WGS3-2620

24+2G Layer 3 Fast/Gigabit Ethernet Switch

User's Manual

Information furnished is believed to be accurate and reliable. However, no responsibility is assumed by for its use, nor for any infringements of patents or other rights of third parties, which may result from its use. No license is granted by implication or otherwise under any patent or patent rights. Right reserved to change specifications at any time without notice.

FCC Compliance Statement

This equipment generates and uses radio frequency energy and if not installed and used properly, that is, in strict accordance with the instructions provided with the equipment, may cause interference to radio and TV communication. The equipment 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 in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. If you suspect this equipment is causing interference, turn your Ethernet Switch on and off while your radio or TV is showing interference, if the interference disappears when you turn your Ethernet Switch off and reappears when you turn it back on, there is interference being caused by the Ethernet Switch.

You can try to correct the interference by one or more of the following measures:

1. Reorient the receiving radio or TV antenna where this may be done safely.
2. To the extent possible, relocate the radio, TV or other receiver away from the Switch.
3. Plug the Ethernet Switch into a different power outlet so that the Switch and the receiver are on different branch circuits.

If necessary, you should consult the place of purchase or an experienced radio/television technician for additional suggestions.

Caution: Do not use a RJ-11 (telephone) cable to connect your network equipment.

Important Safety Instructions

1. Read all of these instructions.
2. Save these instructions for later use.
3. Follow all warnings and instructions marked on the product.
4. Unplug this product from the wall outlet before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning.
5. Do not use this product near water.
6. Do not place this product on an unstable cart or stand. The product may fall, causing serious damage to the product.
7. The air vent should never be blocked by placing the product on a bed, sofa, rug, or other similar surface. This product should never be placed near or over a radiator or heat register. This product should not be placed in a built-in installation unless proper ventilation is provided.
8. This product should be operated from the type of power source indicated on the marking label. If you are not sure of the type of power

available, consult your dealer or local power company.

9. This product is equipped with a three-wire grounding type plug, a plug having a third (grounding) pin. This plug will only fit into a grounding type power outlet. This is a safety feature. If you are unable to insert the plug into the outlet, contact your electrician to replace your outlet. Do not defeat the purpose of the grounding type plug.
10. Do not allow anything to rest on the power cord. Do not place this product where persons will walk on the cord.
11. If an extension cord is used with this product, make sure that the total ampere ratings on the products into the extension cord do not exceed the extension cord ampere rating. Also make sure that the total of all products plugged into the wall outlet does not exceed 15 amperes.
12. Never push objects of any kind into this product through air ventilation slots as they may touch dangerous voltage points or short out parts that could result in a risk of fire or electric shock. Never spill liquid of any kind on the product.
13. Do not attempt to service this product yourself, as opening or removing covers may expose you to dangerous voltage points or other risks. Refer all servicing to service personnel.

Warnings

1. *Wear an anti-static wrist strap or take other suitable measures to prevent electrostatic discharge whenever handling this equipment.*
2. *When connecting to a power outlet, connect the field ground lead on the triple power plug to a valid earth ground line to prevent electrical hazards.*

CE Mark Warning

In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Disclaimer

The publisher assumes no responsibility for errors that may appear in this document, nor does it make any commitment to update information it contains.

All brands and product names mentioned are trademarks or registered trademarks of their respective companies.

Trademarks

PLANET is a registered trademark of PLANET Technology Corp. All other trademarks belong to their respective owners.

Contents subject to revision without prior notice.

Revision

User's manual for PLANET 24+2G Layer 3 Fast/Gigabit Ethernet Switch
Model: WGS3-2620
Rev: 1.0 (November. 2001)
Part No. EMQ-WG26V1

TABLE OF CONTENTS

Chapter 1. Introduction

The WGS3-2620 is a 26-port, IP-based Layer 3 Ethernet Switch with 24-port 10/100Mbps and 2-port 1000Mbps copper interface.

The two RJ-45 copper ports support 1000Mbps auto-MDI detection that can directly connect to any Gigabit Ethernet Servers, Switches, L3 backbone with a straight Category 5/5e, 8-wire UTP cable. The 24-port 10/100Mbps are for L2/L3 network connection.

The wire-speed switch engine provides up to 8.53Gbps switch fabric for L2 and L3 IP routing capability. Up to 256 IP subnet / L2 tagged VLAN are also available to segment the IP or MAC-based networks. IEEE802.1D Spanning Tree, bridging, Port mirroring and IEEE802.3ad port-trunk also support for optimal LAN connection and diagnose. IGMP snooping, filtering, dual priority helps to build a multimedia networks like video-conference etc.

Designed to offer the guaranteed IP Layer 3 routing, the WGS3-2620 empower the performance of pure IP-based network easier then ever.

Features

- ♦ 2-port 1000Mbps, 24-port 10/100Mbps Ethernet Switch
- ♦ Complies with IEEE802.3, 10Base-T, IEEE802.3u, 100Base-TX and IEEE802.3ab, 1000Base-T standards
- ♦ IEEE802.3x, full-duplex flow control compliant; back-pressure half-duplex flow control
- ♦ IEEE802.1p, dual priority; IEEE802.1Q, VLAN Tagging; IEEE802.1D Bridging compliant
- ♦ 32K MAC address table auto-ageing / 64K IP address at most
- ♦ IPv4 Layer 3 routing, supporting RIP-1/2, DVMRP (Distance-Vector Multicast Routing Protocol)
- ♦ 8.53G non-blocking, Store and Forward switching architecture
- ♦ RS-232 console interface for console program managements, Web / Telnet Support
- ♦ IEEE802.3ad link aggregation, port-based Trunking support increase the bandwidth between switches (2/4/8-port in one trunk)
- ♦ 256 port-based VLANs eliminate the broadcast-packet, increase the LAN security for different segments
- ♦ IGMP multicast snooping and filtering
- ♦ Port mirroring for port traffic diagnose with sniffer programs
- ♦ RMON group 1, 2, 3, 9 support
- ♦ 19”, 1U height rack mounting
- ♦ 100~240VAC, 50~60Hz universal Power input
- ♦ FCC, CE class A compliant

Specification

HARDWARE SPECIFICATIONS	
Product	IP Layer 3 10/100/1000Mbps Routing Switch
Model	WGS3-2620
Ports	24-port 10/100Base-TX, RJ-45 Interface 2-port 1000Base-T RJ-45 Interface
Speed per port	Port 1~24: 10/100Mbps, Auto-negotiation, Auto-MDI Port 25, 26: 1000Mbps, Auto-negotiation, Auto-MDI
LED Indicators	Port 1 ~24: Two per port; Link, Mode (Modes include FDX, ACT, Speed) Port 25, 26: Two per port; Link FDX
Rack Mount	1.U, 19" Rack mount
Dimensions	430 mm x 334 mm x 44 mm (W x D x H)
SWITCHING SPECIFICATIONS	
Architecture	High Performance Store & Forward Switching Architecture
Memory	4MB
Switching fabric	8.53Gbps
MAC address Table	Layer 2: 32K MAC-entry Layer 3:64K IP- entry
Forwarding/filtering rate	Layer 2 wired speed forwarding Layer 3 wired speed forwarding
Error Checking	Runt & CRC on all network packets
Media Type	RJ-45 STP, Port 25, 26 MDI Auto-detect
Network Management	IEEE802.1D Spanning Tree Protocol IEEE802.1Q VLAN, up to 256 VLANs IEEE802.p dual Priority IEEE802.1ad Link Aggregation IEEE802.3x Flow control RFC 1757 RMON, Group 1, 2, 3, 9 RFC 2236 IGMP (Internet Group Management Protocol) SNMP MIB II, RFC 1213, RFC 1516 Port Mirroring, Static MAC, Static IP, MAC filtering, IP filtering
Environment Specification	
Cabling	100Mbps: Category 5 UTP, 4-wire 1000Mbps: Category 5/5e or above, 8-wire
Protocol Compatibility	Layer 2: Transparent to higher layer protocols Layer 3: IP RIP-1, RIP-2, DVMRP
Power Consumption	65 watts / 220 BTU
AC Power	100~240V AC, 50/60Hz auto-sensing
Temperature	0~40 degree C operating
Humidity	10~90% non-condensing
Emission	FCC Class A, CE mark

Chapter 2. Installing the Switch

Before installing the switch, verify that you have all the items listed under "Package Contents." Also be sure you have all the necessary tools and cabling before installing the switch. Note that this switch can be installed on any suitably large flat surface or in a standard EIA 19-inch rack. After installing the switch, refer to the following chapter to set up its more advanced features, such as Spanning Tree Protocol or VLAN port groups.

2.1 Package Contents

This package includes:

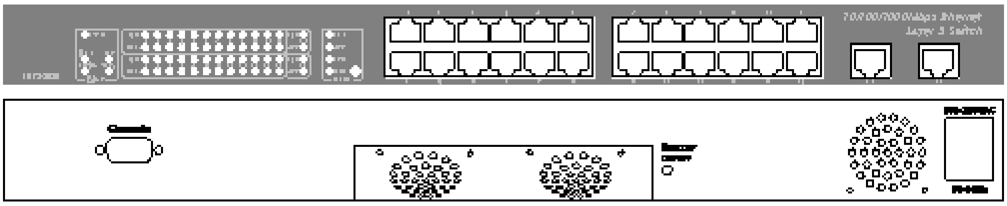
- WGSW-2620
- Quick Installation Guide
- Rack mount bracket kit
- AC power cord
- This Manual CD
- Console cable

2.2 Description of Hardware

The base unit contains 24 10BASE-T/100BASE-TX and 2 1000BASE-T ports. All the 24 10/100M RJ-45 ports operate at 10 or 100 Mbps, and support auto-negotiation of speed, duplex mode (i.e., half or full duplex), and flow control. While the 1000BASE-T module operates at 1Gbps, and supports auto-negotiation or Full duplex mode and flow control. Note that when using auto-negotiation, speed, transmission mode, or flow control can be automatically set if this feature is also supported by the attached device. Otherwise, these items can be manually configured for any connection.

