN ID' is '2'. A section titled 'UnTag Member' contains four ports: PORT1, PORT2, PORT3, and PORT4. Each port has a dropdown menu currently set to 'Untag'. An 'Apply' button is located at the bottom center of the configuration area.

**Figure 6-25. Tag/Untag menu.**

7. After adding ports to the VLAN, use the above page to set the outgoing frames as VLAN-tagged frames. The default is Untag. Using the dropdown box, select **Tag** or **Untag** and click on **Apply**.

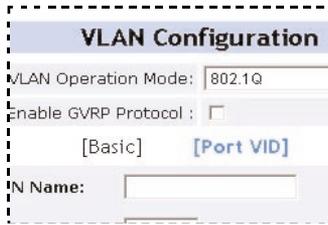
### NOTE

**Unless you are sure the network has no tag-unaware devices, you should leave the default setting of the outgoing frames to Untag.**

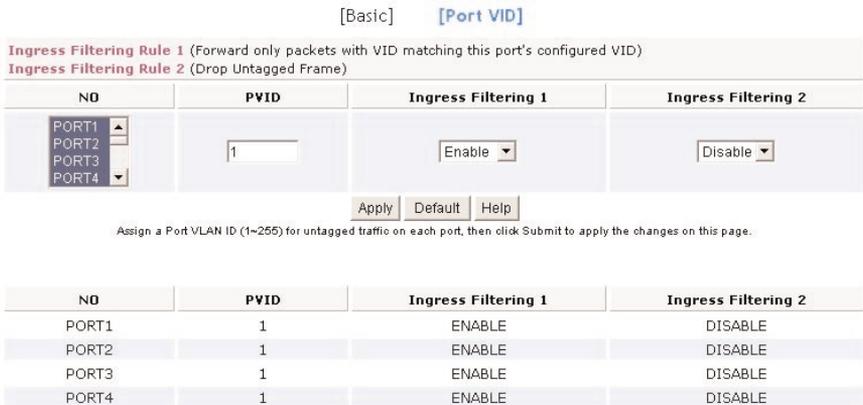
Tag: Outgoing frames with VLAN-tagging.

Untag: Outgoing frames without VLAN-tagging.

From the Main Tag-based VLAN page (Figure 6-24, also see the close-up screen in Figure 6-26), click [Port VID] to enter the Port VID Settings menu (Figure 6-27).



**Figure 6-26. VLAN Configuration screen.**



**Figure 6-27. Port VID screen.**

Figure 6-27 contains PVID and Ingress Filtering fields, which are described next.

**Port VID (PVID):** Set the port VLAN ID that will be assigned to untagged traffic on a given port. This feature is useful for accommodating devices that you want to participate in the VLAN but that don't support tagging. Each port allows you to set one PVID. The range is 1–4095, and the default PVID is 1.

Ports may share a same PVID, but all the PVIDs of the ports on the switch must belong to the same 256 number group segment. (For example: 1–255, 256–511, or any 256-number group segment up to 3840–4095). This allows for faster Ingress processing of frames. The PVID will be used for VLAN ID tagging to untagged frames.

## 24-PORT 10/100 MANAGED SWITCH WITH GIGABIT UPLINK PORT

The PVID must be the same as the member VLAN group IDs that the port belongs to or the untagged traffic will be dropped. This is because the port can't transmit a frame with a VLAN Group ID it doesn't belong to. If a port also joins a protocol VLAN, the switch will apply the protocol VLAN ID to untagged frames first. If the frame doesn't meet one of the protocols the port has defined, then the PVID will be applied for this frame.

Ingress filtering lets frames belonging to a specific VLAN be forwarded. The switch has two ingress filtering rules:

Rule 1: Forward only packets with VID matching this port's configured VID. The default is Enable. By default, only the packets with VID matching this port's configured VID can pass the port.

Rule 2: Drop Untagged Frame. The default is Disable. By default, untagged packets can pass the port.

### 6.6.4 802.1X CONFIGURATION

IEEE 802.1x is a standard for port-based network access control, part of the IEEE 802 (802.1) group of protocols. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. It is often used for wireless access points and is based on the Extensible Authentication Protocol (EAP).

If the protocol is not enabled, the screen shown in Figure 6-28 will appear.

802.1x NOT ENABLE. ( [Change Setting](#) )

**Figure 6-28. Protocol disabled.**

Click on **System Information** and then **Misc Config** to enable the function. See Figure 6-29.



**Figure 6-29. System Information screen.**

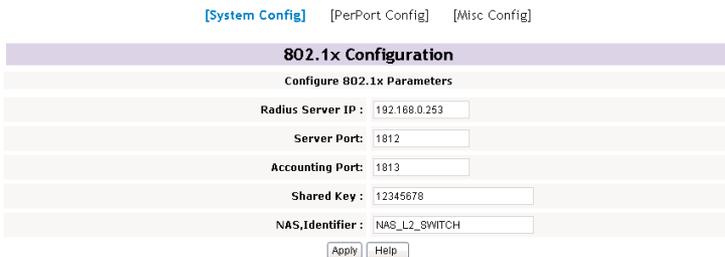
**Table 6-20. System Information parameters.**

<b>Parameter</b>	<b>Description</b>
Collision Retry Forever	Select Enable or Disable from the drop-down menu.
Hash Algorithm	Options include CRC-Hash and DirectMap. It's used to maintain the MAC address table. CRC-Hash (Cyclic Redundancy Checksum) maintains the MAC table by sorting out the entries. DirectMap doesn't sort the entries while maintaining the MAC address table.
IFG compensation	Select Enable or Disable from the drop-down menu.
802.1x Protocol	Select Enable or Disable from the 802.1x Protocol drop-down menu.
Apply button	Click on this button to apply the changes.
Default button	Click on this button to restore the default settings.
Help button	Click on this button for help.

**802.1x System Configuration**

The screen shown in Figure 6-30 appears when you enable 802.1x protocol in Figure 6-29.

In Figure 6-30, you can select System Config, Per Port Config, or Misc Config from the horizontal options menu at the top of the screen. These options are described next.



**Figure 6-30. 802.1x Configuration screen.**

**Table 6-21. 802.1x Configuration screen parameters.**

<b>Parameter</b>	<b>Description</b>
Radius Server IP	Type in the authentication server's IP address.
Server Port	Type in the UDP port number used by the authentication server to authenticate.
Accounting Port	Type the UDP port number used by the authentication server to retrieve accounting information.
Shared Key	Type in key shared between the switch and the authentication server.
NAS, Identifier	Type in a string used to identify the switch.
Apply button	Click on this button to implement the parameters.
Help button	Click on this button for help.

***802.1x Per Port Configuration***

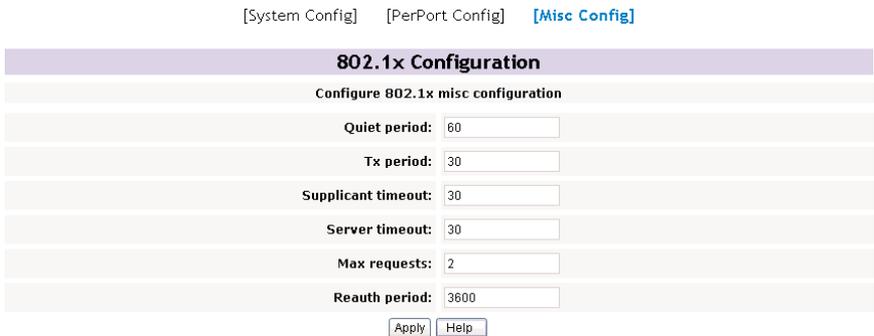
Use this window (not shown) to configure the 802.1x protocol on a per-port basis. Select the port first and then select the options. Click on **Apply** to complete the configurations. You can view the details in the lower part of the window screen while setting the parameters for each port. See Table 6-22.

**Table 6-22. 802.1x Per Port screen parameters.**

<b>Parameter</b>	<b>Description</b>
Fu	Force the specific port to be unauthorized.
Fa	Force the specific port to be authorized.
Au	The state of the specific port that was determined by the outcome of the authentication.
No	The specified port does not support IEEE 802.1x function.
Apply button	Click on this button to implement the parameters.

**802.1x Misc Configuration**

Use this window (Figure 6-31) to configure some of the 802.1x protocol default settings.



**Figure 6-31. 802.1x Misc Configuration screen.**

Table 6-23 describes the parameters shown in Figure 6-31.

**Table 6-23. Misc Configuration screen parameters.**

<b>Parameter</b>	<b>Description</b>
Quiet Period	Type in a period of time during which it will not attempt to acquire a supplicant (default time is 60 seconds).
Tx Period	Type in when an Tx packet is to be transmitted (default value is 30 seconds).
Supplicant Timeout	Type in a timeout value for the exchange between the supplicant and authentication server (default value is 30 seconds).
Server Timeout	Type in a timeout value for the exchange between the authenticator and authentication server (default value is 30 seconds).
Max. Requests	Type in the number of reauthentication attempts that are permitted before the specific port becomes unauthorized (default value is 2 times).
Reauth Period	Type in a nonzero number of seconds between periodic reauthentication of the supplications (default value is 3600 seconds).
Apply button	Click on this button to save the changes.
Help button	Click on this button for help.

**6.6.5 SNMP CONFIGURATION**

Any network management platform running the Simple Network Management Protocol (SNMP) can manage the switch, provided the Management Information Base (MIB) is installed correctly on the management station. The SNMP is a protocol that governs the transfer of information between management station and agent. Configure System Options, Community Strings, or Trap Manager.

1. System Options: Use this page (Figure 6-32) to define management stations as trap managers and to enter SNMP community strings. To get to this screen, click on the **SNMP Configuration** option in the Bridge Mgmt menu (see Figure 6-4). You can also define a name, location, and contact person for the switch. Fill in the system options data, and then click on **Apply** to update the changes on this page. Table 6-24 describes the parameters shown in Figure 6-32.

The screenshot shows a web interface titled "SNMP Configuration". Under the heading "System Options", there are three input fields: "Name :", "Location :", and "Contact :". Below these fields are two buttons: "Apply" and "Help".

**Figure 6-32. SNMP Configuration screen.**

**Table 6-24. SNMP Configuration screen parameters.**

<b>Parameter</b>	<b>Description</b>
Name	Type in a name to be used for the switch.
Location	Type in the switch’s location.
Contact	Type in the name of a person or organization.
Apply button	Click on this button to save the changes.
Help button	Click on this button for help.

2. Community strings serve as passwords and can be entered as one of the following:

**RO:** Read only. Enables requests accompanied by this string to display MIB-object information.

**RW:** Read write. Enables requests accompanied by this string to display MIB-object information and to set MIB objects.

To get to the screen shown in Figure 6-33, select **Community Strings** from the SNMP Configuration menu (not shown).

Community Strings	
Current Strings :	New Community String :
public__RO private__RW	String : <input type="text"/>
<< Add << Remove	<input checked="" type="radio"/> RO <input type="radio"/> RW

**Figure 6-33. Community strings.**

3. **Trap Manager:** The trap manager is a management station that receives traps, the system alerts generated by the switch. If no trap manager is defined, no traps are issued. Create a trap manager by entering the IP address of the station and a community string, then press **Add**. To get to the screen shown in Figure 6-34, select **Trap Managers** from the SNMP Configuration menu (not shown).

Trap Managers	
Current Managers :	New Manager :
(none)	IP Address : <input type="text"/>
<< Add << Remove	Community : <input type="text"/>

**Figure 6-34. Trap Managers.**

## 6.7 User Management

Using this page (Figure 6-35), you can change the Web management user name and password. To get to this page, click on **User Mgmt** in the User Mgmt menu (see Figure 6-4).

The screenshot shows a web interface titled "User Management". It contains three input fields: "User Name:" with the value "admin", "Assign/Change password:", and "Reconfirm pssword:". Below these fields is an "Apply" button.

Figure 6-35. User Management screen.

Table 6-25. User Management parameters.

Parameter	Description
User Name	Type in the new user name.
Assign/Change Password	Type in the new password.
Reconfirm Password	Retype the new password.
Apply button	Click on this button to save the changes.

## 6.8 System Restart

### 6.8.1 RESET TO DEFAULT

Use this function to restore all of the switch’s values/settings to default. To get to the screen shown in Figure 6-36, click on **Reset to Default** in the System Restart menu (see Figure 6-4).

The screenshot shows a web interface titled "Reset System to Default". Below the title is the text "Reset Switch to Default Configuration" and a "reset" button.

Figure 6-36. Reset to Default screen.

### 6.8.2 SYSTEM REBOOT

Reboot the switch with a software reset. To get to the screen shown in Figure 6-37, click on **System Reboot** in the System Restart menu. Then click on the **Reboot** button or the **Help** button.



**Figure 6-37. System Reboot screen.**

### 6.8.3 FIRMWARE MANAGEMENT

The following menu (Figure 6-38) provides some system control functions to allow you to update firmware and remote boot the switch system.



**Figure 6-38. Download New Firmware File screen.**

## NOTE

The address and file name in the above screen are examples.

Table 6-26. Firmware parameters.

Parameter	Description
TFTP Server IP Address	Type in the server's IP address.
Firmware File Name	Type in the file name.
Apply button	Click on this button to save the changes.
Help button	Click on this button for help.

Once you click on **Apply** in Figure 6-38, Figure 6-39 appears. Click on the **Update Firmware** button.



Figure 6-39. Update Firmware screen.

## 6.9 Network Tree

The Web cluster feature will search switch nodes connected to the local network, and it allows users to add/delete any network node(s) to/from the network tree. This way, users not only have a network view, but they also have access or control switches or nodes from the local switch's Web interface. See Figure 6-40.

The screenshot shows two sections of a web interface. The top section, titled "Network Configuration", has a "Network Function" checkbox labeled "Enable" which is currently unchecked. Below this is an "Apply" button. The bottom section, titled "Static Device Table", features a table with two columns: "Device Name" and "Ip Address". The "Ip Address" column contains the value "0.0.0.0". Below the table are input fields for "Device Name" and "Ip Address", and "Add" and "Delete" buttons.

**Figure 6-40. Network Configuration/Static Device Table screen.**

**Table 6-27. Network Configuration/Static Device parameters.**

Parameter	Description
Network Function	Check this box to enable the network function.
Apply button	Click on this button to apply the network function.
Device Name	Type in the device name.
IP Address	Type in the IP address.
Add button	Click on this button to save your settings.
Delete button	Click on this button to delete the settings.

## 7. Console 1K Xmodem Update Firmware

The switch provides a 1K Xmodem to update firmware via console. The application only works in 38,400 bps mode. These are the two instances in which the 1K Xmodem will be used:

- Enter 1K Xmodem receiver mode by pressing any key within 3 seconds after the system is powered on.
- The system will automatically enter 1K Xmodem receiver mode if it detects the firmware checksum failure while booting.

1. Start Xmodem receiver mode (via either option listed above). Figure 7-1 appears. Follow the screen cues by clicking any key.

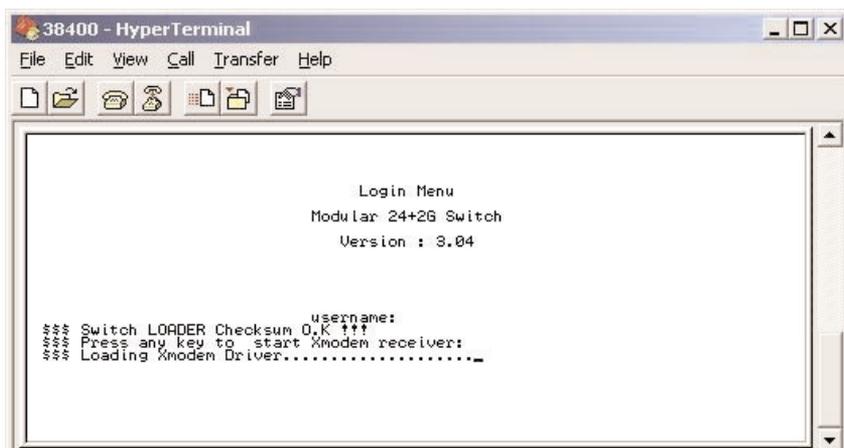
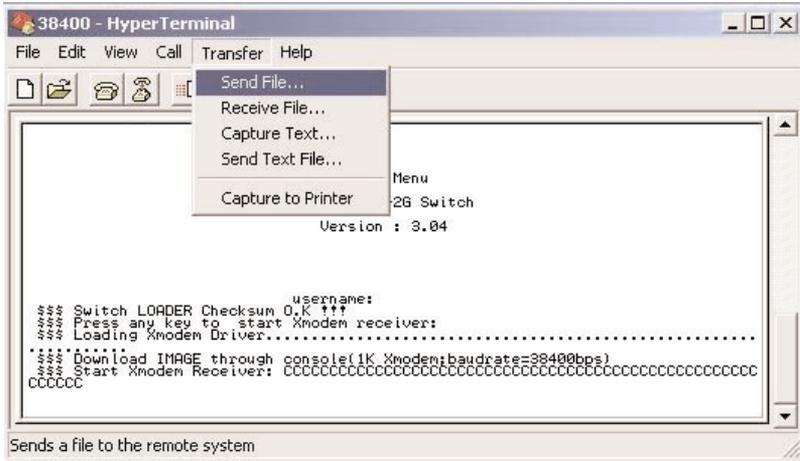


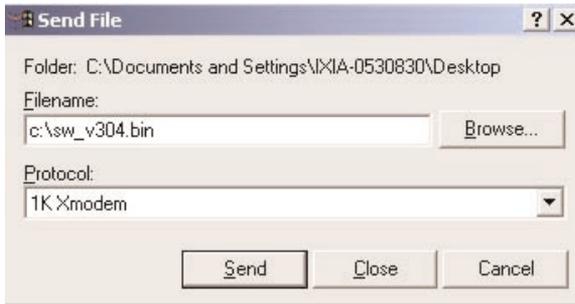
Figure 7-1. Login menu.

2. While waiting for the file to transfer, **CCCC...** will appear on the console. Select **Transfer**, then **Send File** from the drop-down menu. See Figure 7-2.



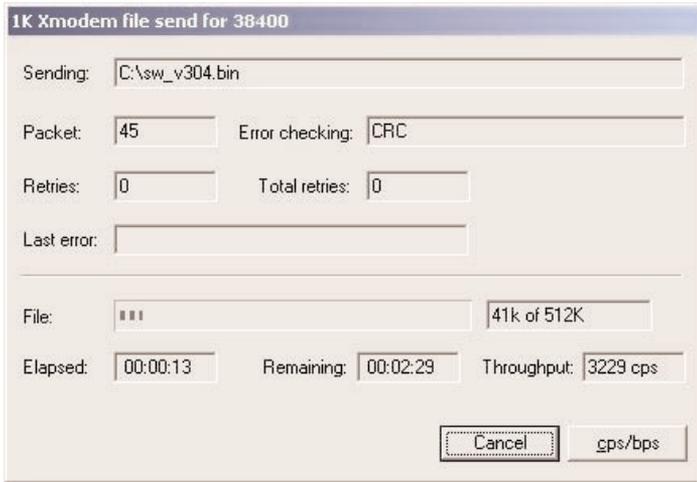
**Figure 7-2. Transfer menu, Send File selected.**

3. Once you select **Send File** in Figure 7-2, Figure 7-3 appears. Select 1K Xmodem in the Protocol area, and specify the path where the image file is to be sent. Then click on the **Send** button. Or, to browse through the available filenames, click on the **Browse** button. Click on **Close** to close the Send File window or **Cancel** to cancel the selections.



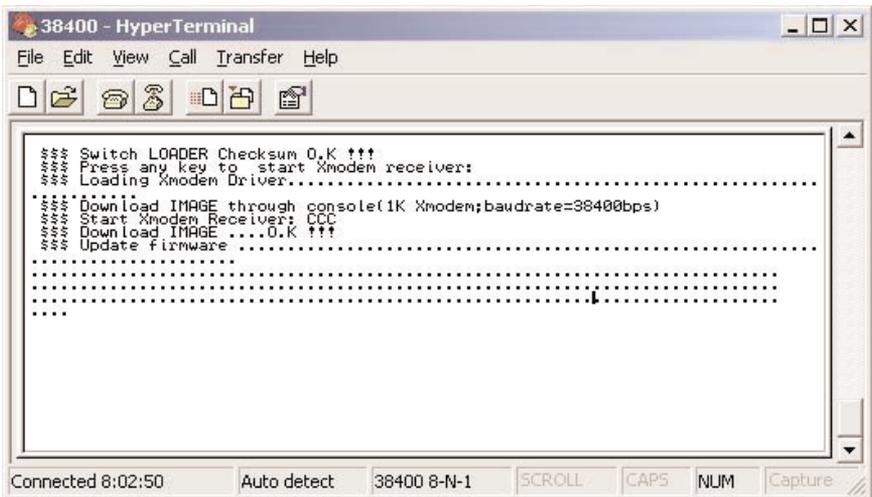
**Figure 7-3. Send File dialog box.**

4. Once you click on the **Send** button in Figure 7-3, Figure 7-4 appears and the image file begins to download.



**Figure 7-4. Download image file screen.**

5. When the image finishes downloading, Figure 7-5 appears. The switch system will update firmware automatically, and the switch will reboot.



**Figure 7-5. Switch download, update firmware messages.**

## 8. Console Menu Line

The Console Menu Line interface can be used by a computer or terminal to control the switch. The DB9 port (DCE) on the switch's front panel connects to the computer or terminal. The default configuration values for the attached terminal are 8 data bits, no parity, 1 stop bit, and no flow control.

1. To get to the Login menu, press **Enter** at the terminal emulation program's (such as HyperTerminal) prompt.
2. Type in your username and press **Enter**, then type in the password and press **Enter** to login. The default username is `admin`, with a null password (to enter a null password, just press **Enter** in the password field). See Figure 8-1.



**Figure 8-1. Login Menu.**

### CONTROL KEYS AND ACTION KEYS

The Console Menu Line program is a set of menus, beginning with the Main Menu and sub-menus. To choose a menu option, use the control keys (Tab, Backspace, Enter, and Space, described in Table 8-1) to navigate and select items provided in all menus.

Table 8-1. Control key functions.

Key	Use
Tab	Move the cursor to the next item.
Backspace	Move the cursor to the previous item.
Enter	Select the highlighted item.
Space	Toggle the selected item.

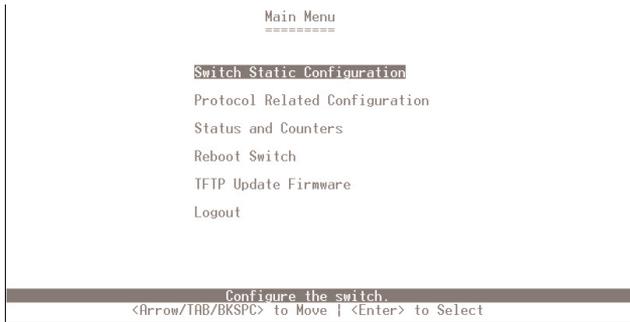
Once you press **Enter** to select an item, a screen appears. From here, you can configure the switch via various options. Use the action keys (Quit, Edit, Save, Previous Page, and Next Page, described in Table 8-2) to select a mode. For example, if you press the Tab or Backspace key to select the Edit mode and then press **Enter**, you can change the entries in the fields on the screen. To move between fields on the screen, use the control keys (Tab, Backspace, Enter, and Space). For example, use the Tab or Backspace keys to move between fields. Press the **Space** bar to toggle between values in a specific field. Press **Ctrl+A** to return to the action menu line, and use the Tab or Backspace keys to go to the **Save** option, and press **Enter** to select it.

Table 8-2. Action key functions.

Key	Use
Quit	Exit the current page and return to the previous menu.
Edit	Configure items. When finished with configurations, press <b>Ctrl+A</b> to return to the action menu line.
Save	Save all configured values.
Previous Page	Return to the previous page.
Next Page	Go to the next page.

## 8.1 Main Menu

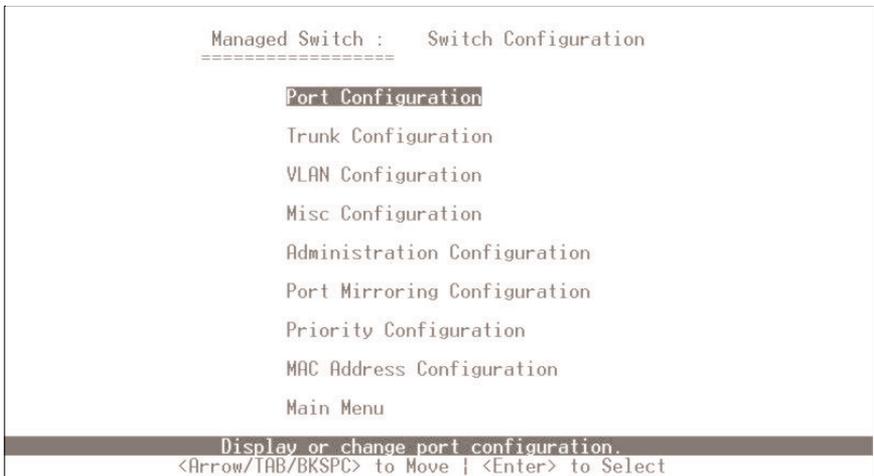
There are six items that you may select from the console's Main Menu page (see Figure 8-2). These options are described in **Sections 8.2** through **8.7**.



**Figure 8-2. Main Menu.**

## 8.2 Switch Static Configuration

The Switch Static Configuration menu enables you to configure the switch. When you use the Tab or Backspace keys to select **Switch Static Configuration** from the Main Menu (Figure 8-2) and press **Enter**, the screen shown in Figure 8-3 appears.



**Figure 8-3. Switch Static Configuration screen.**

## 8.2.1 PORT CONFIGURATION

When you use the Tab or Backspace keys to select **Port Configuration** from the Switch Static Configuration menu (Figure 8-3) and press **Enter**, Figure 8-4 appears. This page allows configuration of each port. Use the Tab or Backspace keys to select **Edit**, then press **Enter**. Use the Tab or Backspace keys to move the cursor between fields. Press the **Space** key to toggle the status of each item described in Table 8-4. Press **Ctrl+A** to return to the action menu line, then use the Tab or Backspace keys to select **Save**. Press **Enter** to save the configuration.

Managed Switch : Port Configuration									
=====									
Port	Type	InRate (100K)	OutRate (100K)	Enable	Auto	Spd/Dpx		FlowControl	
						Full	Half		
PORT1	100Tx	0	0	Yes	AUTO	100	Full	0n	0n
PORT2	100Tx	0	0	Yes	AUTO	100	Full	0n	0n
PORT3	100Tx	0	0	Yes	AUTO	100	Full	0n	0n
PORT4	100Tx	0	0	Yes	AUTO	100	Full	0n	0n
PORT5	100Tx	0	0	Yes	AUTO	100	Full	0n	0n
PORT6	100Tx	0	0	Yes	AUTO	100	Full	0n	0n
PORT7	100Tx	0	0	Yes	AUTO	100	Full	0n	0n
PORT8	100Tx	0	0	Yes	AUTO	100	Full	0n	0n

actions->	<b>&lt;Quit&gt;</b>	<Edit>	<Save>	<Previous Page>	<Next Page>
Select the Action menu.					
<Arrow/TAB/BKSPC> to Move   <Quit> to Previous menu   <Enter> to Select					

**Figure 8-4. Port Configuration screen.**

**Table 8-3. Port Configuration parameters.**

Parameter	Function
Port	The port number that is being configured. Options include PORT1–PORT26.
Type	The port type (choose 10BASE-T or 100BASE-TX).
InRate (100K)	The input rate control. The valid range is 0–1000. Type 0 to disable rate control, or 1–1000 to enable a specific rate.
OutRate (100 K)	The output rate control. The valid range is 0–1000. Type 0 to disable rate control, or 1–1000 to enable a specific rate.
Enable	Enable or disable each port. <b>Yes</b> means that the port is enabled. <b>No</b> means the port is disabled.
Auto	<p>Use the space bar to toggle the autonegotiation mode. (Auto or Force).</p> <p>Auto: Auto automatically determines the highest speed and duplex mode possible.</p> <p>Force: Force specifies the speed/duplex on this port with autonegotiation enable.</p>
Spd/Dpx	Toggle 100 Mbps or 10 Mbps speed on port 1–port 24. Set 1000 Mbps, 100 Mbps, or 10 Mbps speed on port 25–port 26 (depending on the performance of the uplink module card), and set full or half-duplex mode.
FlowControl	Toggle the Space bar to select <b>Full</b> to enable (On) or disable (Off) full flow control function (pause). Select <b>Half</b> to enable (On) or disable (Off) half flow control function (backpressure).

## 8.2.2 TRUNK CONFIGURATION

Use this page (Figure 8-5) to create a maximum of up to seven trunk groups (numbered 1–7 vertically in Figure 8-5). A trunk group is a group of ports that are configured together. To get to this page, use the Tab or Backspace keys to select **Trunk Configuration** from the Switch Static Configuration menu shown in Figure 8-3, then press **Enter**.

```

Managed Switch : Trunk Configuration
=====
 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 M1 M2
1 v  -  -  -  -  -  v  -  -  -  -  -  v  -  -  -  -  -  -  -  v  -  -  -  -  -
2 -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
3 -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
4 -  -  v  v  v  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
5 -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
6 -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
7 -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -

TRK1 Static
TRK2 Disable
TRK3 Disable
TRK4 LACP
TRK5 Disable
TRK6 Disable
TRK7 Disable

actions->      <Edit>      <Save>      <Quit>
Select the action menu.
<Arrow/TAB/BKSPC> to Move | <Quit> to Previous menu | <Enter> to Select

```

**Figure 8-5. Trunk Configuration screen.**

1. Use the Tab or Backspace keys to select **Edit** on the actions menu at the bottom of the screen, then press **Enter**.
2. The numbers running down the left-hand side of the page represent the trunk groups. To arbitrarily select up to four ports from port 1–port 24 or M1–M2 to build a trunking group, select the desired port numbers in the horizontal line next to the trunk group number. Use the **Space** key to toggle between v (for VLAN) and a space (for a port that is not a member of a trunk group).

Below that are the Static or LACP settings for the corresponding trunk groups (TRK1–TRK7). Toggle between **Static**, **LACP**, and **Disable**.

**Static** is the setting for a normal trunk.

**LACP** is trunking with Link Aggregation Control Protocol.

**Disable** deletes the trunk group.

3. Press **Ctrl+A**, to return to the actions menu line, then use the Tab or Backspace keys to select **Save** and press **Enter**.

### NOTE

1. All ports in the same static trunk group will be treated as a single port. So when you set VLAN members and port configuration, they will be toggled on or off simultaneously.
2. If a VLAN group exists, all of the members of the static trunk group must be in the same VLAN group.

### 8.2.3 VLAN CONFIGURATION

Use this page (Figure 8-6) to set port-based VLAN or Tagged (802.1q) VLAN or to deactivate the VLAN function. To get to the VLAN Configuration screen, use the Tab or Backspace keys to select **VLAN Configuration** from the Switch Static Configuration menu (Figure 8-3), then press **Enter**.

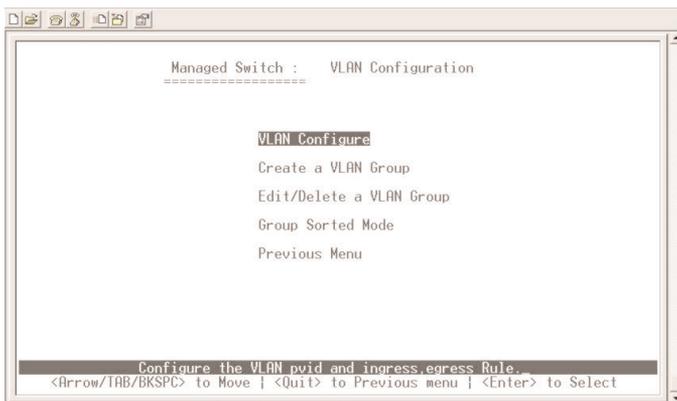


Figure 8-6. VLAN Configuration menu.

### NOTE

Each time you modify the VLANs, you must restart the switch for the new configurations to take effect.

The following sections describe the menu options listed in Figure 8-6.

#### *VLAN Configure*

Use the Tab or Backspace keys to select VLAN Configure in Figure 8-6, then follow the steps below to configure the VLAN.

1. Use the Tab or Backspace keys to **Edit**, then press **Enter**.
2. Use the **Space** bar to toggle between three types: **Disable**, **Port Based**, and **802.1q**. The VLAN Mode by default is disabled.
3. Toggle to Port Based configuration, as shown in Figure 8-7.

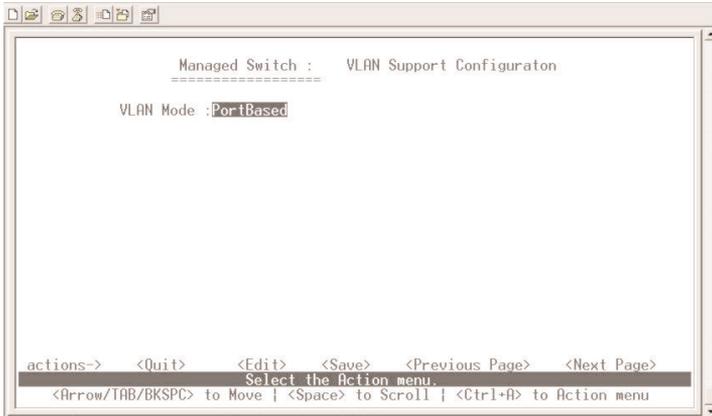


Figure 8-7. VLAN Mode, Port Based.

4. Or, select 802.1q VLAN to set PVID, Ingress Filtering 1, and Ingress Filtering 2 rules on the page shown in Figure 8-8. To get to this screen, use the **Space** bar to toggle to the 802.1q selection in the VLAN Mode field screen shown in Figure 8-7.

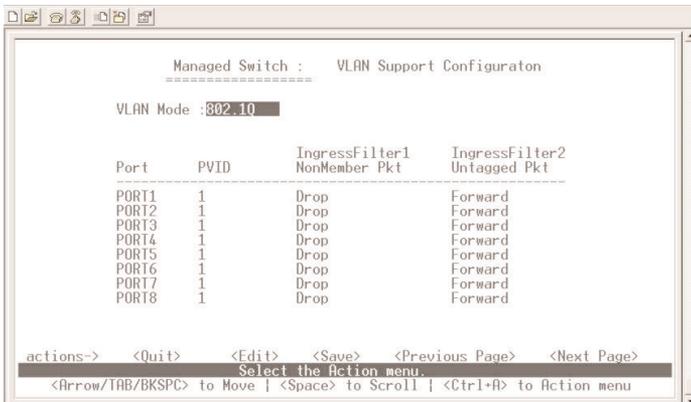


Figure 8-8. VLAN Mode, 802.1q.

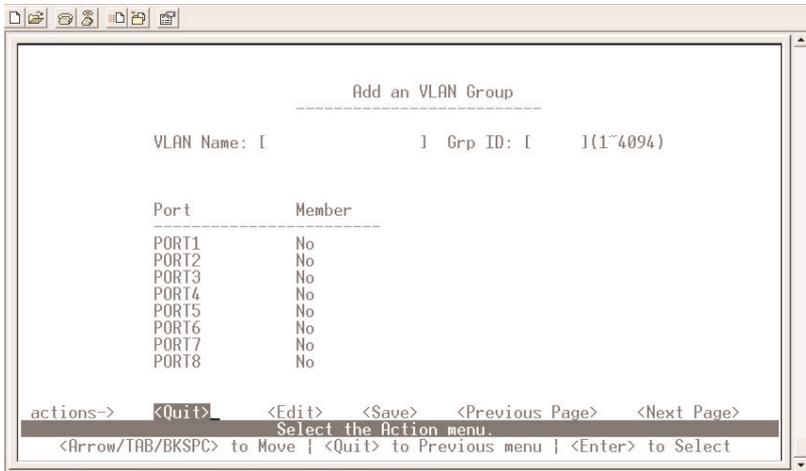
Four fields are shown in Figure 8-8: Port, PVID, NonMember Pkt, and Untagged Pkt.