The unit also includes a display panel for key system and port indications that simplify installation and network troubleshooting.

The following figures show the components of this switch system:



2.3 Mounting the Switch

This switch can be placed directly on your desktop, or mounted in a rack. Before you start installing the switch, make sure you can provide the right operating environment, including power requirements, sufficient physical space, and proximity to other network devices that are to be connected. Verify the following installation requirements:

- Power requirements: 100 to 240 V AC (+/-10%) at 50 to 60 Hz (+/-3Hz). The switch's power supply automatically adjusts to the input voltage level.
- The switch should be located in a cool dry place, with at least 10 cm. (4 in.) of space on the sides for ventilation.
- Place the switch out of direct sunlight, and away from heat sources or areas with a high amount of electromagnetic interference.
- If you intend to mount the switch in a rack, make sure you have all the necessary mounting screws, brackets, bolts and nuts, and the right tools.
- Check if network cables and connectors needed for installation are available.

2.3.1 Mounting Switches in a Rack

Please comply with the following instructions to ensure that your switch is securely mounted in the rack.

1. Use a standard EIA 19-inch rack.
2. Use the brackets and screws supplied in the rack mounting kit.
3. Use a cross-head screwdriver to attach the brackets to the side of the switch.
4. Position the switch in the rack by lining up the holes in the brackets with the appropriate holes on the rack, and then use the supplied screws to mount the switch in the rack.

2.4 Connecting the Switch System

The Switch provides 26 RJ-45 ports. The transmission speed for each port is automatically set by the switch to match the highest speed supported by the connected device. The transmission mode can be set for each port using auto-negotiation (if also supported by the attached device). However, if the device attached to any port on the switch does not support auto-negotiation, you can manually configure the transmission mode via the console port on the rear panel, or via an in-band connection (including Telnet, the Web agent).

2.4.1 Making a Connection to an RJ-45 Port

The RJ-45 ports support Auto-MDI. You can use straight-through or crossover twisted-pair cable to connect any RJ-45 port on the switch to any device that uses a standard network interface such as a workstation or server, or to a network interconnection device such as a bridge or router.

1. Prepare the network devices you wish to network. Make sure you have installed 10BASE-T, 100BASE-TX or 1000BASE-T network interface cards for connecting to the switch's RJ-45 ports.
2. Prepare straight-through shielded or unshielded twisted-pair cables with RJ-45 plugs at both ends. Use 100-ohm Category 3, 4 or 5 cable for standard 10Mbps Ethernet connections, 100-ohm Category 5 cable for 100Mbps Fast Ethernet connections, or Category 5e cable for 1000Mbps Gigabit Ethernet connections.
3. Connect one end of the cable to the RJ-45 port of the network interface card, and the other end to any available RJ-45 port on the switch. When inserting an RJ-45 plug, be sure the tab on the plug clicks into position to ensure that it is properly seated. Using the switch in a stand-alone configuration, you can network up to 26 end nodes

Do not plug a phone jack connector into any RJ-45 port. This may damage the switch. Instead, use only twisted-pair cables with RJ-45 connectors that conform with FCC standards.

NOTES: 1. Make sure each twisted-pair cable does not exceed 100 meters (328 feet).

2. We advise using Category 5e cable for all network connections to avoid any confusion or inconvenience in the future when you upgrade attached devices to Gigabit Ethernet.

Restrictions on Cascade Length - The IEEE 802.3 standard recommends restricting the number of hubs (i.e., repeaters) cascaded via twisted-pair cable to 4; while IEEE 802.3u provides even stricter recommendations for Fast Ethernet. Therefore, when cascading devices other than this switch, please refer to the accompanying documentation for cascade restrictions. However, note that because switches break up the path for connected devices into separate collision domains, you should not include the switch or connected cabling in your calculations for cascade length involving other devices.

2.5 Powering On the Switch

1. Plug the power cord into the power socket on the rear of the switch, and the other end into a power outlet.
2. Check the LED marked PWR on the front panel to see if it is on. The unit will automatically select the setting that matches the connected input voltage. Therefore, no additional adjustments are necessary when connecting it to any input voltage within the range marked on the rear panel.

3. The switch performs a self-diagnostic test upon power-on. (Note that this test takes about one minute to complete.)

NOTES: The unit supports a "hot remove" feature which permits you to connect or disconnect twisted-pair or fiber cables without powering off the switch and without disrupting the operation of the devices attached to the switch. However, due to the spanning tree learning process, the new attached device may takes about 30 seconds to be able to connect the other devices. This period can be shortened by adjusting the spanning tree configuration.

2.6 Verifying Port Status

Check each connection by viewing the port indicators shown in the following table.

LED	State	Indication
System		
Power	On	Switch is receiving power.
SNMP	On	SNMP agent operational.
Console	On	RS-232 Console interface is operating
Fan*1	On	One of the fans is failed and standby fan is running
Temp*2	On	The internal temperature is equal to or higher than 60 degree C
10BaseT/100BaseTX Ports		
LNK	On	Port has established a valid network connection
Mode*3		
COL	On	Collision occurs on the port
ACT	On	Traffic is passing through the port
FDX	On	Been set to full duplex
100M	On	Connected on 100M speed

1000BaseT Ports		
LNK	On	Port has established a valid network connection
ACT	On	Traffic is passing through the port
*1 There are two 4-inch fans and one 2-inch fan in the unit. Normally, one of the 4-inch fans and 2-inch fan is running. Another 4-inch fan is standby and not working. Once one of the two running fans is failed, the standby fan will be drove to run and the Fan LED will light on. *2 When the internal temperature is equal to or higher than 60 degree C, the standby fan will be drove to run and the Temp LED will light on. Once the temperature is equal to or higher than 70 degree C, the buzzer will sound. You can press the buzzer On/Off button to turn off the buzzer. *3 Use the Mode button to select LED display mode.		

2.7 Verifying System Operation

Verify that all attached devices have a valid connection. The switch monitors the link status for each port. If any device is properly connected to the switch and transmitting a link beat signal, the Link indicator will light up for the corresponding port. If the Link indicator fails to light when you connect a device to the switch, check the following items:

- Be sure all network cables and connectors are properly attached to the connected device and the switch.
- See if your cable is functioning properly by using it for another port and attached device that displays valid indications when connected to the network.
- Be sure no twisted-pair cable exceeds 100 meters (328 feet).

Chapter 3. Switch Management

3.1 Configuration Options

For advanced management capability, the on-board management agent provides a menu-driven system configuration program. This program can be accessed by a direct or modem connection to the serial port on the rear panel (out-of-band), or by a Telnet connection over the network (in-band).

The management agent is based on SNMP (Simple Network Management Protocol). This SNMP agent permits the switch to be managed from any PC in the network using in-band management software.

The management agent also includes an embedded HTTP Web agent. This Web agent can be accessed using Microsoft Internet Explorer 4.0 or later from any computer attached to the network.

The system configuration program and the SNMP agent support management functions such as:

- Enable/disable any port
- Set the communication mode for any port
- Configure SNMP parameters
- Add ports to network VLANs
- Configure IP routing and multicast VLANs
- Display system information or statistics
- Configure the switch to join a Spanning Tree
- Download system firmware

3.2 Required Connections

3.2.1Console Port (Out-of-Band) Connections

Attach a VT100 compatible terminal or a PC running a terminal emulation program to the serial port on the switch's rear panel. Use the null -modem cable provided with this package, or use a null modem connection that complies with the wiring assignments shown in Appendix B of this guide.

When attaching to a PC, set terminal emulation type to VT100, specify the port used by your PC (i.e., COM 1~4), and then set communications to 8 data bits, 1 stop bit, no parity, and 19200 bps (for initial configuration). Also be sure to set flow control to "none." (Refer to "Configuring the Serial Port" for a complete description of configuration options.)

Note: If the default settings for the management agent's serial port have been modified and you are having difficulty making a console connection, you can display or modify the current settings using a Web browser as described under "Configuring the Serial Port".

3.2.2 Remote Management via the Console Port

3.2.2.1 Configuring the Switch Site

Connect the switch’ s DB9 serial port to the modem’ s serial port using standard cabling. For most modems which use a 25-pin port, you will have to provide an RS232 cable with a 9-pin connector on one end and a 25-pin connector on the other end. Set the modem at the switch’ s site to force auto-answer mode. The following is a sample initialization string: “ATQ1S0=1&D0&K0&W” as defined below:

Q1 : Inhibit result codes to DTE
S0=1 : Auto answer on first ring
D0 : Don’ t care DTR
K0 : Disables DTE/DCE flow control
W : Write command to modem memory

3.2.2.2 Configuring the Remote Site

At the remote site, connect the PC’ s COM port (COM 1~4) to the modem’ s serial port. Set terminal emulation type to VT100, specify the port used by your PC (i.e., COM 1~4), and then set communications to 8 data bits, 1 stop bit, no parity, 19200 bps, and no flow control.

3.2.3 In-Band Connections

Prior to accessing the switch’ s on -board agent via a network connection, you must first configure it with a valid IP address, subnet mask, and default gateway (for Layer 2 mode) using an out-of-band connection or the BOOTP protocol.