1. Select a port number (PORT1–PORT26).
2. PVID (Port VID: 1–4095): Type in the PVID. Each port allows you to set one PVID. The range is 1–4095, and the default PVID is 1. Some ports can share the same PVID, but all the switch's port PVIDs must belong to the same 256 number segment (for example, 1–255, 256–511, or any 256 number group segment up to 3840–4095).
3. NonMember Pkt: This matches the Ingress Filtering Rule 1 on the Web. Either forward only packets with a VID that matches this port's configured VID, or drop the frame when the VID does not match this port's configured VID. Press the **Space** key to choose Drop or Forward. The default is Drop. It is the same as if the Filtering Rule 1 is enabled on the Web.
4. Untagged Pkt: This matches the Ingress Filtering Rule 2 on the Web. Either drop or forward an untagged frame. Press the **Space** key to choose Drop or Forward. The default is Forward. It is the same as if the Filtering Rule 2 is enabled on the Web.
5. Press **Ctrl+A**, then use the Tab or Backspace keys to select **Save** and press **Enter**.

## Create a VLAN Group

### Create a Port-Based VLAN

To create a port-based VLAN and to add member/nonmember ports to it, go to the screen shown in Figure 8-9. To get to this screen, use the Tab or Backspace keys to select **Create a VLAN Group** in Figure 8-6, then press **Enter**.



**Figure 8-9. Add a VLAN Group screen.**

Follow the steps listed next to add a VLAN group.

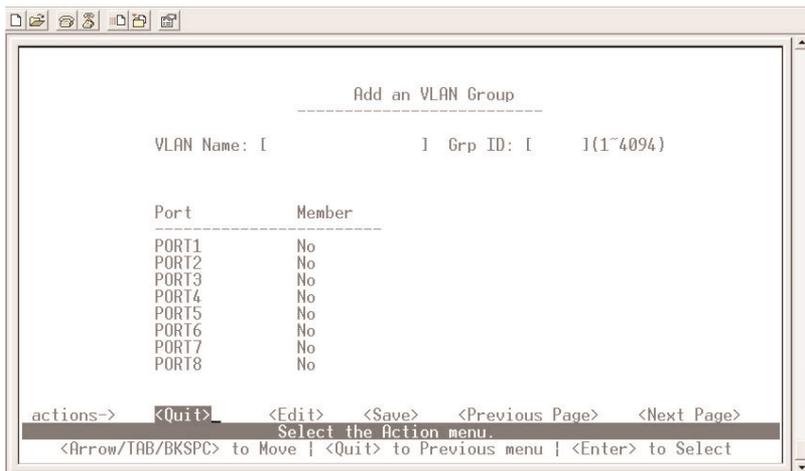
1. Use the Tab or Backspace keys to select **Edit**.
2. VLAN Name: Type a name for the new VLAN.
3. Grp ID: Type the VLAN group ID. The group ID range is 1–4094.
4. Member: Toggle the **Space** key to choose the VLAN member. Options include Member and No. If the port is a member of the current VLAN, choose **Member**. If the port is not a member of the current VLAN, choose **No**.
5. Press **Ctrl+A** to return to the action menu line.
6. Click on **Save** to save all configured values.

## NOTE

If the trunk groups exist, you can see it after port26 (for example, TRK1, TRK2, etc.) and, if desired, can choose to assign it as a member of the VLAN.

*Create 802.1q VLAN*

To create an 802.1q VLAN, go to the screen shown in Figure 8-10. To get to this screen, use the Tab or Backspace keys to select **Create a VLAN Group** in Figure 8-6, then press **Enter**.



**Figure 8-10. Add a VLAN Group screen.**

To create an 802.1q VLAN and add tagged/untagged member ports to it, follow the procedure below.

1. Use the Tab or Backspace keys to select **Edit** and press **Enter**.
2. VLAN Name: Type a name for the new VLAN.
3. VLAN ID: Type a VID (between 1–4094). The default is 1. There are 256 VLAN groups provided for configuration. Each port can join more than one (up to 256) tagged VLAN groups.
4. Protocol VLAN: Press the **Space** key to choose the protocols type. If you are not applying protocol VLAN, you must set the value to None. You can't set a port to join more than one VLAN/VID with a same protocol.

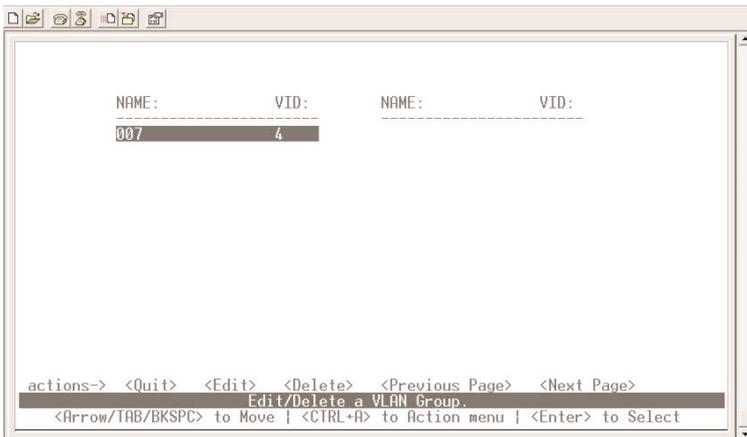
5. Member: Press the **Space** key to choose a VLAN member. There are three types to select from.
  1. Untagged: This port is a member port of this VLAN group, and outgoing frames are not VLAN tagged frames.
  2. Tagged: This port is a member port of this VLAN group, and outgoing frames are VLAN tagged frames.
  3. No: The port is not a member port of this VLAN group.
6. Press **Ctrl+A** to go back to the action menu line.
7. Click on **Save** to save all configuration values.

## NOTE

**If the trunk groups exist, you can see it after port26 (for example, TRK1, TRK2, etc.) and, if desired, can choose to assign it as a member of the VLAN.**

### *Edit/Delete a VLAN Group*

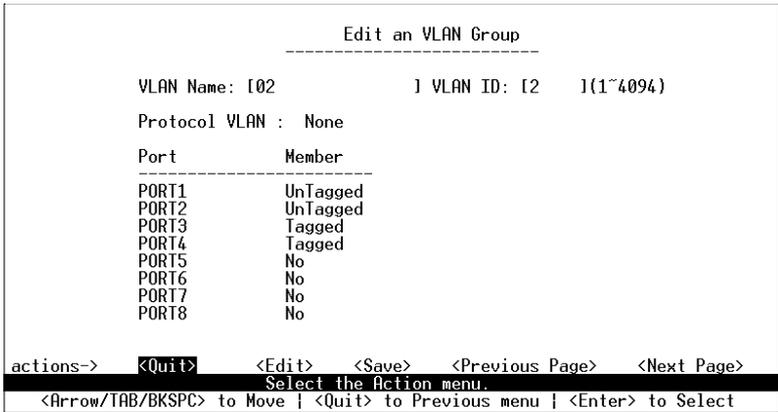
To edit or delete an existing VLAN group, go to the screen shown in Figure 8-11. To get to this screen, use the Tab or Backspace keys to select **Edit/Delete a VLAN Group** in Figure 8-6, then press **Enter**.



**Figure 8-11. Edit/Delete a VLAN Group.**

Use this page to edit or delete a VLAN group.

1. Use the Tab or Backspace keys to select **Edit** or **Delete** and then press **Enter**. The cursor appears in the VLAN Name field.
2. Type in the name of the VLAN group that you want to edit or delete and its VLAN ID.
3. You can modify the protocol VLAN item and whether the member port is tagged or untagged, and remove some member ports from an existing VLAN group. See Figure 8-12.



**Figure 8-12. Edit a VLAN Group screen.**

4. After editing the VLAN, press the **Save** key to save all configuration values.

## NOTE

1. Press **Enter** once to complete the deletion in delete mode.
2. The **VLAN Name** and **VLAN ID** cannot be modified.
3. The **Default VLAN** cannot be deleted.

### *Group Sorted Mode*

In this page (Figure 8-13), you can select VLAN group sort mode. To get to this page, use the Tab or Backspace keys to select **Group Sorted Mode** in Figure 8-6, then press **Enter**. Select **Edit**, then use the **Space** bar to toggle to the desired sort option. The options in Figure 8-13 are **Sorted by Name** and **Sorted by VID**.



**Figure 8-13. Group Sorted Selection screen.**

If you select **Sorted By Name**, Figure 8-14 appears.

NAME:	VID:	NAME:	VID:
DEFAULT	1		
A1	3		
B4	4		
U2	2		

**Figure 8-14. Sort By Name result.**

If you select **Sorted by VID**, Figure 8-15 appears.

NAME:	VID:	NAME:	VID:
DEFAULT	1		
U2	2		
A1	3		
B4	4		

**Figure 8-15. Sort By VID result.**

### *Previous Menu*

Use the Tab or Backspace keys to select this option in Figure 8-6 and then press **Enter** to go back to the Switch Static Configuration menu (Figure 8-2).

## 8.2.4 MISC CONFIGURATION

To get to the Misc Configuration screen (Figure 8-16), use the Tab or Backspace keys to select **Misc Configuration** in the Switch Static Configuration screen (Figure 8-3), then press **Enter**.



**Figure 8-16. Misc Configuration screen.**

### *MAC Age Interval*

Use the Tab or Backspace keys to select **MAC Age Interval** in Figure 8-16, then press **Enter**, and Figure 8-17 appears.

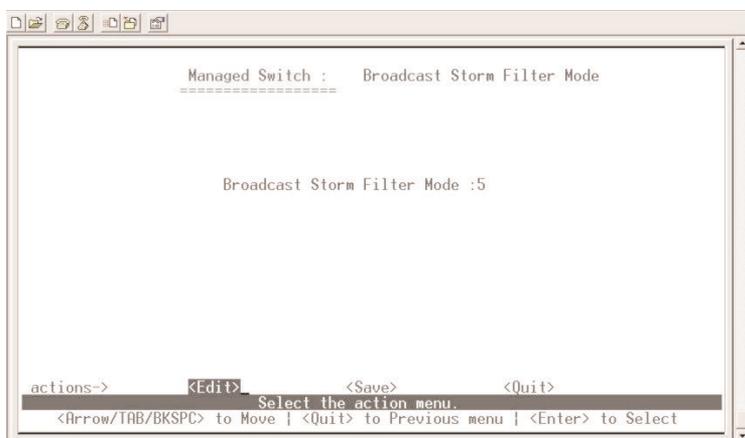


**Figure 8-17. MAC Aging Time screen.**

1. Use the Tab or Backspace keys to select **Edit**, then press **Enter**. The cursor appears in the MAC Age Interval field.
2. Type the number of seconds that an inactive MAC address remains in the switch's address table. The valid range is 300–765 seconds. The default is 300 seconds.
3. Press **Ctrl+A**, then use the Tab or Backspace keys to **Save** and press **Enter**.

### *Broadcast Storm Filtering*

Use this page (Figure 8-18) to configure broadcast storm control. To get to this screen, use the Tab or Backspace keys to select **Broadcast Storm Filtering** in the Misc Configuration screen (Figure 8-16), then press **Enter**.

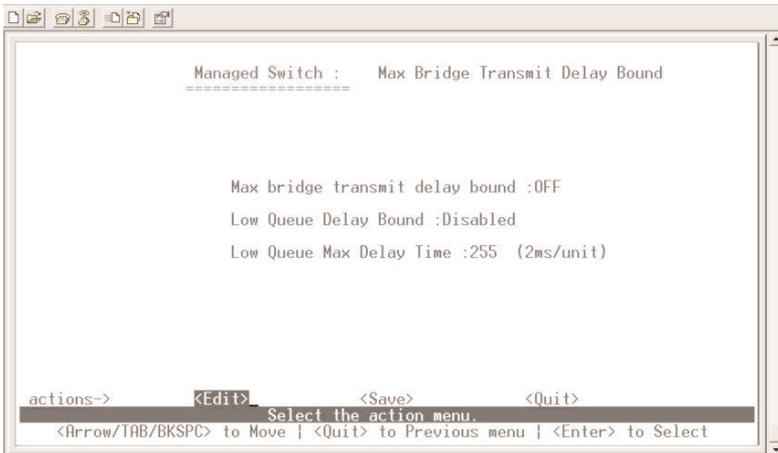


**Figure 8-18. Broadcast Storm Filter Mode screen.**

1. Use the Tab or Backspace keys to select **Edit** and press **Enter** to configure the broadcast storm filter mode.
2. Press the **Space** key to toggle the threshold value. The valid threshold values are 5%, 10%, 15%, 20%, 25%, and NO.
3. Once you select the threshold value, press **Ctrl+A** and then use the Tab or Backspace keys to select **Save** and then press **Enter**.

### *Max Bridge Transmit Delay Bound*

The screen shown in Figure 8-19 appears when you use the Tab or Backspace keys to select **Max bridge transmit delay bound** in the Misc Configuration menu (Figure 8-16), then press **Enter**.



**Figure 8-19. Max Bridge Transmit Delay Bound screen.**

Choose from three options (use the Tab or Backspace keys to move the cursor to each field):

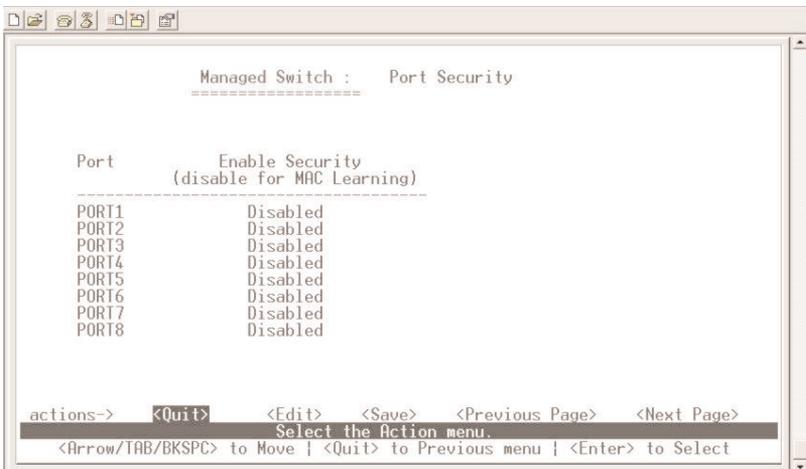
1. **Max bridge transmit delay bound:** Limit the packets queuing time in the switch. If enabled, the packets queued that have exceeded this time frame will be dropped. Press the **Space** key to toggle between valid time values (1, 2, and 4 secs, and OFF). The default is OFF.
2. **Low Queue Delay Bound:** Limits the low-priority packets' queuing time in the switch. When enabled, the low-priority packets in the switch that have exceeded the Low Queue Max Delay Time will be sent. Press the **Space** key to toggle between **Enable** or **Disable**.
3. **Low Queue Max Delay Time:** Sets the time that low-priority packets are queued in the switch. The default Low Queue Max Delay Time is 255 ms. Type in a value between 1 and 255 ms.
4. Press **Ctrl+A**, then use the Tab or Backspace keys to select **Save** and press **Enter**.

**NOTE**

Make sure that the Max Bridge Transmit Delay Bound control is enabled before the Low Queue Delay Bound is enabled, because the former must be activated before the latter will work.

*Port Security*

A port in security mode will be locked and does not permit address learning. To get to the screen shown in Figure 8-20, use the Tab or Backspace keys to select **Port Security** in the Misc Configuration menu (Figure 8-16), then press **Enter**. Only incoming packets with Static Media Access Control (SMAC) already existing in the address table can be forwarded normally.



**Figure 8-20. Port Security screen.**

1. Use the Tab or Backspace keys to select **Edit** and press **Enter**.
2. Press the **Space** key to toggle between **Enable** and **Disable**.
3. Press **Ctrl+A** to go back to the action menu line.
4. Use the Tab or Backspace keys to select **Save** and press **Enter** to save all configured values.
5. Press **Next Page** to configure port9–port26, or press **Previous Page** to return to the last page.

### *Collisions Retry Forever*

To get to the screen shown in Figure 8-21, use the Tab or Backspace keys to select **Collisions Retry Forever** in the Misc Configuration menu (Figure 8-16), then press **Enter**. When Collisions Retry Forever is disabled in half-duplex, if a collision happens, the switch will retry to send the frame 48 times before the frame is dropped.

When this option is enabled in half-duplex, if a collision happens, the switch will retry to send the frame indefinitely.

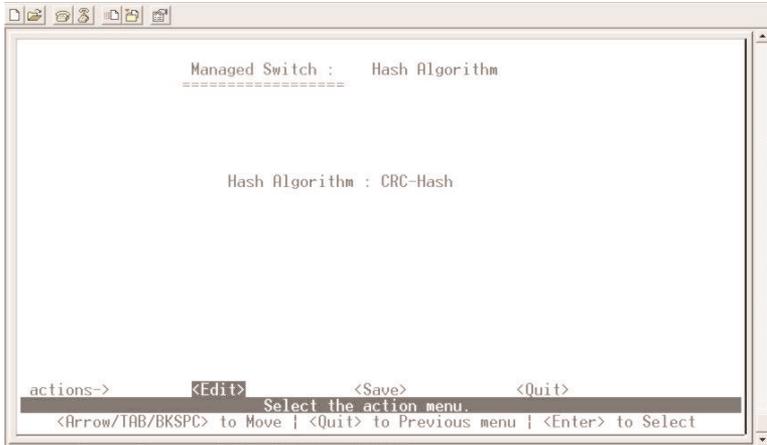


**Figure 8-21. Collisions Retry Forever screen.**

1. Use the Tab or Backspace keys to select **Edit** and press **Enter**.
2. Toggle between **Enabled** and **Disabled**.
3. Press **Ctrl+A**, then use the Tab or Backspace keys to select **Save** and press **Enter**.

*Hash Algorithm*

To get to the screen shown in Figure 8-22, use the Tab or Backspace keys to select **Hash Algorithm** in the Misc Configuration menu (Figure 8-16), then press **Enter**. Options include CRC-Hash (the default) or Direct-Map Hash Algorithm. CRC-Hash (Cyclic Redundancy Checksum) maintains the MAC table by sorting out the entries. Direct-Map Hash maintains the MAC table without sorting the entries.

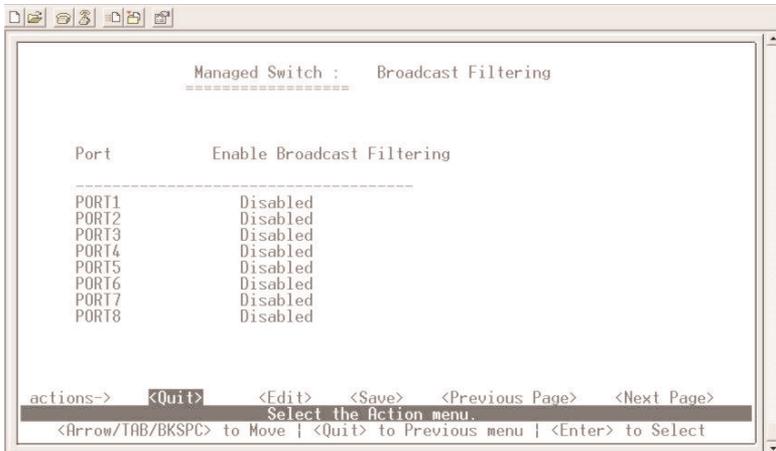


**Figure 8-22. Hash Algorithm screen.**

1. Use the Tab and Backspace keys to select **Edit** and press **Enter**.
2. Press the **Space** key to toggle between CRC-Hash and Direct-Map Hash.
3. Press **Ctrl+A**, then use the Tab and Backspace keys to select **Save** and press **Enter**.

## Broadcast Filtering

In a regular wired LAN network, there is a lot of broadcasted traffic. In order to filter broadcast traffic, you may disable or enable Broadcast Filtering for each port. To get to the screen shown in Figure 8-23, use the Tab or Backspace keys to select **Broadcast Filtering** in the Misc Configuration menu (Figure 8-16), then press **Enter**.



**Figure 8-23. Broadcast Filtering screen.**

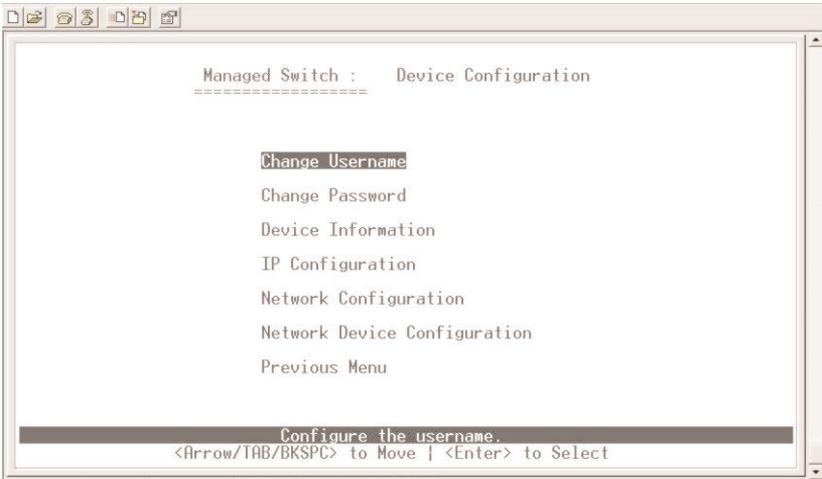
1. Use the Tab or Backspace keys to select **Edit** and then press **Enter**.
2. Press the **Space** key to toggle between **Enabled** and **Disabled**.
3. Press **Ctrl+A**, then use the Tab or Backspace keys to select **Save** and press **Enter**.

## Previous Menu

Use the Tab or Backspace keys to select this option in Figure 8-16, then press **Enter**, to go back to the Switch Static Configuration menu (Figure 8-3).

## 8.2.5 ADMINISTRATION CONFIGURATION

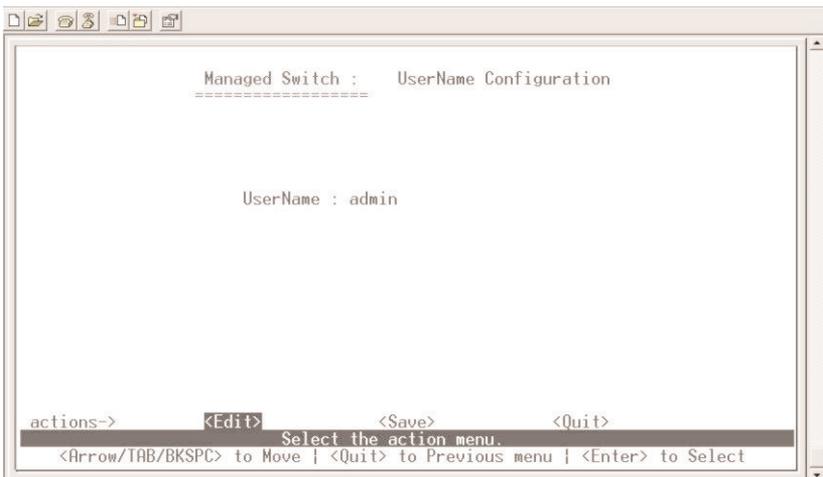
Several administration functions can be configured from the switch's Device Configuration menu. To get to the screen shown in Figure 8-24, use the Tab or Backspace keys to select **Administration Configuration** in the Switch Static Configuration menu (Figure 8-3), then press **Enter**.



**Figure 8-24. Device Configuration screen.**

### *Change Username*

Use this page (Figure 8-25) to change the Web management user name. To get to this screen, use the Tab or Backspace keys to select **Change Username** in Figure 8-24, then press **Enter**.



**Figure 8-25. UserName Configuration screen.**

1. Use the Tab or Backspace keys to select **Edit**, then press **Enter**.
2. Type the new user name.
3. Press **Ctrl+A**.
4. Use the Tab or Backspace keys to select **Save** and then press **Enter** to change the username.

### *Change Password*

Use this page (Figure 8-26) to change the Web management login password. To get to this screen, use the Tab or Backspace keys to select **Change Password** in Figure 8-24, then press **Enter**.

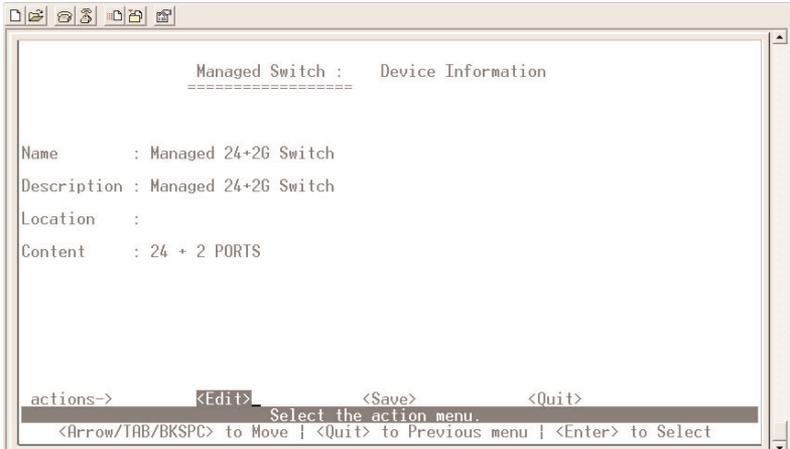


**Figure 8-26. Password Configuration screen.**

1. Use the Tab or Backspace keys to select **Edit** and then press **Enter**.
2. Type in the old password, then press **Enter**.
3. Type in the new password, then press **Enter**.
4. Press **Enter** again.
5. Press **Ctrl+A**, then use the Tab or Backspace keys to select **Save** and press **Enter**.

*Device Information*

Use this page (Figure 8-27) to configure the device information. To get to this screen, use the Tab or Backspace keys to select **Device Information** in Figure 8-24, then press **Enter**.

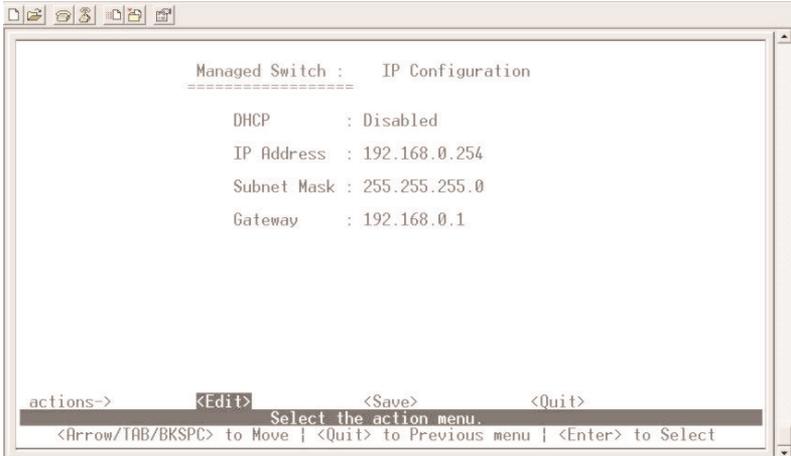


**Figure 8-27. Device Information screen.**

1. Use the Tab or Backspace keys to select **Edit** and press **Enter**.
2. Type in the name, description, location, and content. (Content is the number of twisted-pair plus fiber ports.)
3. Press **Ctrl+A**, then use the Tab or Backspace keys to select **Save** and press **Enter**.

## IP Configuration

Use this page (Figure 8-28) to configure the IP setting and fill in the new value. To get to this screen, use the Tab or Backspace keys to select **IP Configuration** in Figure 8-24, then press **Enter**.

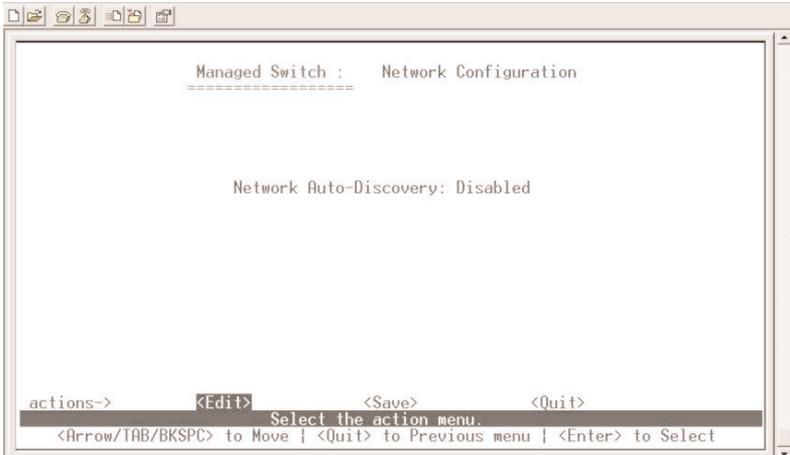


**Figure 8-28. IP Configuration screen.**

1. Use the Tab or Backspace keys to select **Edit**, then press **Enter**.
2. Type in the DHCP, IP address, subnet mask, and gateway.
3. Press **Ctrl+A**, then use the Tab or Backspace keys to select **Save** and then press **Enter**.

*Network Configuration*

Use this page (Figure 8-29) to enable or disable the network device autodiscovery feature. To get to this screen, use the Tab or Backspace keys to select **Network Configuration** in Figure 8-24, then press **Enter**.

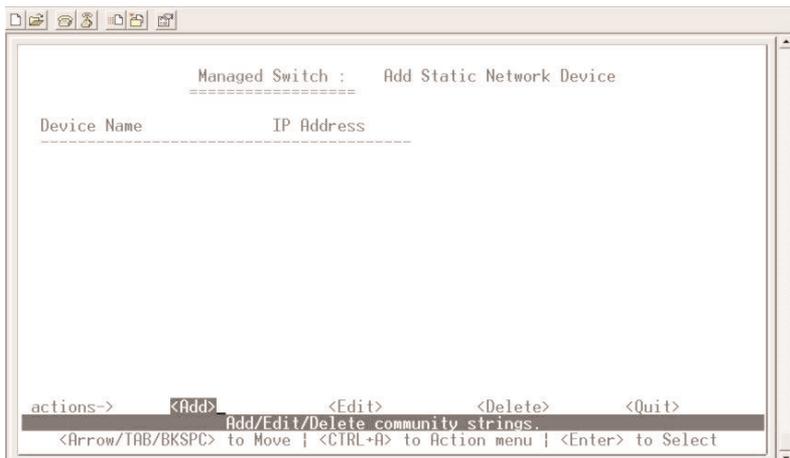


**Figure 8-29. Network Configuration screen.**

1. Use the Tab or Backspace keys to select **Edit** and press **Enter**.
2. Use the **Space** bar to toggle between **Disabled** and **Enabled**.
3. Press **Ctrl+A**, then use the Tab or Backspace keys to select **Save** and press **Enter**.

### Network Device Configuration

Configure and add static network devices. Use the Tab or Backspace keys to select **Network Device Configuration** in Figure 8-24, then press **Enter** to get to the screen shown in Figure 8-30.

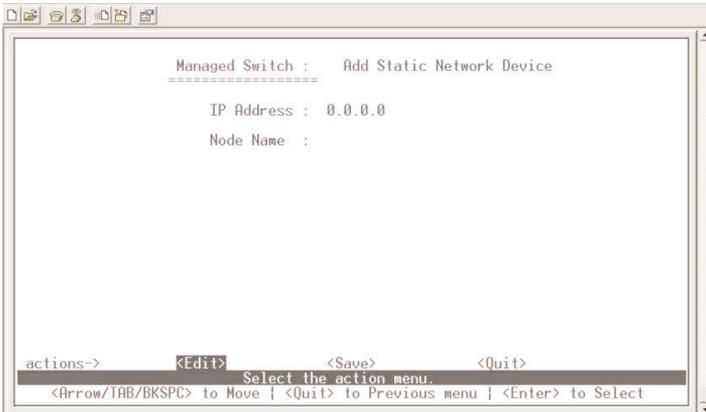


**Figure 8-30. Add Static Network Device screen.**

1. Use the Tab or Backspace keys to select **Add** and then press **Enter**.
2. Type in the device name and IP address.
3. Press **Ctrl+A**, then use the Tab or Backspace keys to select **Save** and then press **Enter**.

Or,

1. Use the Tab or Backspace keys to select **Edit** in Figure 8-30, then press **Enter** to get to the screen shown in Figure 8-31.



**Figure 8-31. Edit Static Network Device screen.**

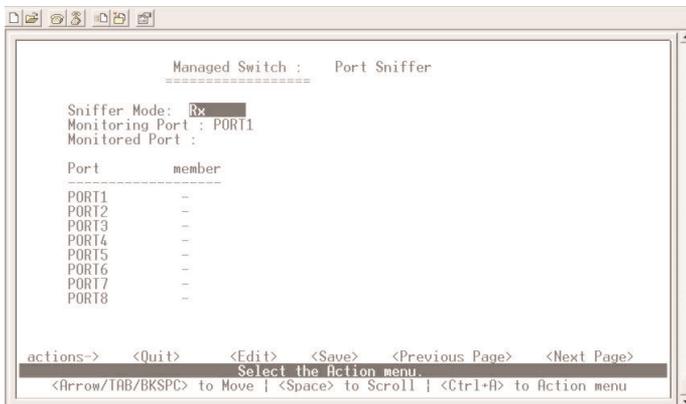
2. Type in the IP address and node name.
3. Press **Ctrl+A**, then use the Tab or Backspace keys to select **Save** and press **Enter**.

### *Previous Menu*

Use the Tab or Backspace keys to select this option in Figure 8-24, then press **Enter** to go back to the Switch Static Configuration menu (Figure 8-3).

## 8.2.6 PORT MIRRORING CONFIGURATION

The port mirroring is a method for monitoring traffic in switched networks. Traffic passing through ports can be monitored by one specific port. That is, the traffic going in or out of the monitored ports will be duplicated into a separate monitoring port. See Figure 8-32. To get to this screen, use the Tab or Backspace keys to select **Port Mirroring Configuration** in Figure 8-3, then press **Enter**.



**Figure 8-32. Port Sniffer screen.**

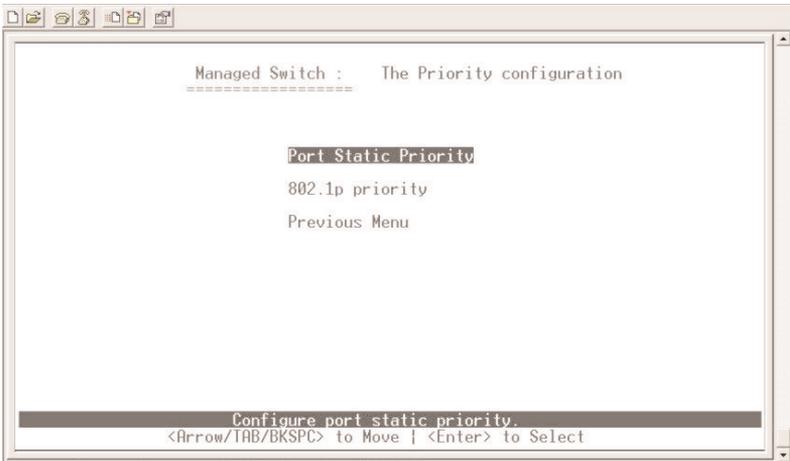
1. Use the Tab or Backspace keys to select **Edit** and press **Enter**.
2. Sniffer Mode: Press the **Space** key to toggle the sniffer mode. The options are: Disable, Rx, Tx, and Both.
3. Monitoring Port: The sniffer port can be used to monitor all ports' traffic. Press the **Space** key to select the desired port.
4. Monitored Port: This is the port you want to monitor. All monitored port traffic will be copied to the sniffer port. You can select a maximum of 25 monitored ports in the switch. Choose the ports to be monitored in one sniffer mode. Press the **Space** key to select the member port: "V" is a member, and "-" isn't a member.
5. Press **Ctrl+A** go back to the action menu line.
6. Use the Tab or Backspace keys to select **Save** and press **Enter** to save all configured values.
7. On the action menu line you can press **Next Page** to configure port9–port26, or select **Previous Page** to return to the last page.

**NOTE**

Only one sniffer mode can be activated at a time.

**8.2.7 PRIORITY CONFIGURATION**

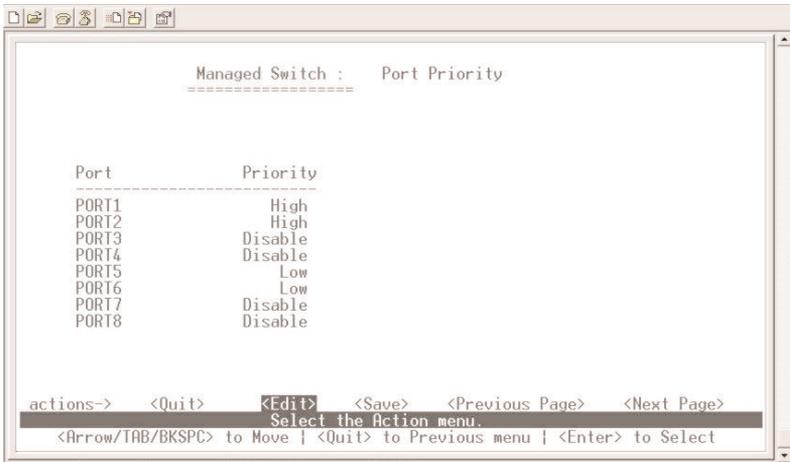
From the Priority Configuration screen (Figure 8-33), you can set Port Static Priority or 802.1p Priority. To get to this screen, use the Tab or Backspace keys to select **Priority Configuration** in Figure 8-3, then press **Enter**.