After configuring the switch’ s IP parameters, you can access the on -board configuration program from anywhere within the attached network. The on-board configuration program can be accessed using Telnet from any computer attached to the network. The switch can also be managed by any computer using a Web browser (Internet Explorer 4.0 or above, or Netscape Navigator 4.0 or above), or from a network computer using network management software.

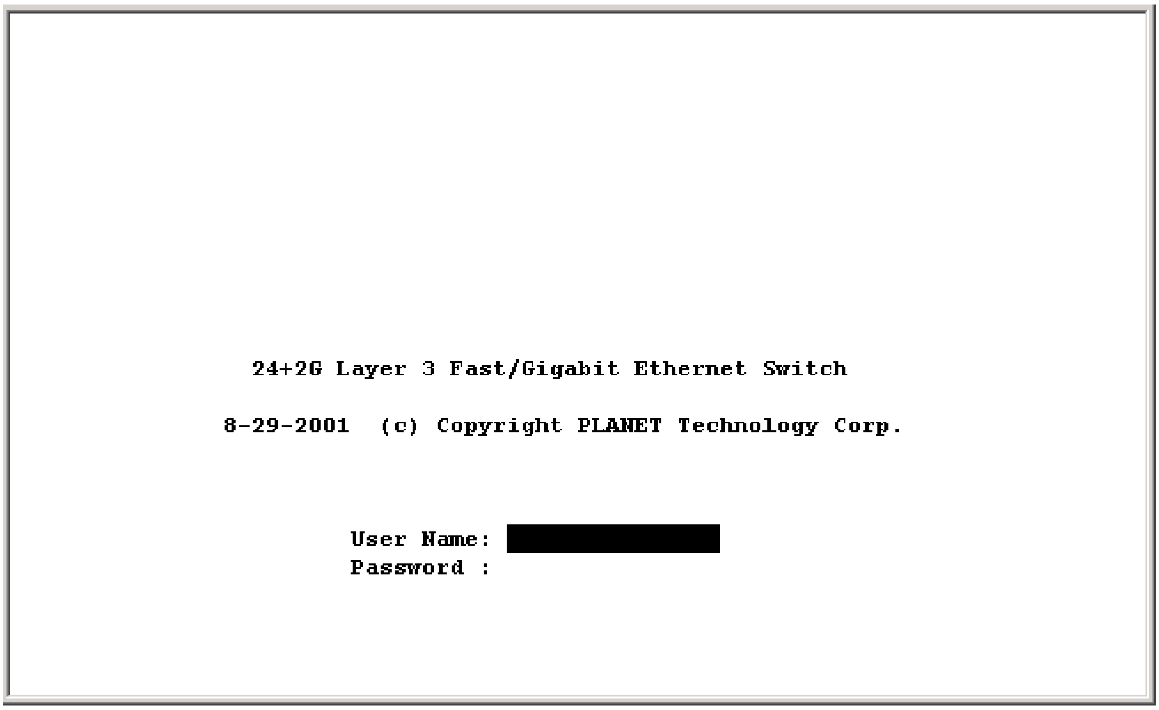
Notes:

1. By default BOOTP is disabled. To enable BOOTP, see “IP Configuration (Layer 2 Mode)”.
2. Each VLAN group can be assigned its own IP interface address. Therefore, if the port connected to the management station has joined several VLANs, you can manage the switch via any of these IP addresses.
3. This switch supports four concurrent Telnet sessions.
4. The on-board program only provides access to basic configuration functions. To access the full range of SNMP management functions, you must use SNMP- based network management software.

Chapter 4. Console Interface

4.1 Login Screen

Once a direct connection to the serial port or a Telnet connection is established, the login screen for the on-board configuration program appears as shown below.



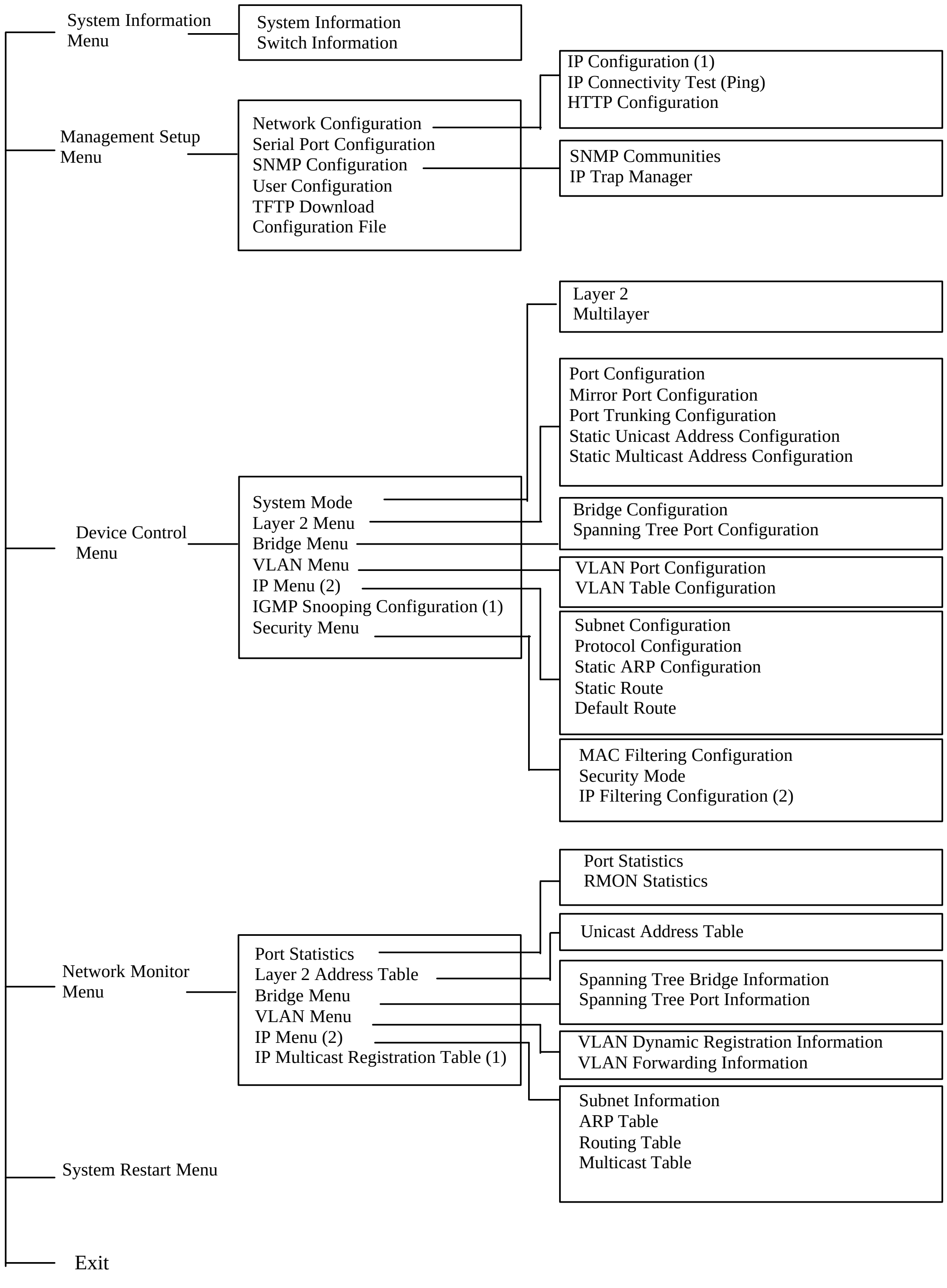
```
                24+2G Layer 3 Fast/Gigabit Ethernet Switch

              8-29-2001  (c) Copyright PLANET Technology Corp.


                         User Name:
                         Password :
```

If this is your first time to log into the configuration program, then the default user names are “admin” with no password. The administrator has Read/Write access to all configuration parameters and statistics.

You should define a new administrator password, record it and put it in a safe place. Select User Configuration from the Management Setup Menu and enter a new password for the administrator. Note that passwords can consist of up to 15 alphanumeric characters and are not case sensitive.

Note: You are allowed three attempts to enter the correct password; on the third failed attempt the current connection is terminated.

After you enter the user name and password, you will have access to the system configuration program illustrated by the following menu map:

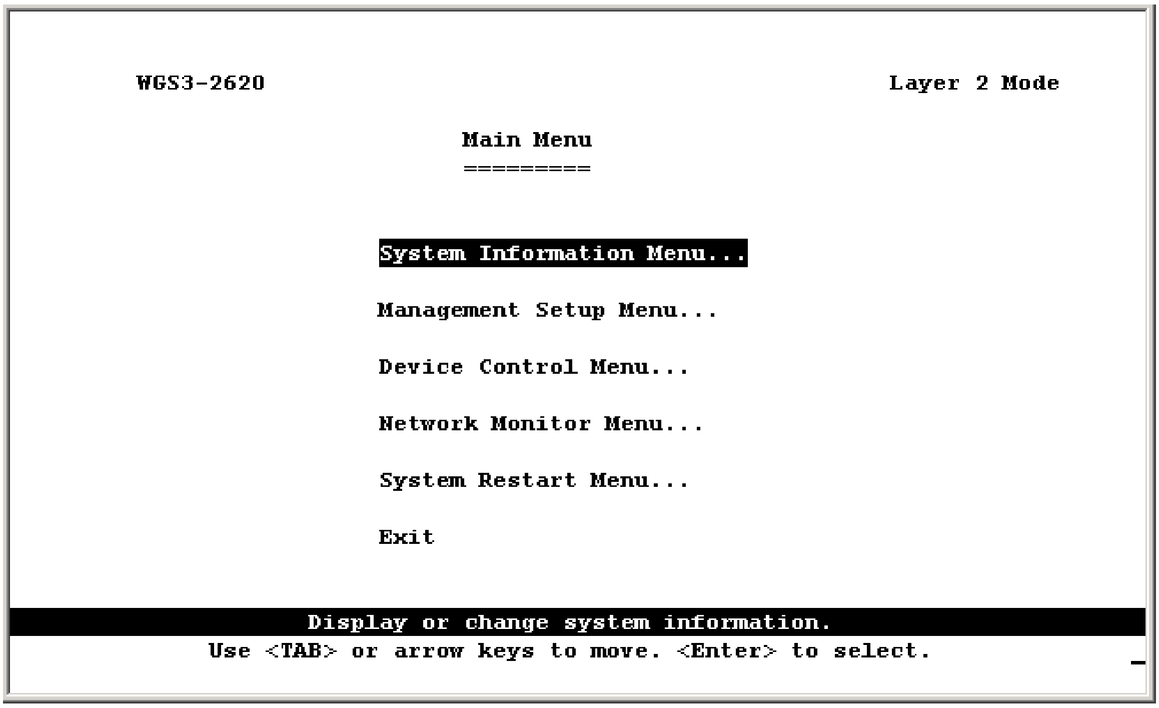


1.Displayed for layer 2 mode only.
2.Displayed for multilayer mode

4.2 Main Menu

With the system configuration program you can define system parameters, manage and control the switch and all its ports, or monitor network conditions. The figure below of the Main Menu and the following table briefly describe the selections available from this program.

Note: Options for the currently selected item are displayed in the highlighted area at the bottom of the interface screen.



```
        WGS3-2620                                          Layer 2 Mode

                              Main Menu
                              =========

                         System Information Menu...

                         Management Setup Menu...

                         Device Control Menu...

                         Network Monitor Menu...

                         System Restart Menu...

                         Exit

                  Display or change system information.
            Use <TAB> or arrow keys to move. <Enter> to select.
```

Menu	Description
(Operation Mode)	The text string in the top right corner of the screen shows if the switch is operating as a Layer 2 switch or as a multilayer routing switch.
System Information Menu	
System Information	Provides basic system description, including contact information.
Switch Information	Shows hardware/firmware version numbers, power status, and expansion modules used in the switch.
Management Setup Menu	
Network Configuration	Includes IP Configuration ^{*1}, Ping facility, and HTTP (Web agent) setup.
Serial Port Configuration	Sets communication parameters for the serial port, including baud rate, console time-out, and screen data refresh interval.
SNMP Configuration	Activates authentication failure traps; and configures community access strings, and trap managers.
User Configuration	Sets the user names and passwords for system access.
TFTP Download	Downloads new version of firmware to update your system (in-band).
Configuration File	Download the VLAN and routing configuration to a file or upload the configuration file to the switch.

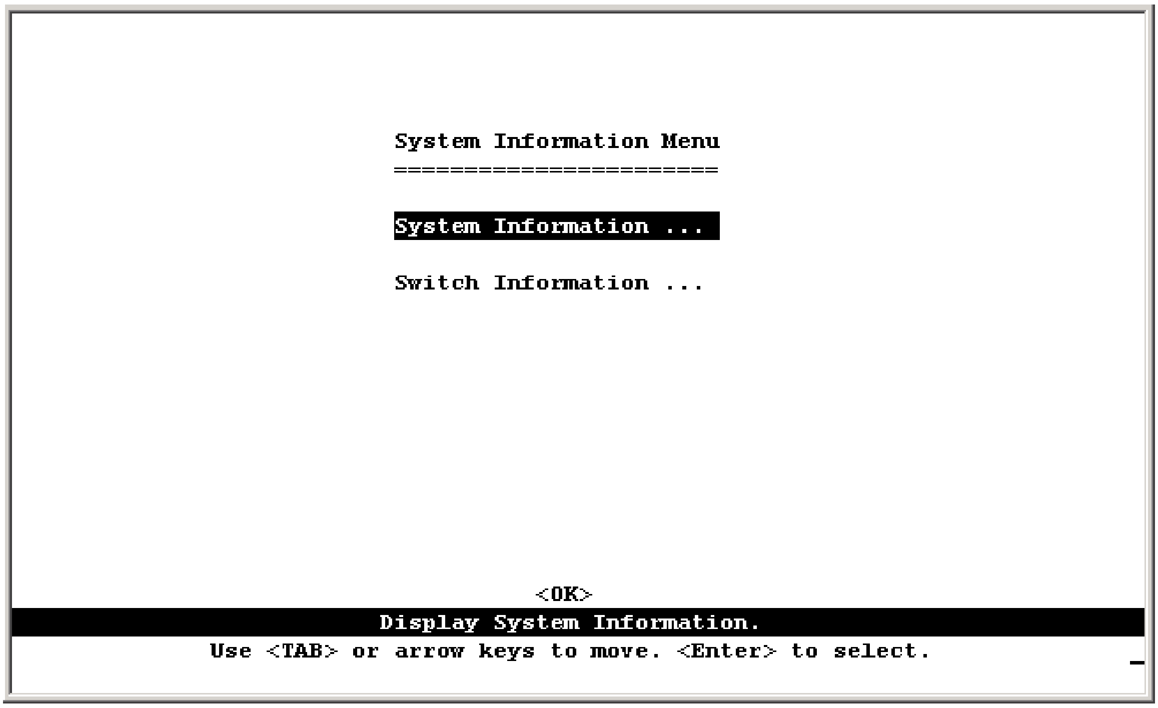
Device Control Menu	
System Mode	Sets the switch to operate as a Layer 2 switch or as a multilayer routing switch.
Layer 2 Menu	Configures port communication mode, mirror ports, port trunking and static unicast/multicast address.
Bridge Menu	Configures GMRP and GVRP for the bridge, and STA for the global bridge or for specific ports.
VLAN Menu	Configures VLAN settings for specific ports, and defines the port membership for VLAN groups.
IGMP Snooping Configuration [*1]	Configures IGMP multicast filtering.
IP Menu [*2]	Configures the subnets for each VLAN group, global configuration for unicast and multicast protocols, BOOPP/DHCP relay, static ARP table entries, static routes and the default route.
Security	Restrict access through MAC address or IP address[*2]
Network Monitor Menu	
Port Statistics	Displays statistics on port traffic, including information from the Interfaces Group, Ethernet-link MIB, and RMON MIB.
Layer 2 Address Table	Contains tables for all unicast, static unicast, and static multicast addresses, as well as the filter table for MAC addresses.
Bridge Menu	Displays Spanning Tree Bridge and Port information
VLAN Menu	Displays dynamic port registration information for VLANs, as well as all VLAN forwarding information for static and dynamic assignment.
IP Multicast Registration Table [*1]	Displays all the multicast groups active on this switch, including the multicast IP addresses and corresponding VLANs.
IP Menu [*2]	Displays all the IP subnets used on this switch, as well as the corresponding VLANs and ports. Also contains the ARP table, routing table and multicast table.
Restart System Menu	Restarts the system with options to reload factory defaults.
Exit	Exits the configuration program.

*1: Only displays when the switch is set to Layer 2 mode.

*2. Only displays when the switch is set to multilayer mode.

4.3 System Information Menu

Use the System Information Menu to display a basic description of the switch, including contact information, and hardware/firmware versions.

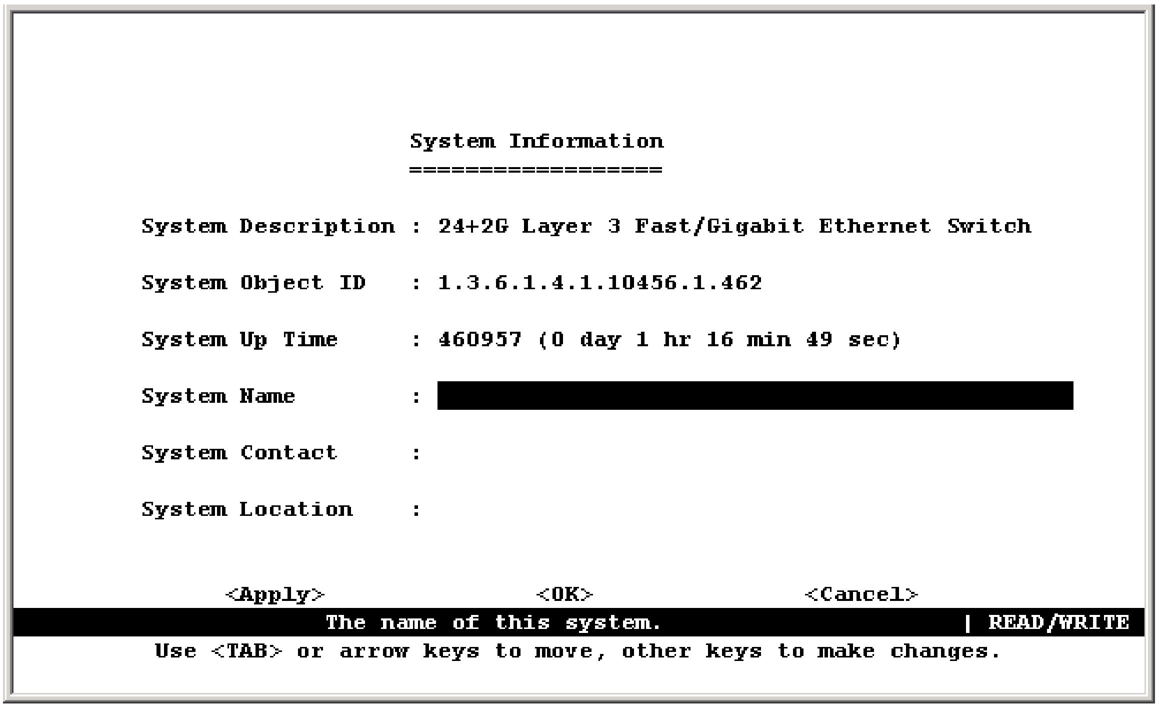


```
System Information Menu
=======================

System Information ...

Switch Information ...

<OK>
Display System Information.
Use <TAB> or arrow keys to move. <Enter> to select.
```

Menu	Description
System Information	Provides basic system description, including contact information.
Switch Information	Shows hardware/firmware version numbers, power status, and expansion modules used in the switch.