**Figure 8-33. Priority Configuration screen.**

## Port Static Priority

The static priority is port-based. When a port is assigned with a high priority, incoming frames from this port always have a high priority. To get to the screen shown in Figure 8-34, use the Tab or Backspace keys to select **Port Static Priority** in Figure 8-33, then press **Enter**.

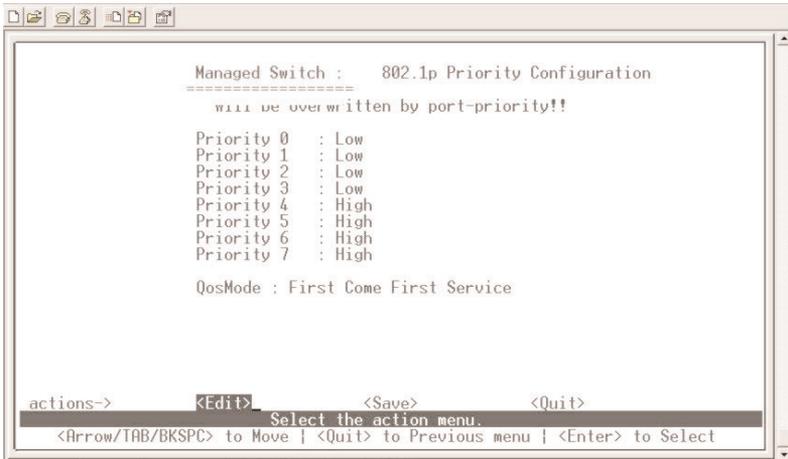


**Figure 8-34. Port Priority screen.**

1. Use the Tab or Backspace keys to select **Edit** and press **Enter**.
2. Press the **Space** key to toggle between High, Low, and Disable for each port.
3. Press **Ctrl+A** to go back to the action menu line.
4. Use the Tab or Backspace keys to select **Save** and press **Enter** to save all configured values.

### 802.1p Priority

There are 0–7 priority queue levels that can be assigned. To get to the screen shown in Figure 8-35, use the Tab or Backspace keys to select **802.1p Priority** in Figure 8-33, then press **Enter**.



**Figure 8-35. 802.1p Priority Configuration screen.**

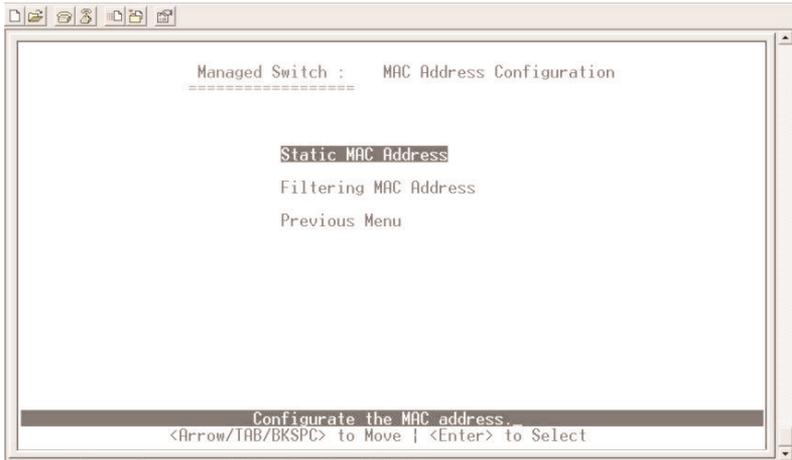
1. Use the Tab or Backspace keys to select **Edit** and press **Enter**.
2. Press the **Space** key to select the priority level mapping from Low to High queue.
3. High/Low Queue Service Ratio H:L—Select the ratio of high-priority packets and low-priority packets.
4. Press **Ctrl+A** to go back to the action menu line.
5. Use the Tab or Backspace keys to select **Save** and press **Enter** to save all configured values.

### Previous Menu

Use the Tab or Backspace keys to select this option in Figure 8-33 to go back to the Switch Static Configuration Menu (Figure 8-3).

### 8.2.8 MAC ADDRESS CONFIGURATION

To get to the screen shown in Figure 8-36, use the Tab or Backspace keys to select **MAC Address Configuration** in Figure 8-3, then press **Enter**.



**Figure 8-36. MAC Address Configuration screen.**

#### *Static MAC Address*

When you add a static MAC address, it remains in the switch's address table regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the switch is disconnected or powered off and becomes active on the network again.

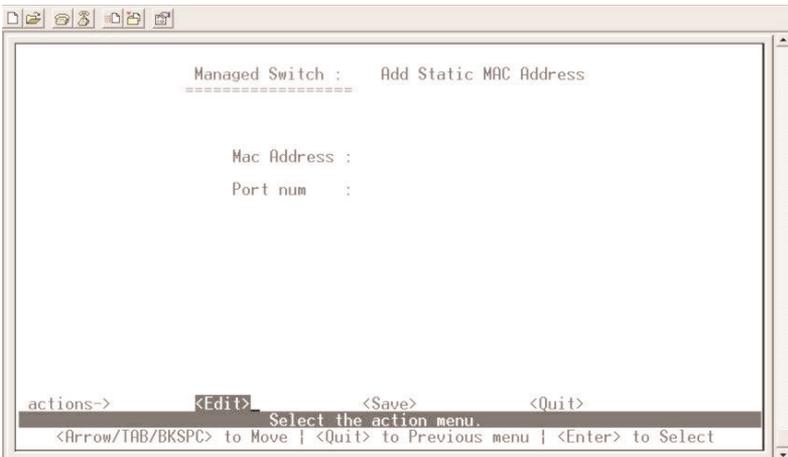
In this screen (Figure 8-37), you can add, edit, or delete a static MAC address. To get to this screen, use the Tab or Backspace keys to select **Static MAC Address Configuration** in Figure 8-36, then press **Enter**.



**Figure 8-37. Static MAC Address Configuration screen.**

#### *Add Static MAC Address*

1. Select **Add** and then **Edit** to add a static MAC address. Figure 8-38 appears.



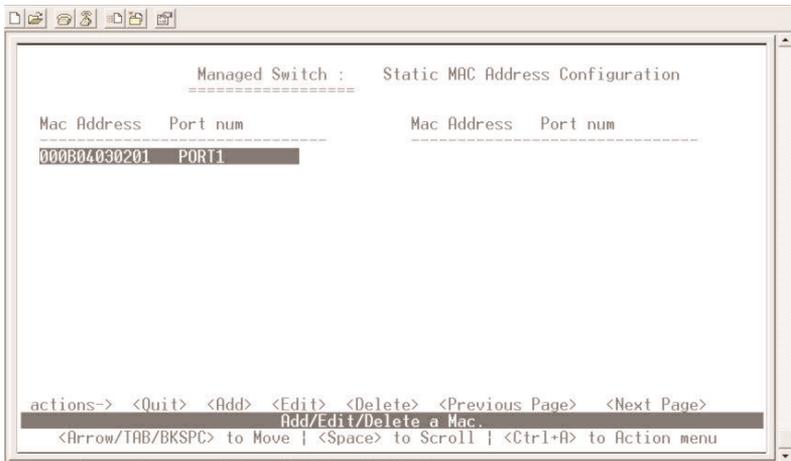
**Figure 8-38. Add Static MAC Address screen.**

2. MAC Address: Type in the MAC address to the port that should permanently forward traffic regardless of the switch's network activity.

3. Port num: Type in the port number.
4. Press **Ctrl+A** to go back to the action menu line, and then use the Tab or Backspace keys to select **Save** and press **Enter** to save all configured values.

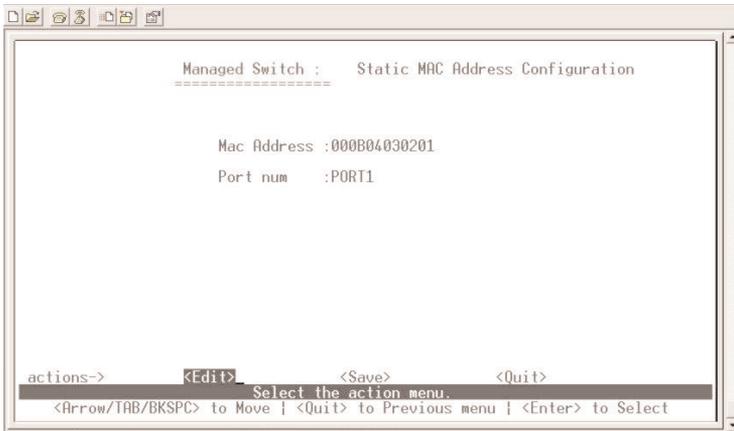
### *Edit Static MAC Address*

1. Use the Tab or Backspace keys to select the **Edit** key and press **Enter**. Figure 8-39 appears.



**Figure 8-39. Static MAC Address Configuration screen.**

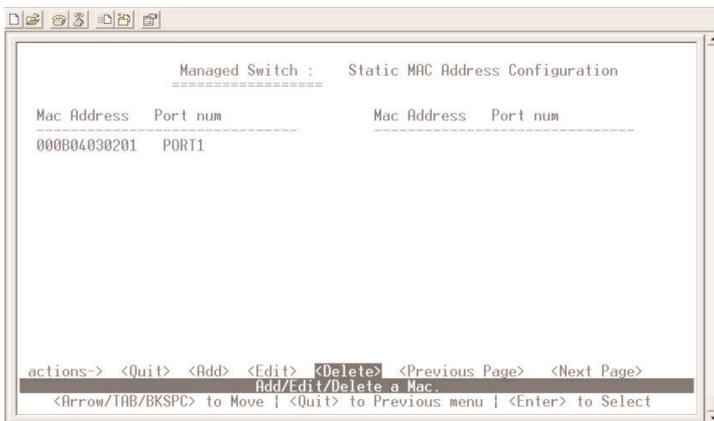
2. Press the **Edit** key to modify all the items.
3. Press **Ctrl+A** to go back to the action menu line, and then select **Save** to save all configured values.



**Figure 8-40. Edit Static MAC Address Configuration screen.**

#### *Delete Static MAC Address*

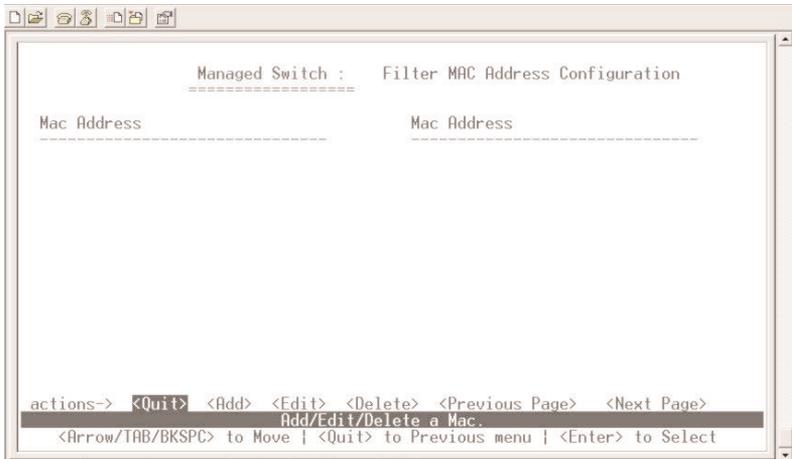
1. Use the Tab or Backspace keys to select the **Delete** key in Figure 8-41, then press **Enter**.
2. Use the **Space** bar to toggle to the MAC address that you want to delete and then press **Enter**.
3. Press **Enter** once to complete the deletion.



**Figure 8-41. Delete Static MAC Address Configuration screen.**

### Filtering MAC Address

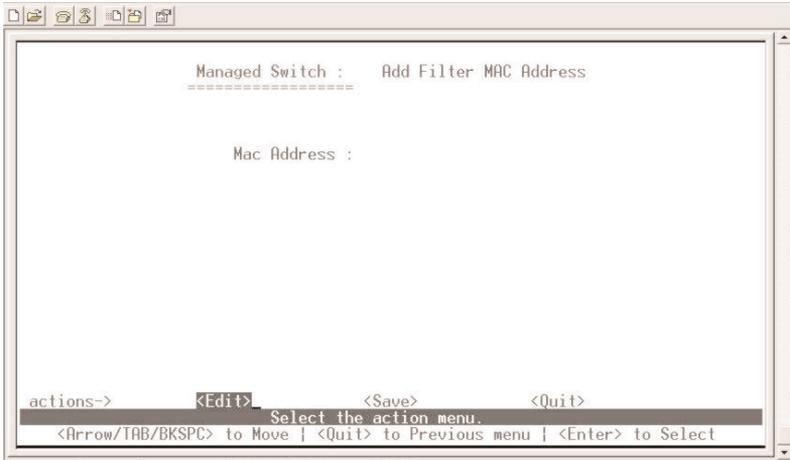
MAC address filtering allows the switch to drop unwanted traffic. Traffic is filtered based on the destination addresses. In this page (Figure 8-42), you can add, modify, or delete filter MAC addresses. To get to this screen, use the Tab or Backspace keys to select **Filter MAC Address Configuration** in Figure 8-36, then press **Enter**.



**Figure 8-42. Filter MAC Address Configuration screen.**

### Add Filter MAC Address

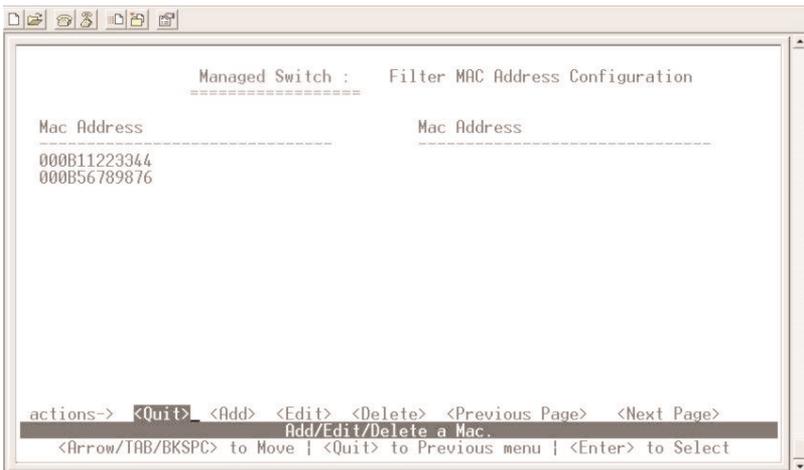
1. Use the Tab or Backspace keys to select **Add** and press Enter, then select **Edit** and press **Enter** to add a filter MAC address.
2. MAC Address: Type in the MAC address to be filtered.
3. VLAN ID: If they are tag-based (802.1q), VLANs are set up on the switch. Type the VID to associate with the MAC address.
4. Press **Ctrl+A** to go back to the action menu line, and then select **Save** and press **Enter** to save all configured values.



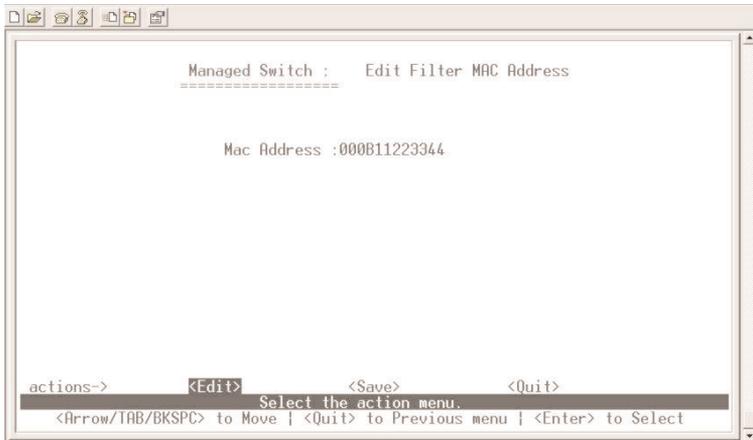
**Figure 8-43. Add Filter MAC Address screen.**

#### *Edit Filter MAC Address*

1. Use the Tab or Backspace keys to select **Edit**, then press **Enter**.
2. Type in the MAC address that you want to modify. Figure 8-44 appears.



**Figure 8-44. Filter MAC Address Configuration screen.**



**Figure 8-45. Edit Filter MAC Address screen.**

3. Use the Tab or Backspace keys to select **Edit** and then press **Enter** to modify all the items.
4. Press **Ctrl+A** to go back to the action menu line, and then use the Tab or Backspace keys to select **Save** and press **Enter** to save all configured values.

### *Delete Filter MAC Address*

1. Use the Tab or Backspace keys to select **Delete** and then press **Enter** to delete a filter MAC address.
2. Use the Tab or Backspace keys to toggle to the MAC address that you want to delete and then press **Enter**.
3. By pressing **Enter** once, the deletion will be completed.

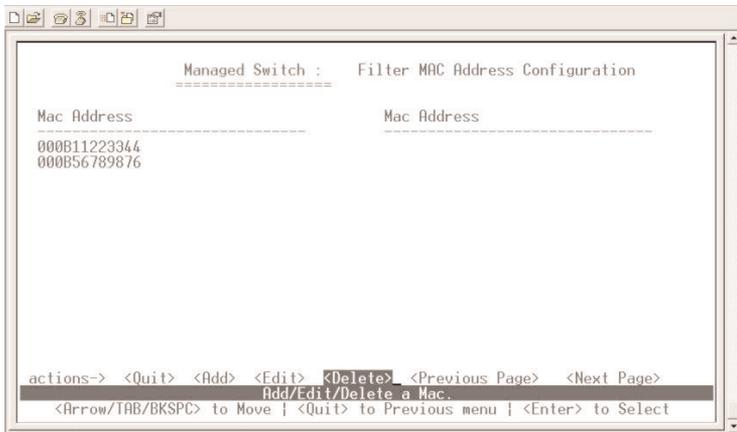


Figure 8-46. Delete Filter MAC Address Configuration screen.

### Previous Menu

Use the Tab or Backspace keys to select this option in Figure 8-36, then press **Enter** to go back to the Switch Static Configuration menu (Figure 8-3).

## 8.3 Protocol Related Configuration

To get to the screen shown in Figure 8-47, use the Tab or Backspace keys to select **Protocol Related Configuration** in the Main Menu (Figure 8-2), then press **Enter**.

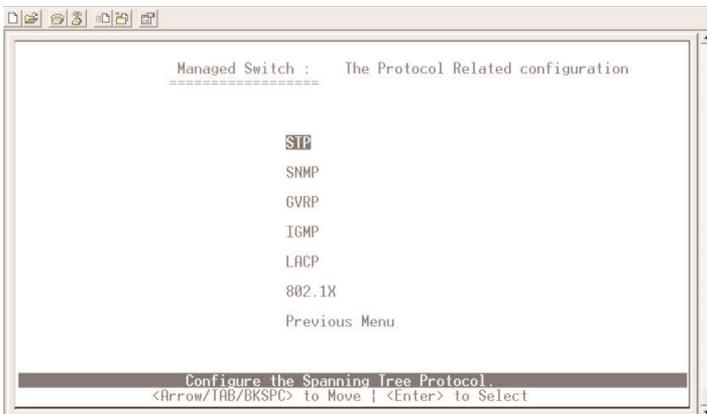


Figure 8-47. Protocol Related Configuration screen.

## 8.3.1 SPANNING TREE PROTOCOL (STP)

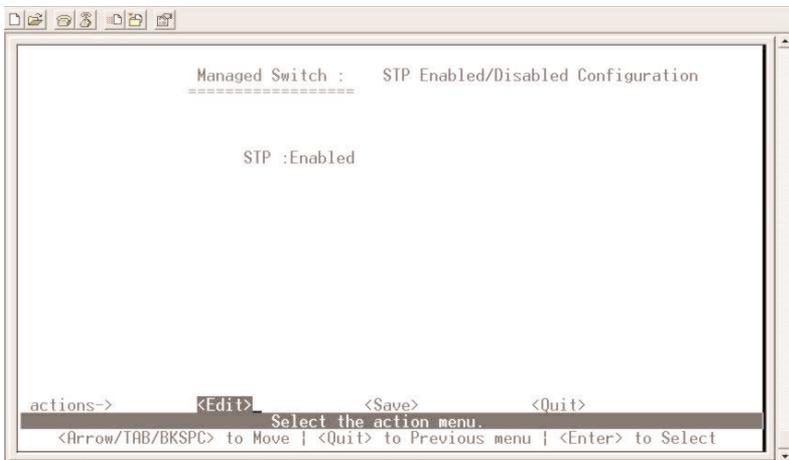
Use the Tab or Backspace keys to go to the STP option. Then press **Enter**, and Figure 8-48 appears.



**Figure 8-48. Spanning Tree Protocol screen.**

### *STP Enable*

Use this page (Figure 8-49) to enable or disable the Spanning Tree Protocol (STP) function.

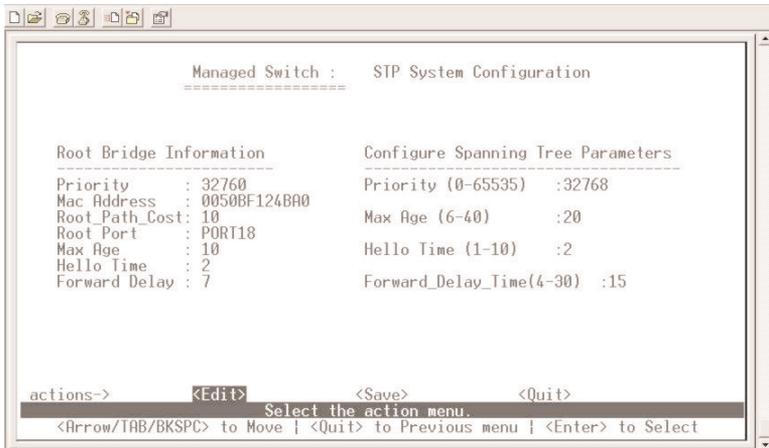


**Figure 8-49. STP Enabled/Disabled Configuration screen.**

1. Use the Tab or Backspace keys to select **Edit**, then press **Enter**.
2. Press the **Space** key to select enable or disable.
3. Press **Ctrl+A**, then use the Tab or Backspace keys to select **Save** and press **Enter**.

### System Configuration

In the STP System Configuration screen (Figure 8-50), you can view spanning tree information about the root bridge on the left. On the right, you can set new values for STP parameters.

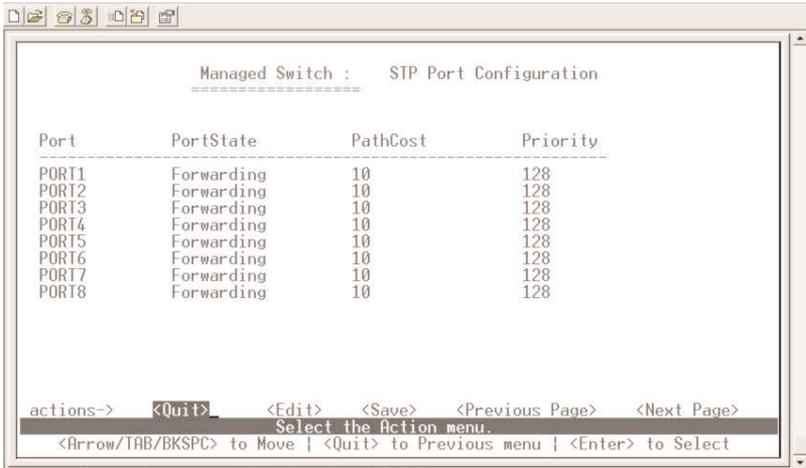


**Figure 8-50. STP System Configuration screen.**

1. Use the Tab or Backspace keys to select **Edit**, then press **Enter**.
2. Press the **Tab** or **Backspace** keys to move between fields.
3. Press the **Space** key to toggle STP parameters including Priority, Max. Age, Hello Time, and Forward Delay Time.
4. Press **Ctrl+A**, then use the Tab or Backspace keys to select **Save** and press **Enter**.

## Per Port Configuration

To configure each port, use the Tab or Backspace keys to select **Perport Configuration** from the STP screen (Figure 8-48). Figure 8-51 appears.



**Figure 8-51. STP Port Configuration screen.**

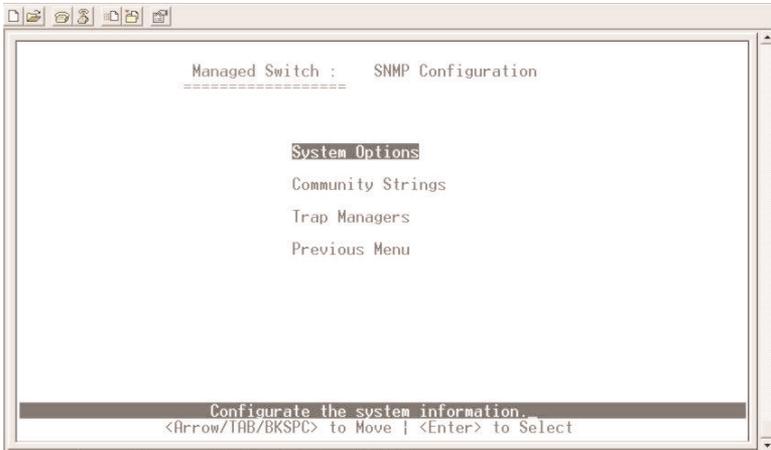
1. PortState: Display spanning tree status about each port whether it is forwarding or blocking.
2. Use the Tab or Backspace keys to select **Edit** and then press **Enter**.
3. PathCost: Specifies the path cost of the port that the switch uses to determine which ports are the forwarding ports.
4. Priority: This means port priority. You can make it higher or lower or, more likely, the root port.
5. Press **Ctrl+A** go back to the action menu line.
6. Use the Tab or Backspace keys to select **Save** and press **Enter** to save all configured values.
7. On the action menu line you can press **Next Page** to configure port9–port26, or press **Previous Page** to return to the last page.

## Previous Menu

Use the Tab or Backspace keys to select this option in Figure 8-48, then press **Enter** to go back to the Switch Static Configuration menu (Figure 8-3).

### 8.3.2 SNMP

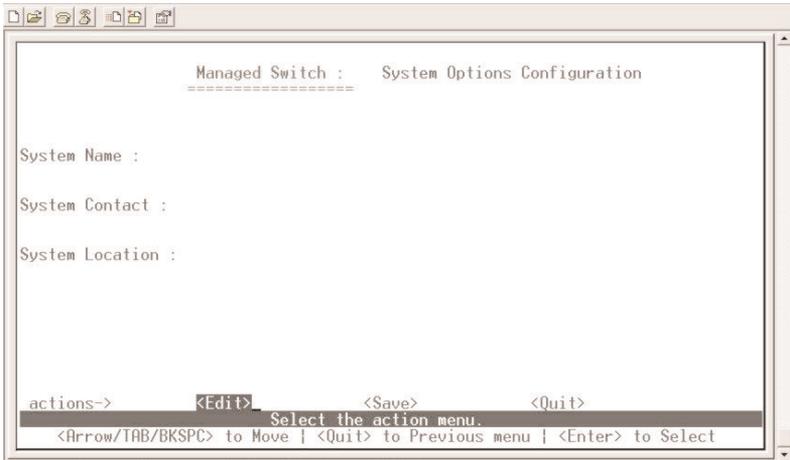
Any network management running the Simple Network Management Protocol (SNMP) can manage the switch. Use this page (Figure 8-52) to define management stations as trap managers and to enter SNMP community strings. You can also define a name, location, and contact person for the switch. To get to this page, use the Tab or Backspace keys to select **SNMP** in Figure 8-47. Then press **Enter**.



**Figure 8-52. SNMP Configuration screen.**

### *System Options*

Configure the system name, contact, and location via Figure 8-53. To get to this screen, use the Tab or Backspace keys to select **System Options** in Figure 8-52. Then press **Enter**.

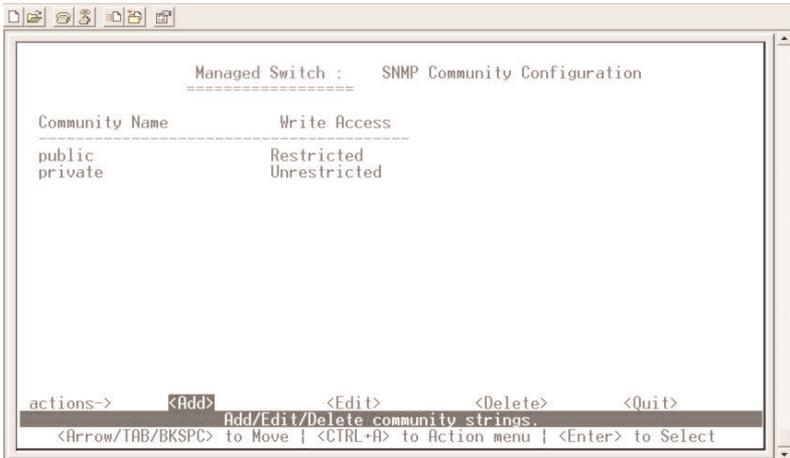


**Figure 8-53. System Options Configuration screen.**

1. Use the Tab or Backspace keys to select **Edit** and then press **Enter**.
2. System Name: Type a name to be used for the switch.
3. System Contact: Type the name of contact person or organization.
4. System Location: Type the location of the switch.
5. Press **Ctrl+A** to return to the action menu line.
6. Use the Tab or Backspace keys to select **Save** and press **Enter** to save the configured value.

### Community Strings

Use this page (Figure 8-54) to add, edit, or delete SNMP community strings. To get to this page, use the Tab or Backspace keys to select **Community Strings** in Figure 8-52, then press **Enter**.



**Figure 8-54. SNMP Community Configuration screen.**

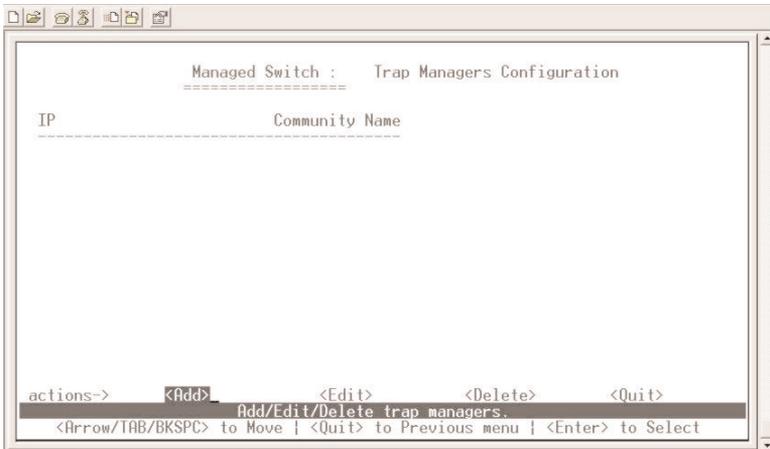
1. Community Name: The name of current strings.
2. Write Access: Enable the rights as read only or read-write.

**Restricted:** Read-only, enables requests accompanied by this string to display MIB-object information.

**Unrestricted:** Read-write, enables requests accompanied by this string to display MIB-object information and to set MIB objects.

### *Trap Managers*

A trap manager is a management station that receives traps (system alerts generated by the switch). If no trap manager is defined, no traps can be issued. Create a trap manager by entering the IP address of the station and a community string. See Figure 8-55. To get to this screen, use the Tab or Backspace keys to select **Trap Managers** in Figure 8-52, then press **Enter**.



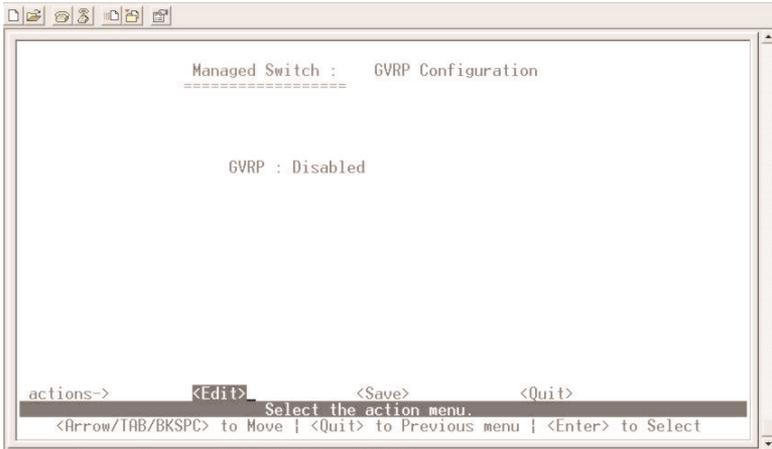
**Figure 8-55. Trap Managers Configuration screen.**

### *Previous Menu*

Use the Tab or Backspace keys to select this option in Figure 8-52, then press **Enter** to go back to the Protocol Related Configuration menu (Figure 8-47).

### 8.3.3 GVRP

Use this page (Figure 8-56) to enable or disable the GVRP (GARP VLAN Registration Protocol) support. To get to this page, use the Tab or Backspace keys to select **GVRP** in Figure 8-47, then press **Enter**.

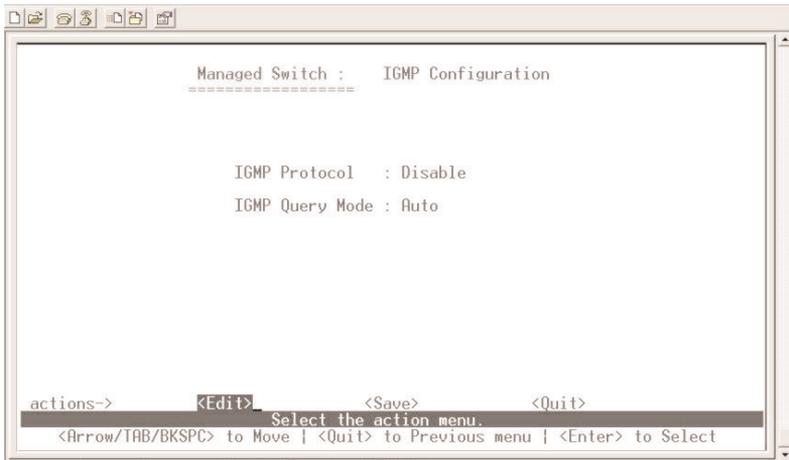


**Figure 8-56. GVRP Configuration screen.**

1. Use the Tab or Backspace keys to select **Edit** and then press **Enter**.
2. Press the **Space** key to choose Enabled or Disabled.
3. Press **Ctrl+A** go to the action menu line.
4. Use the Tab or Backspace keys to select **Save** and press **Enter** to save the configured value.

## 8.3.4 IGMP

Use this page (Figure 8-57) to enable or disable the IGMP support. To get to this page, use the Tab or Backspace keys to select **IGMP** in Figure 8-47, then press **Enter**.

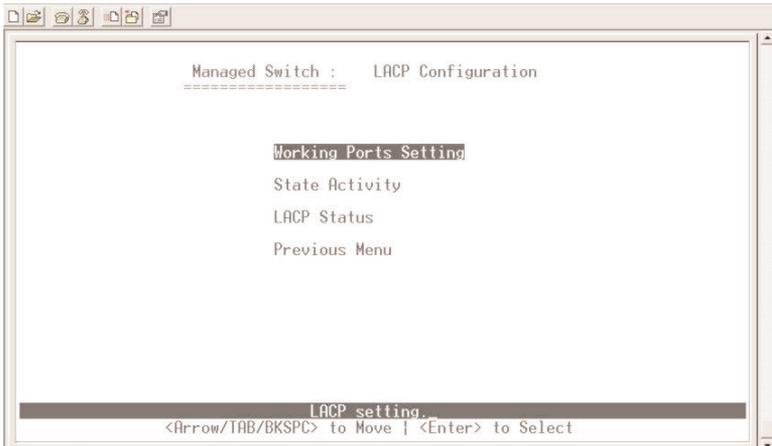


**Figure 8-57. IGMP Configuration screen.**

1. Use the Tab or Backspace keys to select **Edit** and then press **Enter**.
2. Press the **Space** key to choose **Enabled** or **Disabled**.
3. Press **Ctrl+A** go to the action menu line.
4. Use the Tab or Backspace keys to select **Save** and press **Enter** to save the configured value.