4.3.1 Displaying System Information

Use the System Information screen to display descriptive information about the switch, or for quick system identification as shown in the following figure and table.



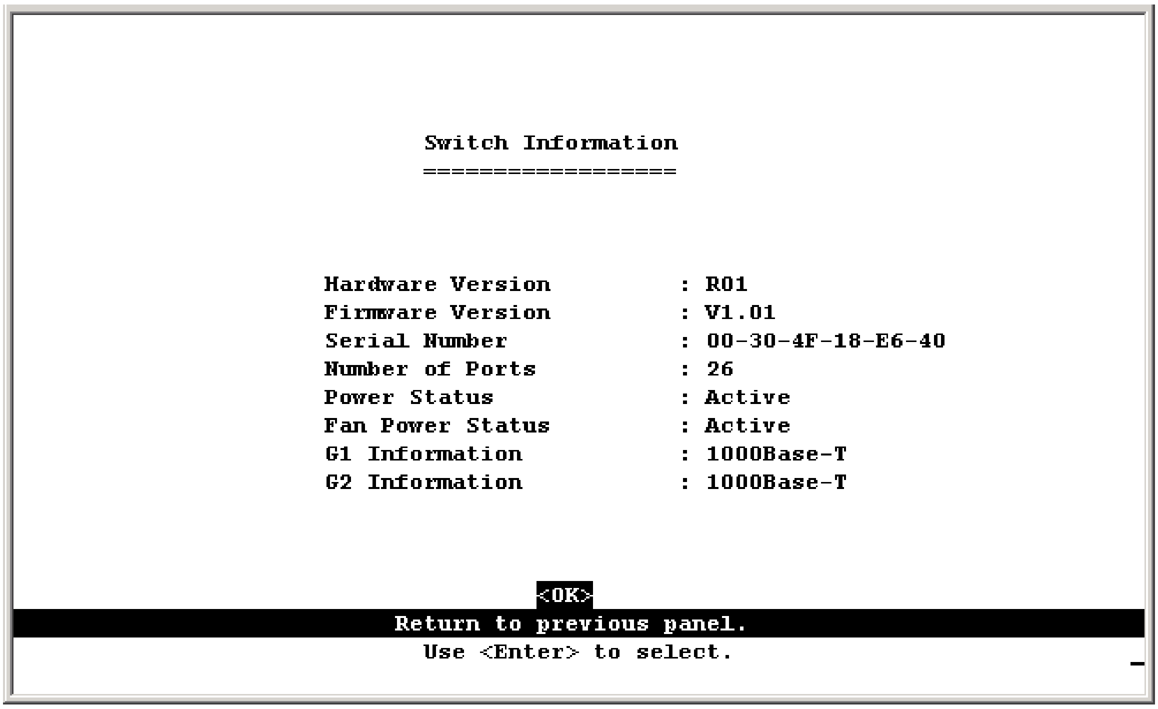
```
                         System Information
                         ==================

        System Description : 24+2G Layer 3 Fast/Gigabit Ethernet Switch

        System Object ID   : 1.3.6.1.4.1.10456.1.462

        System Up Time     : 460957 (0 day 1 hr 16 min 49 sec)

        System Name        :

        System Contact     :

        System Location    :


              <Apply>              <OK>               <Cancel>
                    The name of this system.                   | READ/WRITE
          Use <TAB> or arrow keys to move, other keys to make changes.
```

Parameter	Description
System Description	System hardware description.
System Object ID	MIB II object identifier for switch's network management subsystem.
System Up Time	Length of time the current management agent has been running. (Note that the first value is centiseconds.)
System Name*	Name assigned to the switch system.
System Contact*	Contact person for the system.
System Location*	Specifies the area or location where the system resides.

* Maximum string length is 99, but the screen only displays 45 characters. You can use the arrow keys to browse the whole string.

4.3.2 Displaying Switch Version Information

Use the Switch Information screen to display hardware/firmware version numbers for the main board, as well as the fan power status.

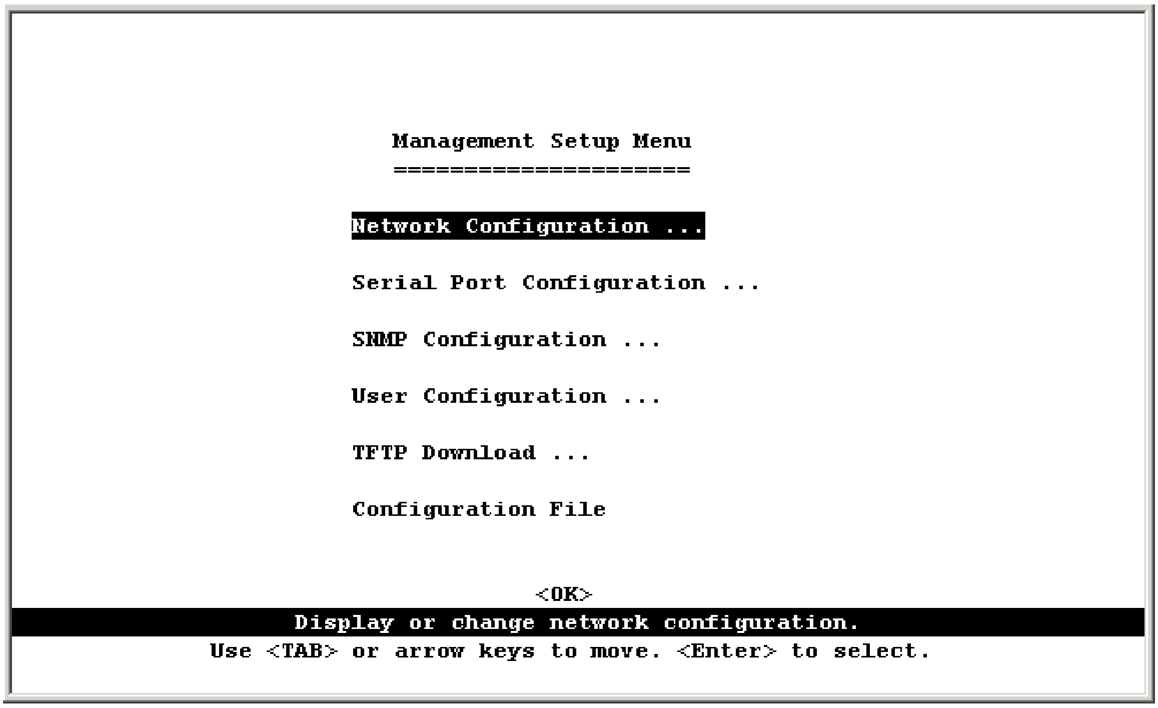


```
                     Switch Information
                     ==================


       Hardware Version          : R01
       Firmware Version          : V1.01
       Serial Number             : 00-30-4F-18-E6-40
       Number of Ports           : 26
       Power Status              : Active
       Fan Power Status          : Active
       G1 Information            : 1000Base-T
       G2 Information            : 1000Base-T


                          <OK>
                  Return to previous panel.
                   Use <Enter> to select.
```

Parameter	Description
Hardware Version	Hardware version of the main board.
Firmware Version	System firmware version in ROM.
Serial Number	The serial number of the main board.
Port Number	Number of ports on this switch.
Power Status	Shows if power is active
Fan Power Status	Shows if power to the fan is active or inactive.
G1 and G2 Information	Shows the G1 and G2 connection type. It is always 1000Base-T on this version

4.4 Management Setup Menu

After initially logging onto the system, adjust the communication parameters for your console to ensure a reliable connection (Serial Port Configuration). Specify the IP addresses for the switch (Network Configuration / IP Configuration), and then set the Administrator and User passwords (I User Configuration). Remember to record them in a safe place. Also set the community string which controls access to the on-board SNMP agent via in-band management software (SNMP Configuration). The items provided by the Management Setup Menu are described in the following sections.