### 8.3.5 LACP

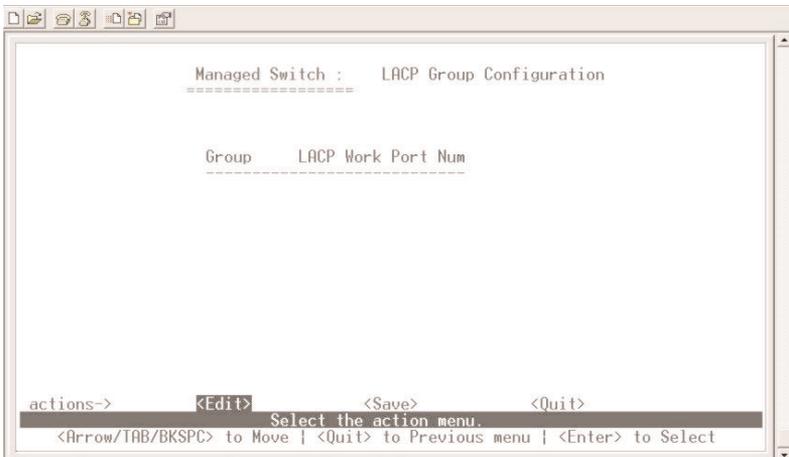
Use this page (Figure 8-58) to configure and view all LACP status. To get to this page, use the Tab or Backspace keys to select **LACP** in Figure 8-47, then press **Enter**.



**Figure 8-58. LACP Configuration screen.**

#### *Working Ports Setting*

Use this page (Figure 8-59) to set the actual work ports in a trunk group. To get to this page, use the Tab or Backspace keys to select **Working Ports Setting** in Figure 8-58, then press **Enter**.



**Figure 8-59. LACP Group Configuration screen.**

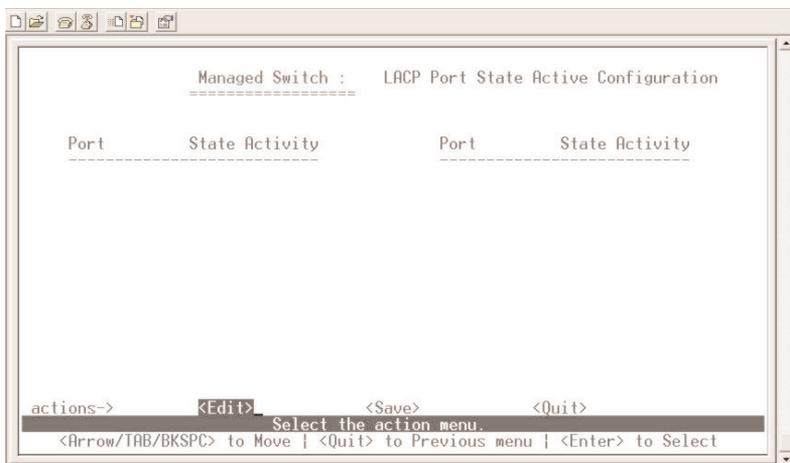
1. Select **Edit**.
2. Group: Display the trunk group ID.
3. LACP: Display the trunk group's LACP status.
4. LACP Work Port Num: The maximum number of ports that can be aggregated at the same time. If it is a LACP static trunking group, ports that exceed the maximum number of ports are standby and able to aggregate if work ports fail. If it is a local static trunking group, the number must be the same as group ports.

### NOTE

**Before setting this page, you have to set the trunk groups on the Trunk Configuration screen (Figure 8-5) first.**

#### *State Activity*

To get to the screen shown in Figure 8-60, use the Tab or Backspace keys to select **State Activity** in Figure 8-58, then press **Enter**.



**Figure 8-60. LACP Port State Active Configuration screen.**

1. Use the Tab or Backspace keys to select **Edit** and then press **Enter**.
2. Press the **Space** key to choose the item.

Active: The port automatically sends LACP protocol packets.

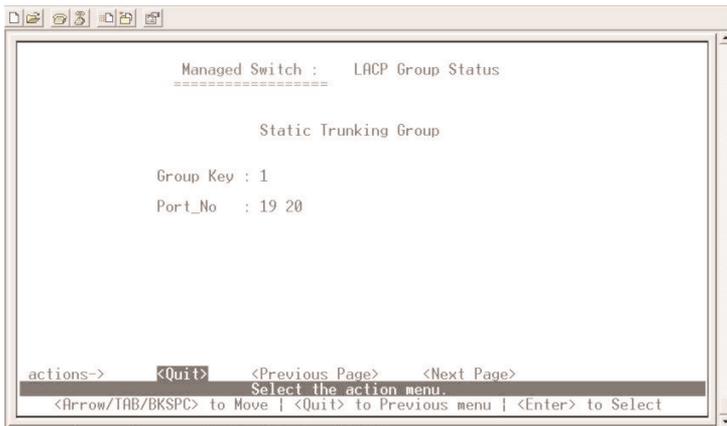
Passive: The port does not automatically send LACP protocol packets, and responds only if it receives LACP protocol packets from another device.

3. Press **Ctrl+A** to go to the action menu line.
4. Use the Tab or Backspace keys to select **Save** and press **Enter** to save the configured value.

If you set LACP mode in the trunk group, all of the member ports of this trunk group will be set to an Active status automatically.

### *LACP Status*

When you have set the trunking groups, go to the following page (Figure 8-61) to see the related static trunk group information. To get to this page, use the Tab or Backspace keys to select **LACP Status** in Figure 8-58, then press **Enter**.



**Figure 8-61. LACP Group Status screen.**

Quit: Exit this page and return to the previous menu.

Previous Page: Return to the previous page.

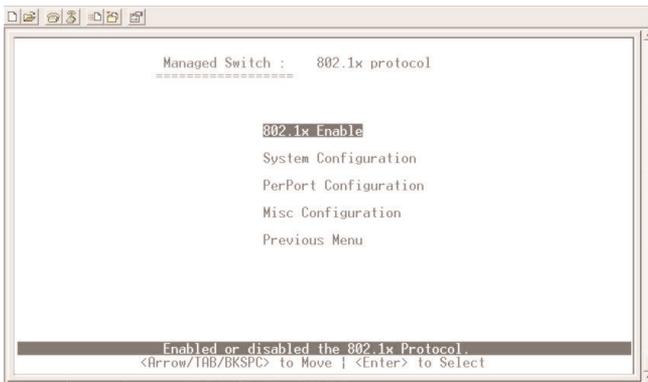
Next Page: Go to the next page.

## Previous Menu

Use the Tab or Backspace keys to select this option in Figure 8-58, then press **Enter** to go back to the Protocol Related Configuration menu (Figure 8-47).

### 8.3.6 802.1X PROTOCOL

This page (Figure 8-62) can configure and view all the 802.1x status. To get to this page, use the Tab or Backspace keys to select **802.1X** in Figure 8-47, then press **Enter**.



**Figure 8-62. 802.1x Protocol screen.**

### 802.1x Enable

To enable or disable 802.1x, go to Figure 8-63. To get to this page, use the Tab or Backspace keys to select **802.1x Enable** in Figure 8-62, then press **Enter**.

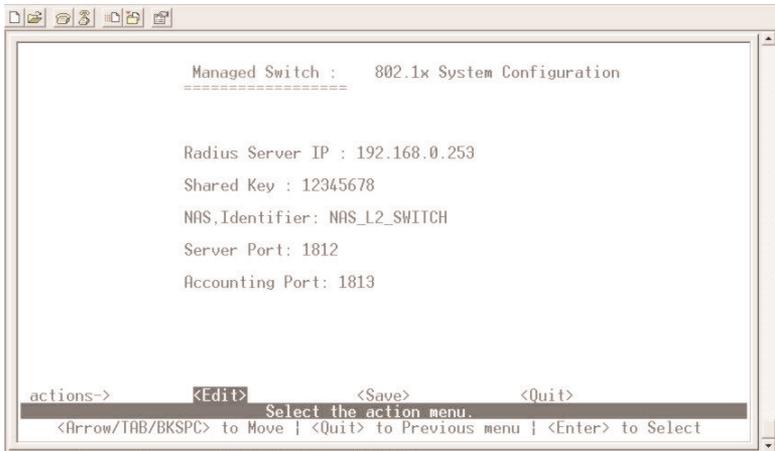


**Figure 8-63. 802.1x Enabled/Disabled Configuration screen.**

1. Use the Tab or Backspace keys to select **Edit** and then press **Enter**.
2. Press the **Space** key to choose Enabled/Disabled.
3. Press **Ctrl+A** to go back to the action menu line.
4. Use the Tab or Backspace keys to select **Save** and press **Enter** to save the configured value.

### System Configuration

To configure the system, go to Figure 8-64. To get to this page, use the Tab or Backspace keys to select **System Configuration** in Figure 8-62, then press **Enter**.



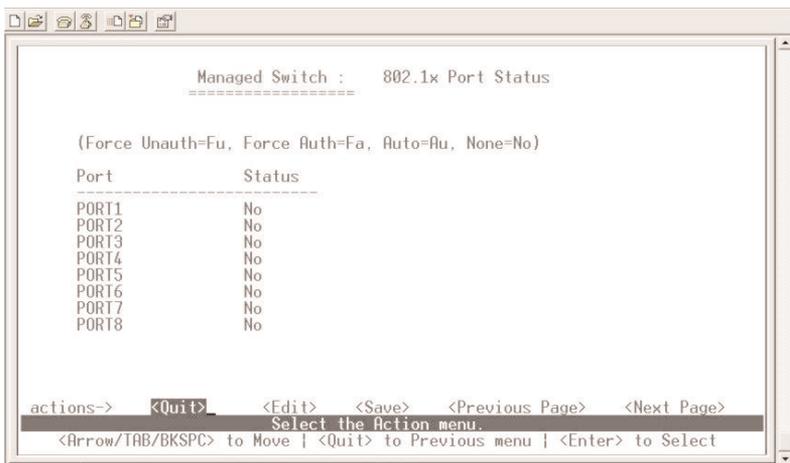
**Figure 8-64. 802.1x System Configuration screen.**

1. Use the Tab or Backspace keys to select **Edit** and then press **Enter**.
2. Radius Server IP: The IP address of the authentication server.
3. Shared Key: A key shared between the switch and authentication server.
4. NAS, Identifier: A string used to identify the switch.
5. Server Port: The UDP port number used by the authentication server to authenticate.
6. Accounting Port: The UDP port number used by the authentication server to retrieve accounting information.

7. Press **Ctrl+A** to return to the action menu line.
8. Use the Tab or Backspace keys to select **Save** and press **Enter** to save the configured value.

### *PerPort Configuration*

In this page (Figure 8-65), set the authorization status to activate the 802.1x function by port setting. To get to this page, use the Tab or Backspace keys to select Perport Configuration in Figure 8-62, then press **Enter**.

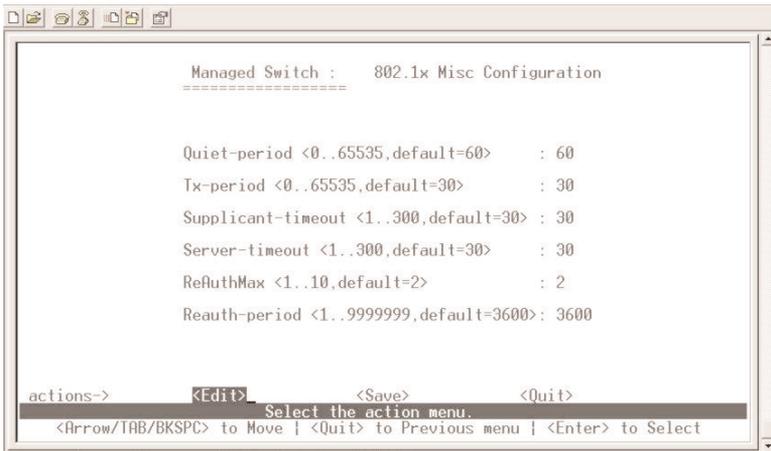


**Figure 8-65. 802.1x Port Status screen.**

1. Use the Tab or Backspace keys to select **Edit** and then press **Enter**.
2. Status: Press the **Space** key to choose Fu, Fa, Au, or No authorization status.
  - Fu: Force the specific port to be unauthorized.
  - Fa: Force the specific port to be authorized.
  - Au: The state of the specific port that was determined by the outcome of the authentication.
  - No: The specified port does not support IEEE 802.1x function.
3. Press **Ctrl+A** go back action menu line.
4. Use the Tab or Backspace keys to select **Save** and press **Enter** to save the configured value.

*Misc Configuration*

Figure 8-66 lists Misc Configuration options. To get to this screen, use the Tab or Backspace keys to select **Misc Configuration** in Figure 8-62, then press **Enter**.



**Figure 8-66. 802.1x Misc Configuration screen.**

1. Use the Tab or Backspace keys to select **Edit** and then press **Enter**.
2. Quiet Period: Used to define a period of time during which it will not attempt to acquire a supplicant (default time is 60 seconds).
3. Tx Period: Used to determine when an EAPOL PDU is to be transmitted (default value is 30 seconds).
4. Supplicant Timeout: Used to determine timeout conditions in the exchange between the supplicant and authentication server (default value is 30 seconds).
5. Server Timeout: Used to determine timeout conditions in the exchange between the authenticator and authentication server (default value is 30 seconds).
6. ReAuthMax: Used to determine the number of reauthentication attempts that are permitted before the specific port becomes unauthorized (default value is 2 times).

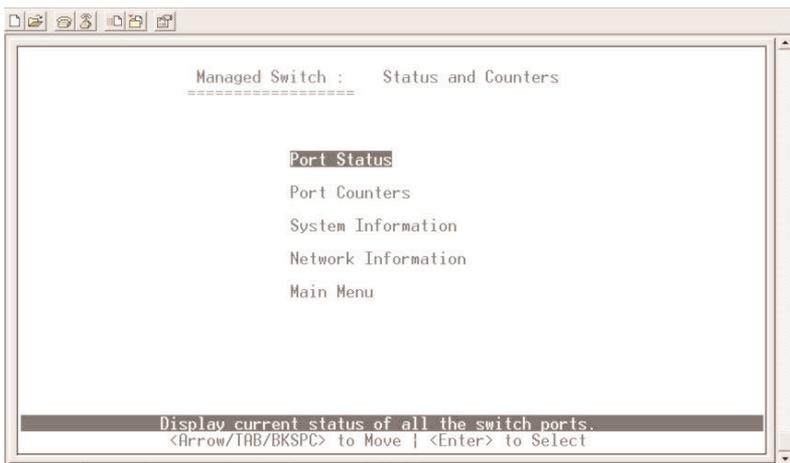
7. Reauth Period: Used to determine a nonzero number of seconds between periodic reauthentication of the supplications (default value is 3600 seconds).
8. Press **Ctrl+A** to go back to the action menu line.
9. Use the Tab or Backspace keys to select **Save** and press **Enter** to save the configured value.

### *Previous Menu*

Select this option to return to the main menu.

## 8.4 Status and Counters

Status and counters options are shown in Figure 8-67. To get to this screen, use the Tab or Backspace keys to select **Status and Counters** from the Main Menu (Figure 8-2), then press **Enter**.



**Figure 8-67. Status and Counters screen.**

Press the Tab or Backspace keys to choose an item, then press the **Enter** key to select it.

### 8.4.1 PORT STATUS

This page (Figure 8-68) displays the status of each port. To get to this page, use the Tab or Backspace keys to select **Port Status** in Figure 8-67, then press **Enter**.

Port	Link Status	InRate (100K)	OutRate (100K)	Enable	Auto	Spd/Dplx	Flow Control
PORT1	Down	0	0	Yes	AUTO	10 Half	Off
PORT2	Down	0	0	Yes	AUTO	10 Half	Off
PORT3	Down	0	0	Yes	AUTO	10 Half	Off
PORT4	Down	0	0	Yes	AUTO	10 Half	Off
PORT5	Down	0	0	Yes	AUTO	10 Half	Off
PORT6	Down	0	0	Yes	AUTO	10 Half	Off
PORT7	Down	0	0	Yes	AUTO	10 Half	Off
PORT8	Down	0	0	Yes	AUTO	10 Half	Off

actions-> <Quit> <Previous Page> <Next Page>  
 Select the action menu.  
 <Arrow/TAB/BKSPC> to Move | <Quit> to Previous menu | <Enter> to Select\_

**Figure 8-68. Port Status screen.**

**Link Status:** Displays whether the port is linked or not linked.

**InRate:** Displays the input rate control (100K/unit) setting value.

**OutRate:** Displays the output rate control (100K/unit) setting value.

**Enable:** Displays whether the port is enabled or disabled. Depending on the user's setting, a Yes or No status will be displayed respectively. If the port is not linked, its status will be treated as No.

**Auto:** Displays the port NWay link mode: Auto, NWay\_Force, Force.

**Spd/Dplx:** Displays the port speed and duplex.

**FlowCtrl:** In auto/NWay force mode, the display for the flow control status is enabled or disabled after autonegotiation.

In force mode, the display for flow control status is enabled or disabled depending on the user's setting.

**Quit:** Exit the Port Status page and return to the previous menu.

Previous Page: Display the previous page.

Next Page: Display the next page.

## 8.4.2 PORT COUNTERS

The following screen (Figure 8-69) provides a view of the current status of the unit. To get to this screen, use the Tab or Backspace keys to select **Port Counters** in Figure 8-67, then press **Enter**.

Port	TxGoodPkt	TxBadPkt	RxGoodPkt	RxBadPkt	TxAbort	Collision	DropPkt
PORT1	0	0	0	0	0	0	0
PORT2	0	0	0	0	0	0	0
PORT3	0	0	0	0	0	0	0
PORT4	0	0	0	0	0	0	0
PORT5	0	0	0	0	0	0	0
PORT6	0	0	0	0	0	0	0
PORT7	0	0	0	0	0	0	0
PORT8	0	0	0	0	0	0	0

actions-> **<Quit>** <Reset All> <Previous Page> <Next Page>  
Configure the action menu.  
<Arrow/TAB/BKSPC> to Move | <Quit> to Previous menu | <Enter> to Select

**Figure 8-69. Port Counters screen.**

Quit: Exit the Port Counters page and return to the previous menu.

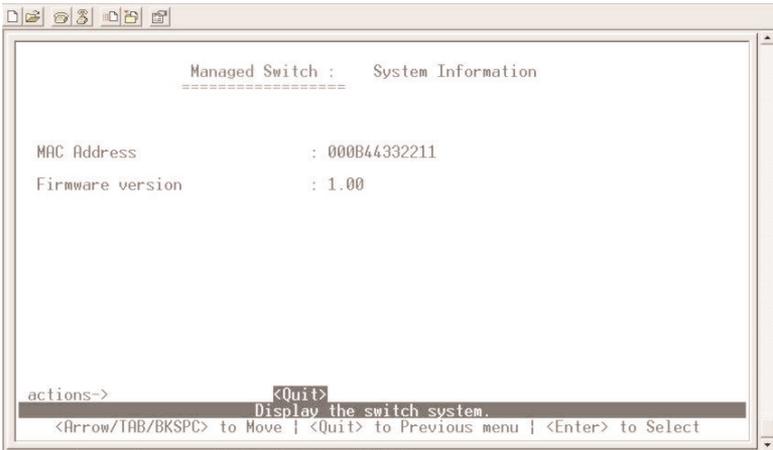
Reset All: Set all counts to 0.

Previous Page: Display the previous page.

Next Page: Display the next page.

### 8.4.3 SYSTEM INFORMATION

This screen (Figure 8-70) shows system information. To get to this screen, use the Tab or Backspace keys to select **System Information** in Figure 8-67, then press **Enter**.



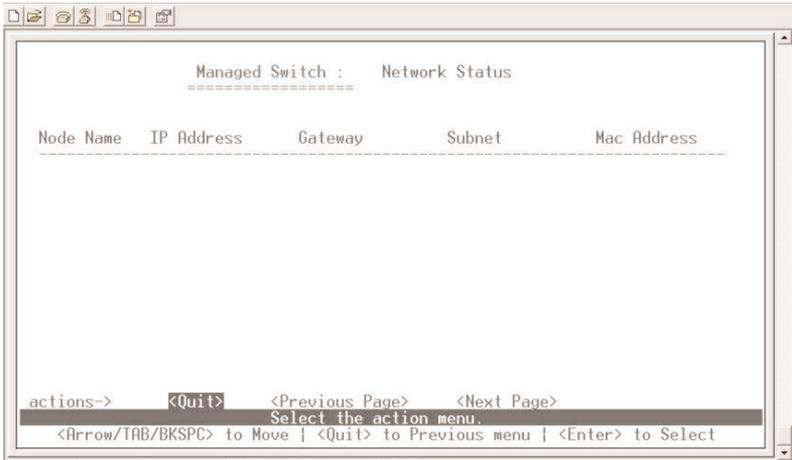
**Figure 8-70. System Information screen.**

**MAC Address:** Media Access Control—The unique hardware address assigned by the manufacturer.

**Firmware Version:** Displays the switch’s firmware version.

## 8.4.4 NETWORK INFORMATION

Display the network devices (see Figure 8-71). To get to this screen, use the Tab or Backspace keys to select **Network Information** in Figure 8-67, then press **Enter**.



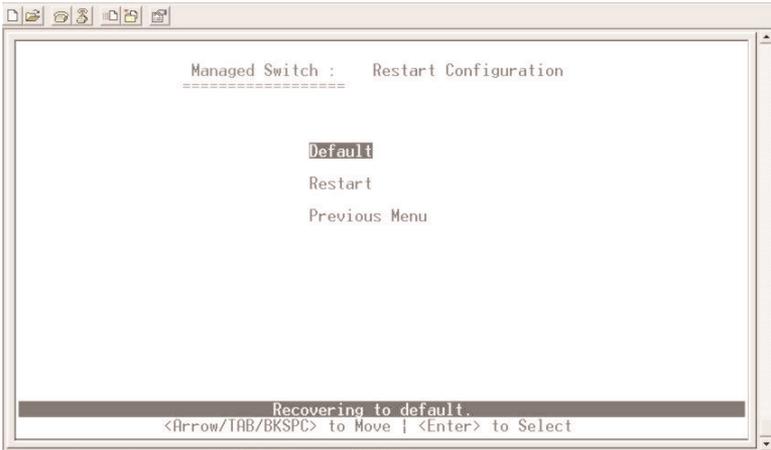
**Figure 8-71. Network Status screen.**

### *Main Menu*

Use the Tab or Backspace keys to select this option in Figure 8-67, then press **Enter** to return to the Main Menu (Figure 8-2).

## 8.5 Reboot Switch

To get to the Restart Configuration screen, use the Tab or Backspace keys to select **Reboot Switch** in the Main Menu (Figure 8-2), then press **Enter**.

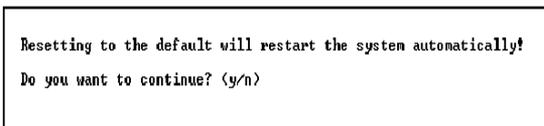


**Figure 8-72. Restart Configuration screen.**

### 8.5.1 DEFAULT

Reset the switch to the default configurations.

Press **Y** and the switch will load the default setting. After the default settings are loaded, the switch will reboot automatically.



**Figure 8-73. Reset to Default screen.**

### 8.5.2 RESTART

Reboots the switch with a software reset.

## Previous Menu

Use the Tab or Backspace keys to select this option in Figure 8-72, then press **Enter** to go back to the Main menu (Figure 8-2).

## 8.6 TFTP Update Firmware

Use this page (Figure 8-74) to update firmware, restore EEPROM value, or upload the current EEPROM value. To get to this screen, use the Tab or Backspace keys to select **TFTP Update Firmware** in Figure 8-2. Then press **Enter**.

```
Managed Switch :   TFTP Update firmware Configuration
=====
```

```
TFTP Update Firmware
TFTP Restore configuration
TFTP Backup configuration
TFTP Import TEXT Configuraton File
TFTP Export TEXT Configuration File
Previous Menu
```

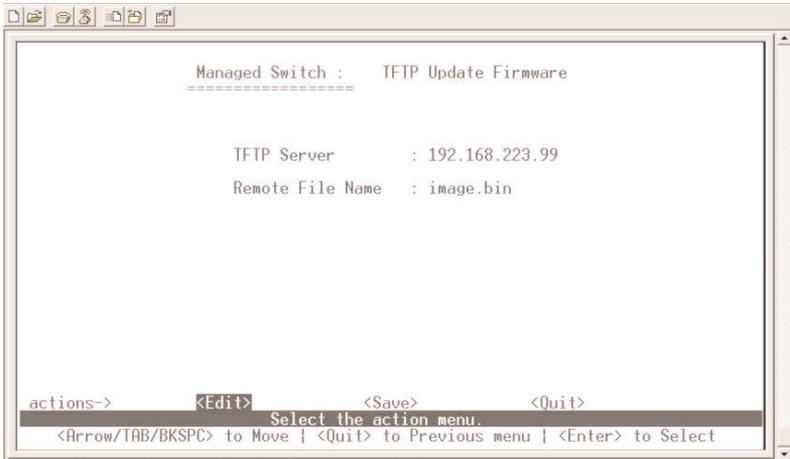
```
Use TFTP to update firmware.
<Arrow/TAB/BKSPC> to Move | <Enter> to Select
```

**Figure 8-74. TFTP Update Firmware Configuration screen.**

### 8.6.1 TFTP UPDATE FIRMWARE

Use this page (Figure 8-75) to update firmware via TFTP. To get to this screen, use the Tab or Backspace keys to select **TFTP Update Firmware** in Figure 8-74. Press **Enter**.

1. When you select **TFTP Update Firmware** and press **Enter**, Figure 8-75 appears.

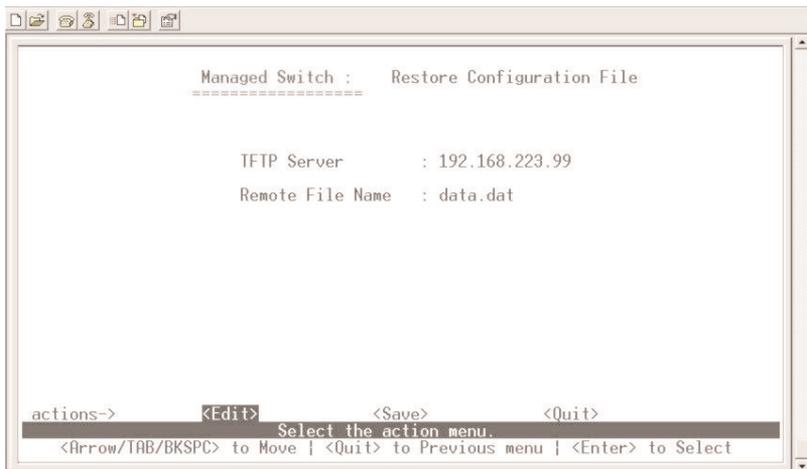


**Figure 8-75. TFTP Update Firmware screen.**

2. Use the Tab or Backspace keys to select **Edit** and then press **Enter**.
3. TFTP Server: Type the IP address of the TFTP server.
4. Remote File Name: Type the image filename.
5. Press **Ctrl+A** to go to the action line.
6. Select **Save**, and the switch will start to download the image file.
7. When the update is successful, the image file will be downloaded.
8. Restart the switch to launch the new version of firmware.

## 8.6.2 TFTP RESTORE CONFIGURATION

Use this page (Figure 8-76) to restore the EEPROM value from a saved image file in a TFTP server. To get to this screen, use the Tab or Backspace keys to select **TFTP Restore Configuration** in Figure 8-74. Press **Enter**.

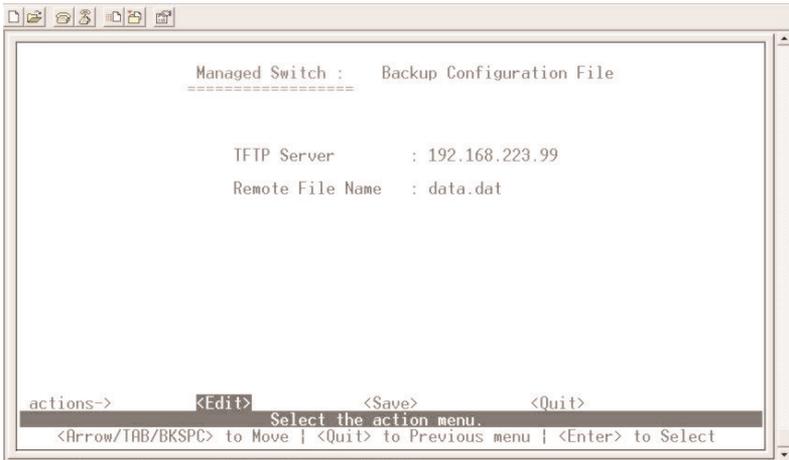


**Figure 8-76. Restore Configuration File screen.**

1. Start the TFTP server.
2. Use the Tab or Backspace keys to select **Edit** and then press **Enter**.
3. TFTP Server: Type the TFTP server's IP address.
4. Remote File Name: Type the image file name.
5. Press **Ctrl+A** to go to the action line.
6. Select **Save**. The switch will start to download the image file.
7. When the restore function is successful, the image is downloaded.
8. Restart the switch to resume normal operations.

### 8.6.3 TFTP BACKUP CONFIGURATION

Use this page (Figure 8-77) to save the current EEPROM value to an image file. To get to this page, use the Tab or Backspace keys to select **TFTP Backup Configuration** in Figure 8-74. Press **Enter**.



**Figure 8-77. Backup Configuration File screen.**

1. Start the TFTP server.
2. Use the Tab or Backspace keys to select **Edit** and then press **Enter**.
3. TFTP Server: Type the TFTP server's IP address.
4. Remote File Name: Type the image file name.
5. Press **Ctrl+A** to go to the action line.
6. Select **Save**. The switch will start to save the image file.
7. When the backup function is successful, the image file is saved to the designated TFTP server.
8. Follow the instructions given in the Restore Configure File screen (Figure 8-76) to restore lost settings.

## 8.6.4 TFTP IMPORT TEXT CONFIGURATION FILE

Use this page (Figure 8-78) to restore EEPROM value from a saved text file in a TFTP server. To get to this screen, use the Tab or Backspace keys to select **TFTP Import Text Configuration File** in Figure 8-74. Press **Enter**.

```
Managed Switch : TFTP Import TEXT Configuraton File
=====
TFTP Server      : 192.168.223.99
Remote File Name : config.txt
```

```
actions->      <Edit>          <Save>          <Quit>
                Select the action menu.
<Arrow/TAB/BKSPC> to Move | <Quit> to Previous menu | <Enter> to Select
```

**Figure 8-78. TFTP Import Text Configuration File screen.**

1. Start the TFTP server.
2. Use the Tab or Backspace keys to select **Edit** and then press **Enter**.
3. TFTP Server: Type the TFTP server's IP address.
4. Remote File Name: Type the text file name.
5. Press **Ctrl+A** to go to the action line.
6. Select **Save**. The switch will start to download the text file.
7. When the restore function is successful, the image is downloaded. If there is an error, you can view the error information in the Report.txt file located in your TFTP server. It's a good idea to always view the Report.txt to make sure that your restore was good, even if you don't suspect an error. In some cases, a non-fatal error might cause only partial configuration settings.
8. Restart the switch to resume normal operations.

### 8.6.5 TFTP EXPORT TEXT CONFIGURATION FILE

Use this page (Figure 8-79) to save the current EEPROM value to a text file. To get to this screen, use the Tab or Backspace keys to select **TFTP Export Text Configuration File** in Figure 8-74. Then press **Enter**.

```
Managed Switch :   TFTP Export TEXT Configuration File
=====

TFTP Server      : 192.168.223.99
Remote File Name : config.txt
```

```
actions->      <Edit>          <Save>          <Quit>
Select the action menu.
<Arrow/TAB/BKSPC> to Move | <Quit> to Previous menu | <Enter> to Select
```

**Figure 8-79. TFTP Export Text Configuration File screen.**

1. Start the TFTP server.
2. Use the Tab or Backspace keys to select **Edit** and then press **Enter**.
3. TFTP Server: Type the TFTP server's IP address.
4. Remote File Name: Type the image file name.
5. Press **Ctrl+A** to go to the action line.
6. Select **Save**. The switch will start to save the image file.
7. When the Export function is successful, the image file is saved to the designated TFTP server.
8. Follow the instructions given in the TFTP Import Text Configuration File screen (**Section 8.6.4**) to restore settings.

#### *Previous Menu*

Use the Tab or Backspace keys to select this option in Figure 8-74, then press **Enter** to go back to the Main menu (Figure 8-2).

### 8.7 Logout

Use the Tab or Backspace keys to select this option to log out of the console line interface program.

## 9. Menu-Driven Interface via Telnet

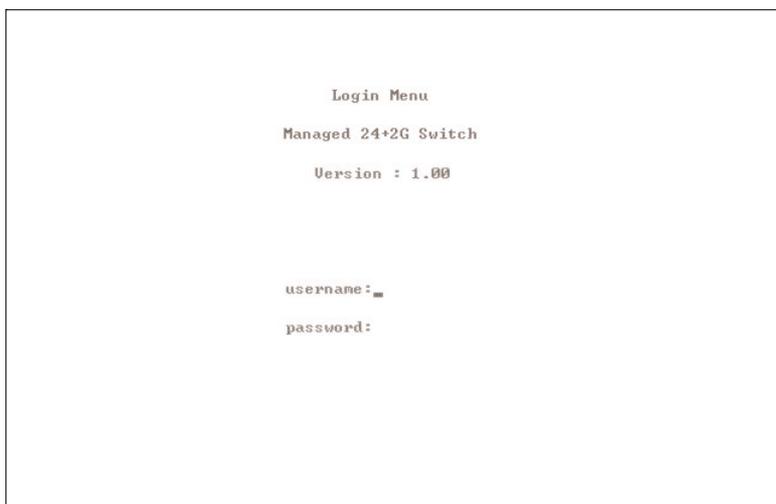
This section provides some basic instructions for using a menu-driven interface to configure the switch. Follow the instructions below.

1. Open a Command Prompt window and type:

```
telnet xxx.xxx.xxx.xxx
```

where the *xxx* represents the IP address.

2. Press the **Enter** key to start. Figure 9-1 appears.



**Figure 9-1. Login menu.**

3. The default Login name is `admin`, with a null password (just press Enter in the password field). The system provides a menu-driven user interface via console or Telnet. After you log into the system, you will see a window similar to the Main menu shown in **Chapter 8**.

To use the switch's management functions via Telnet, refer to **Chapter 6**.

# 10. Troubleshooting

## 10.1 Symptoms/Causes/Solutions

The network administrator can observe and monitor the switch's status using the front-panel LED indicators to quickly identify problems. This section contains a few of the more common problems that may arise and possible solutions.

**Symptom:** The Power LED does not light after power on.

**Cause:** The power outlet, power cord, or internal power supply is defective.

**Solution:** Verify that the power outlet is functioning normally by plugging in another properly operating device. Connect the power cord to another device to test. If these two tests fail to resolve the problem, replace the power supply unit.

**Symptom:** The Link LED does not light after making a connection.

**Cause:** The network cable or fiber switch port is defective.

**Solution:** Make sure that the attached device and the switch are powered on. Verify that the fiber cable has been properly connected to both devices. Confirm that the cable distance does not exceed specified limits. Inspect the cable for defects, and replace it if necessary.

**Symptom:** The switch powers off during operation after a period of time.

**Cause:** Loose power connections, power surges/loss, or inadequate ventilation may be present.

**Solution:** Make sure that all power connections are secure and that the switch's fans have proper ventilation. If you are unable to correct the problem, you might have to replace the internal power supply unit.

## **10.2 Calling Black Box**

If you determine that your 24-Port 10/100 Managed Switch with Gigabit Uplink Port is malfunctioning, do not attempt to alter or repair the unit. It contains no user-serviceable parts. Contact Black Box at 724-746-5500.

Before you do, make a record of the history of the problem. We will be able to provide more efficient and accurate assistance if you have a complete description, including:

- the nature and duration of the problem.
- when the problem occurs.
- the components involved in the problem.
- any particular application that, when used, appears to create the problem or make it worse.

## **10.3 Shipping and Packaging**

If you need to transport or ship your 24-Port 10/100 Managed Switch with Gigabit Uplink Port:

- Package it carefully. We recommend that you use the original container.
- If you are shipping the 24-Port 10/100 Managed Switch with Gigabit Uplink Port for repair, make sure you include everything that came in the original package. Before you ship, contact Black Box to get a Return Authorization (RA) number.