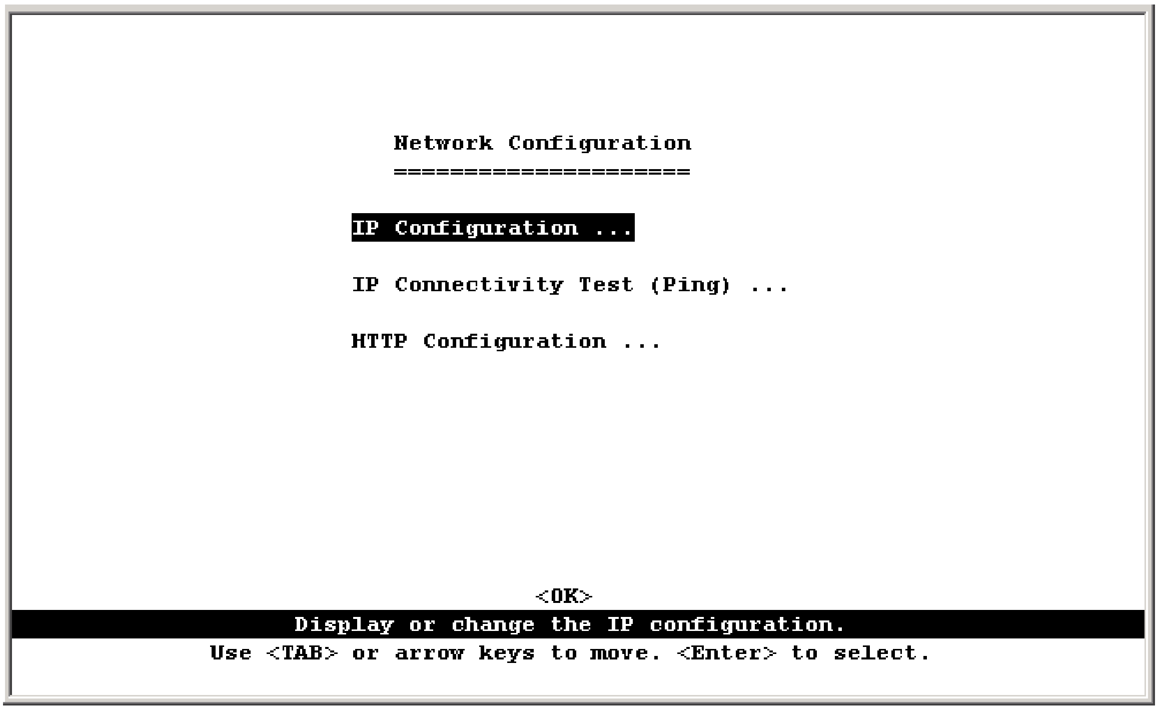


```
                    Management Setup Menu
                    =====================

                 Network Configuration ...

                 Serial Port Configuration ...

                 SNMP Configuration ...

                 User Configuration ...

                 TFTP Download ...

                 Configuration File


                            <OK>
              Display or change network configuration.
          Use <TAB> or arrow keys to move. <Enter> to select.
```

Menu	Description
Network Configuration	Includes IP Configuration ^{*1}, Ping facility, and HTTP (Web agent) setup.
Serial Port Configuration	Sets communication parameters for the serial port, including baud rate, console time-out, and screen data refresh interval.
SNMP Configuration	Activates authentication failure traps; and configures communities and trap managers.
User Configuration	Sets the user names and passwords for system access.
TFTP Download	Downloads new version of firmware to update your system (in-band).
Configuration File	Download the configuration to a file or upload the configuration file to the switch.

4.4.1 Changing the Network Configuration

Use the Network Configuration menu to set the bootup option, configure the switch' s Interne t Protocol (IP) parameters, or enable the on-board Web agent. The screen shown below is described in the following table.



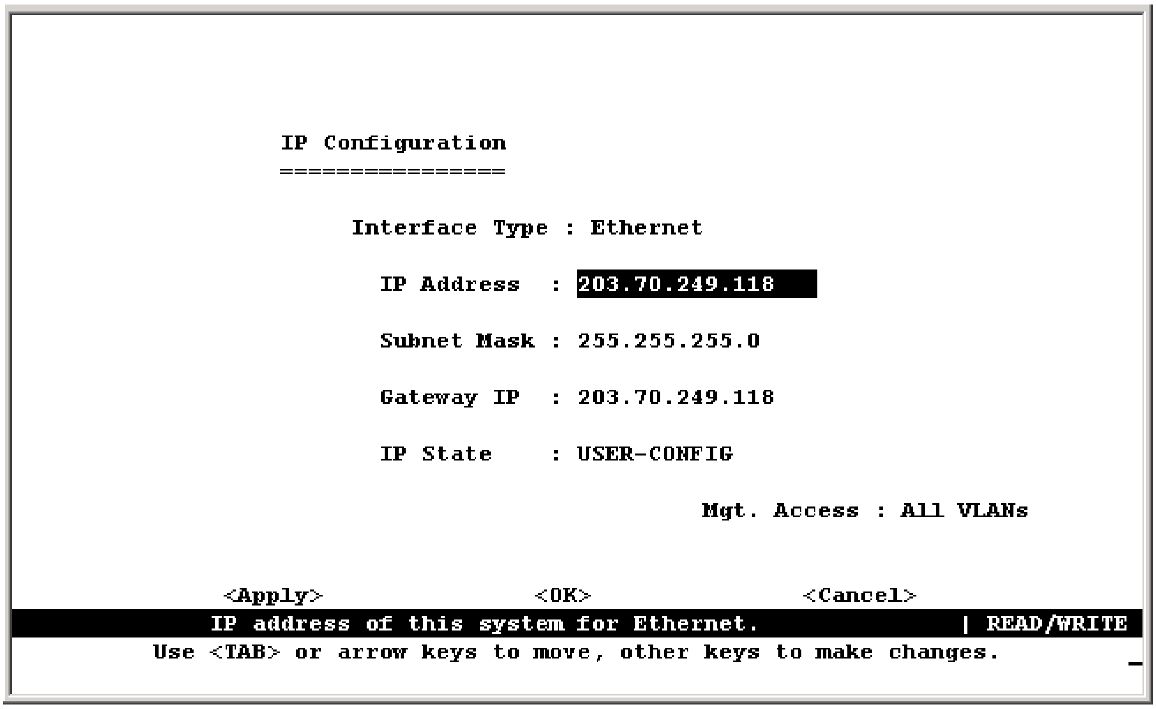
```
                    Network Configuration
                    =====================

                 IP Configuration ...

                 IP Connectivity Test (Ping) ...

                 HTTP Configuration ...




                           <OK>
              Display or change the IP configuration.
          Use <TAB> or arrow keys to move. <Enter> to select.
```

Parameter	Description
IP Configuration*	Screen used to set the bootup option, or configure the switch' s IP parameters.
IP Connectivity Test (Ping)	Screen used to test IP connectivity to a specified device.
HTTP Configuration	Screen used to enable the Web agent.

* This menu does not appear if the switch is set to multilayer mode. In this case, you need to configure an IP interface for each VLAN that needs to connect to any device outside of its own VLAN group. (See “Subnet Configuration”)

4.4.1.1 IP Configuration (Layer 2 Mode)

Use the IP Configuration screen to set the boot-up option, or configure the switch's IP parameter s. The screen shown below is described in the following table.

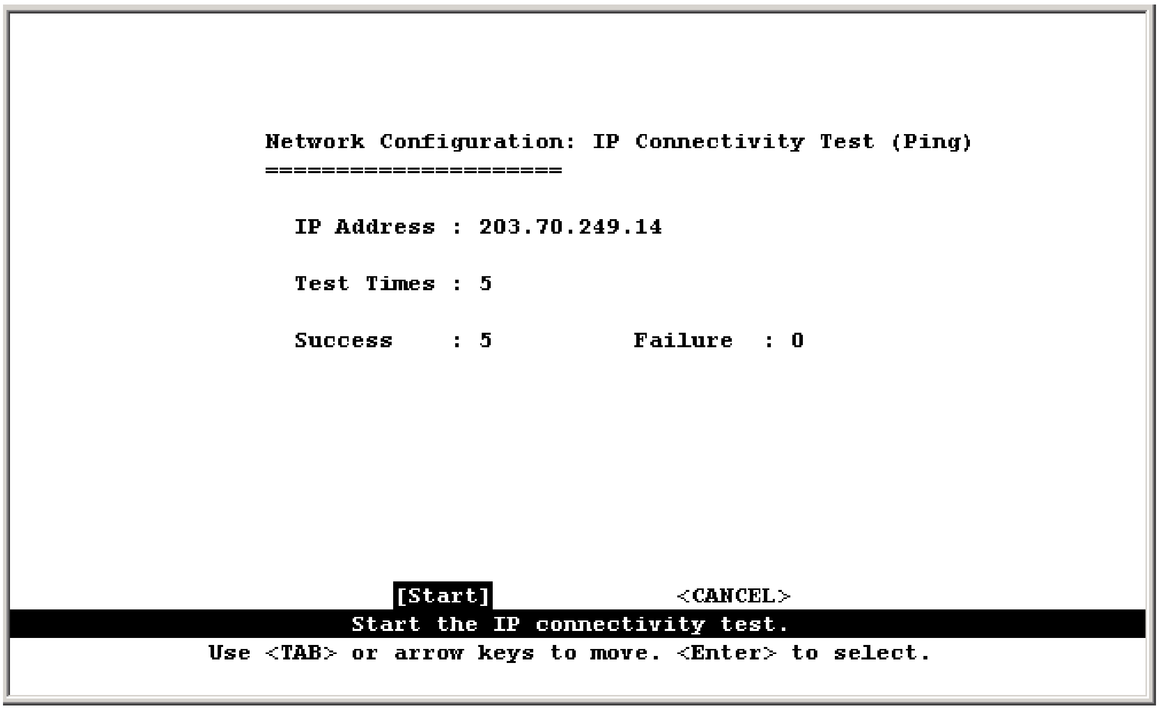


```
                    IP Configuration
                    ================

                         Interface Type : Ethernet

                           IP Address   : 203.70.249.118

                           Subnet Mask : 255.255.255.0

                           Gateway IP   : 203.70.249.118

                           IP State     : USER-CONFIG

                                                      Mgt. Access : All VLANs


               <Apply>                <OK>                <Cancel>
              IP address of this system for Ethernet.              | READ/WRITE
          Use <TAB> or arrow keys to move, other keys to make changes.
```

Parameter	Description
Interface Type	Indicates IP over Ethernet.
IP Address	IP address of the switch you are managing. The system supports SNMP over UDP/IP transport protocol. In this environment, all systems on the Internet, such as network interconnection devices and any PC accessing the agent module must have an IP address. Valid IP addresses consist of four numbers, of 0 to 255, and separated by periods. Anything outside of this format will not be accepted by the configuration program.
Subnet Mask	Subnet mask of the switch. This mask identifies the host address bits used for routing to specific subnets.
Default Gateway	Gateway used to pass trap messages from the system's agent to the management station. Note that the gateway must be defined (when operating at Layer 2) if the management station is located in a different IP segment.
IP State	Specifies whether IP functionality is enabled via manual configuration, or set by Boot Protocol (BOOTP). Options include: USER-CONFIG - IP functionality is enabled based on the default or user specified IP Configuration. (This is the default setting.) BOOTP Get IP - IP is enabled but will not function until a BOOTP reply has been received. BOOTP requests will be periodically broadcasted by the switch in an effort to learn its IP address. (BOOTP values can include the IP address, default gateway, and subnet mask.)
VLAN ID	The VLAN used for management access when "Mgmt VLAN" is selected. See the next item.
Mgt. Access	Specifies which VLAN have access right to its management interface. Options include: All VLANs – All VLANs have access right to its management interface. (This is the default setting.) Mgmt VLAN – Only the specified VLAN have access right to its management interface

4.4.1.2 IP Connectivity Test (Ping)

Use the IP Connectivity Test to see if another site on the Internet can be reached. The screen shown below is described in the following table.



```
Network Configuration: IP Connectivity Test (Ping)
=====================

  IP Address : 203.70.249.14

  Test Times : 5

  Success    : 5          Failure  : 0
```

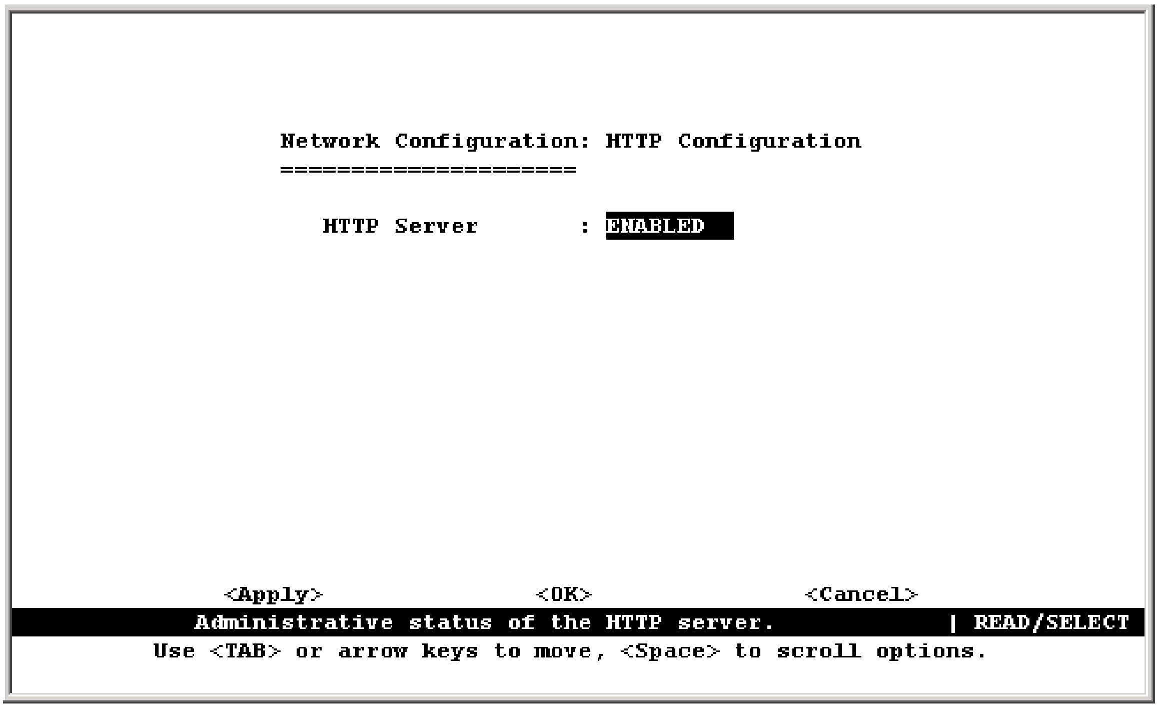
[Start]
<CANCEL>
Start the IP connectivity test.
Use <TAB> or arrow keys to move. <Enter> to select.

Parameter	Description
IP Address	IP address of the site you want to ping.
Test Times	The number of ICMP echo requests to send to the specified site. Range: 1~1000
Success / Failure	The number of times the specified site has responded or not to pinging.

Note: The switch waits up to 10 seconds for a response to each ping.

4.4.1.3 HTTP Configuration

Use the HTTP Configuration screen to enable/disable the on-board Web agent.

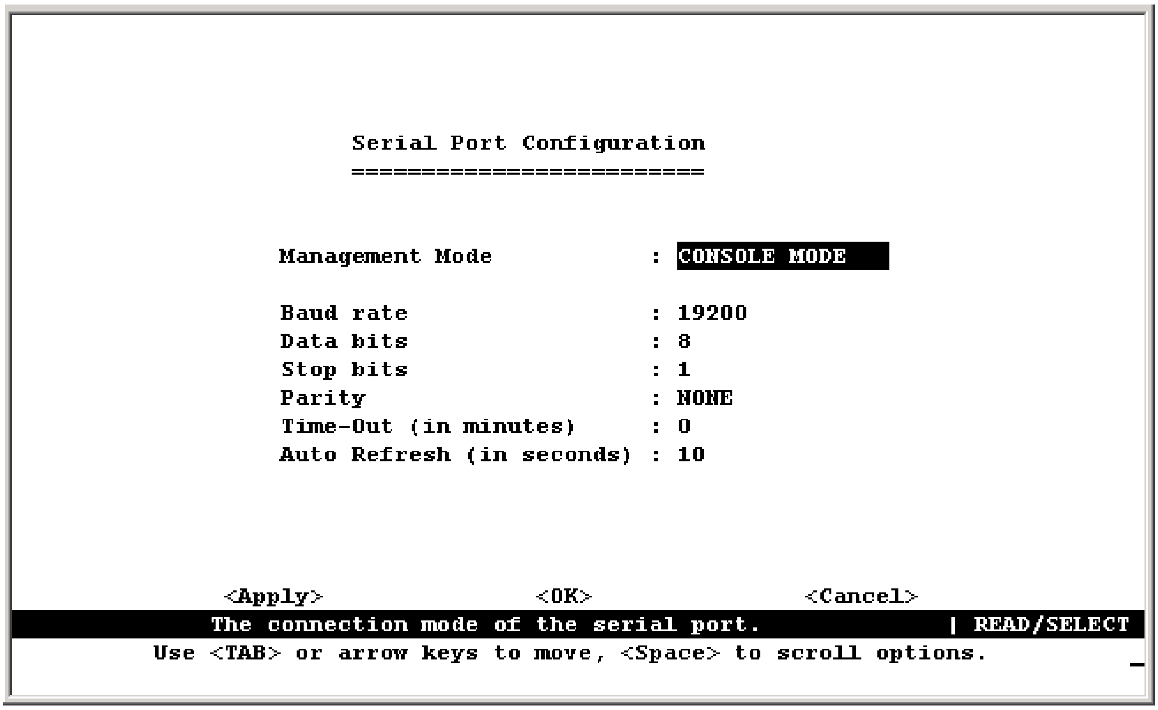


```
                    Network Configuration: HTTP Configuration
                    =====================

                       HTTP Server       : ENABLED





               <Apply>                 <OK>                 <Cancel>
             Administrative status of the HTTP server.            | READ/SELECT
          Use <TAB> or arrow keys to move, <Space> to scroll options.
```

Note: Port 80 is used for HTTP service.

4.4.2 Configuring the Serial Port

You can access the on-board configuration program by attaching a VT100 compatible device to the switch' s serial port. (For more information on connecting to this port, see "Required Connections" on Chapter 1) The communication parameters for this port can be accessed from the Serial Port Configuration screen shown below and described in the following table.

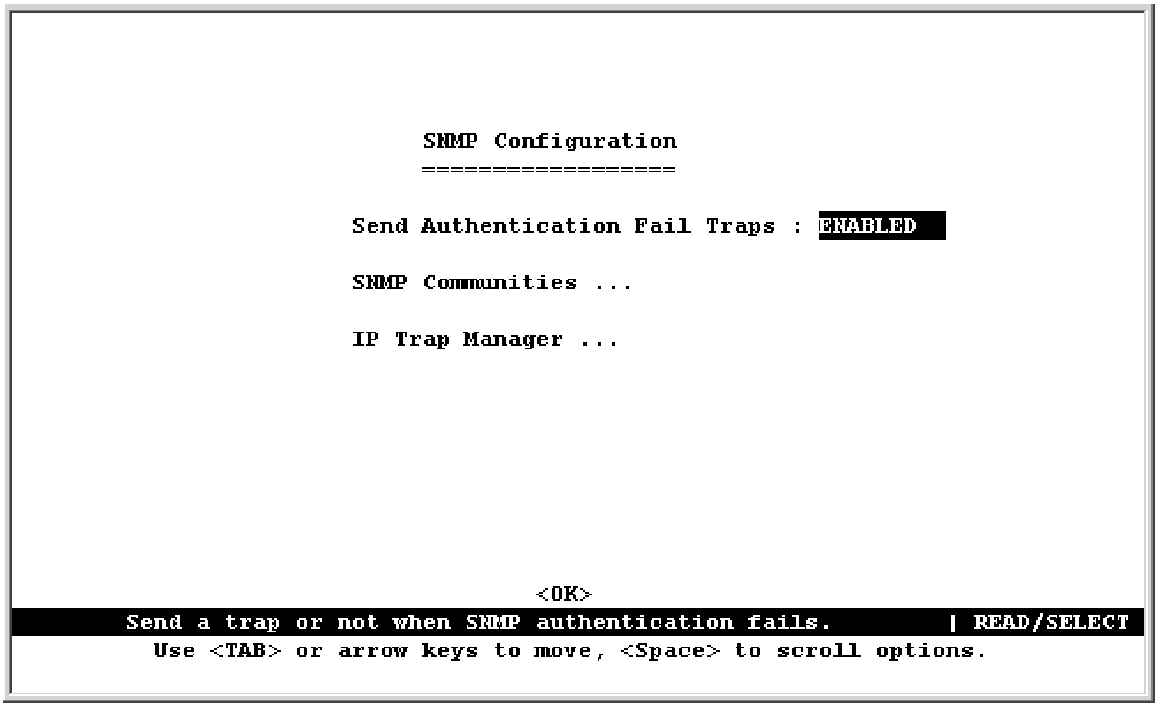


```
                 Serial Port Configuration
                 =========================

            Management Mode            : CONSOLE MODE

            Baud rate                  : 19200
            Data bits                  : 8
            Stop bits                  : 1
            Parity                     : NONE
            Time-Out (in minutes)      : 0
            Auto Refresh (in seconds)  : 10



         <Apply>              <OK>              <Cancel>
        The connection mode of the serial port.             | READ/SELECT
     Use <TAB> or arrow keys to move, <Space> to scroll options.
```

Parameter	Default	Description
Management Mode	Console Mode	Indicates that the port settings are for direct console connection.
Baud Rate	19200	The rate at which data is sent between devices. Options : 9600, 19200 and 38400 baud.
Data Bits	8 bits	Sets the data bits of the RS-232 port. Options : 7, 8
Stop Bits	1 bit	Sets the stop bits of the RS-232 port. Options : 1, 2
Parity	None	Sets the parity of the RS-232 port. Options : none/odd/even
Time-Out	0	If no input is received from the attached device after this interval, the current session is automatically closed. Range : 0 - 100 minutes; where 0 indicates disabled
Auto Refresh	10 second	Sets the interval before a console session will auto refresh the console information, such as Spanning Tree Information, Port Configuration, Port Statistics, and RMON Statistics. Range : 0, or 5-255 seconds; where 0 indicates disabled

4.4.3 Assigning SNMP Parameters

Use the SNMP Configuration screen to display and modify parameters for the Simple Network Management Protocol (SNMP). The switch includes an on-board SNMP agent which monitors the status of its hardware, as well as the traffic passing through its ports. A computer attached to the network, called a Network Management Station (NMS), can be used to access this information. Access rights to the on-board agent are controlled by community strings. To communicate with the switch, the NMS must first submit a valid community string for authentication. The options for configuring community strings and related trap functions are described in the following sections.

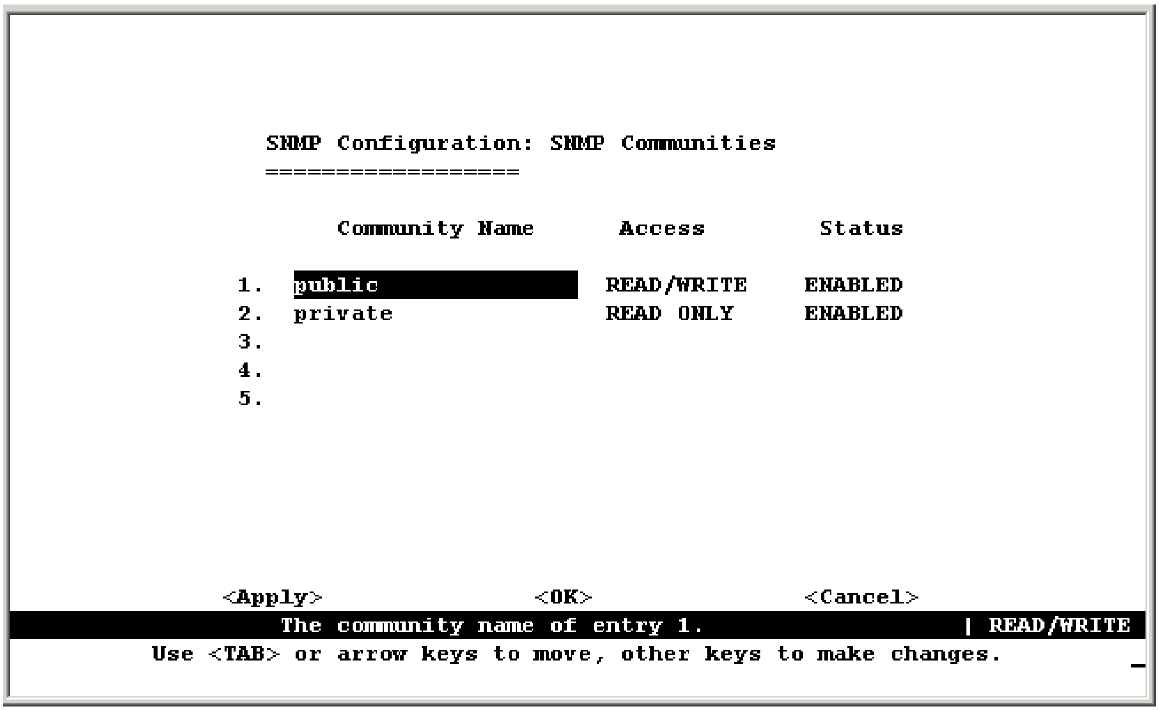


```
                    SNMP Configuration
                    ==================

     Send Authentication Fail Traps : ENABLED

     SNMP Communities ...

     IP Trap Manager ...



                         <OK>
   Send a trap or not when SNMP authentication fails.       | READ/SELECT
      Use <TAB> or arrow keys to move, <Space> to scroll options.
```

Parameter	Description
Send Authentication Fail Traps	Issue a trap message to specified IP trap managers whenever authentication of an SNMP request fails. (The default is enabled.)
SNMP Communities	Assigns SNMP access based on specified strings.
IP Trap Managers	Specifies management stations that will receive authentication failure messages or other trap messages from the switch.

4.4.3.1 Configuring Community Names

The following figure and table describe how to configure the community strings authorized for management access. Up to 5 community names may be entered.



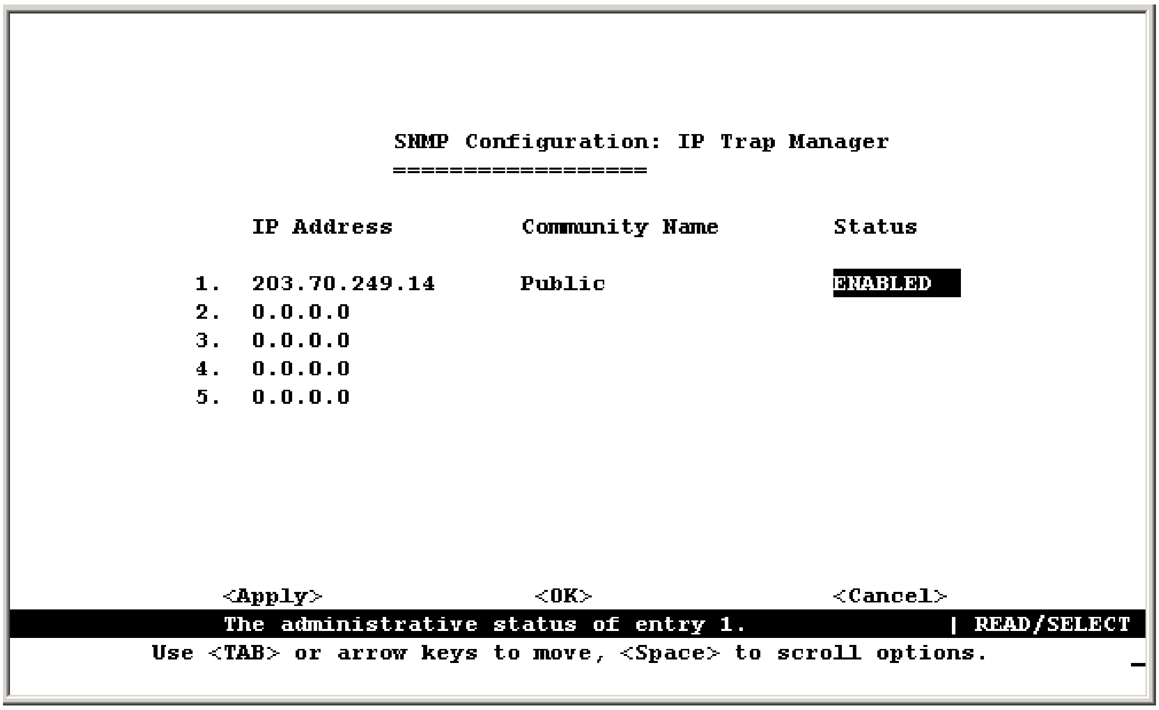
```
                SNMP Configuration: SNMP Communities
                =================

                     Community Name       Access        Status

              1.  public                 READ/WRITE    ENABLED
              2.  private                READ ONLY     ENABLED
              3.
              4.
              5.




             <Apply>               <OK>               <Cancel>
                  The community name of entry 1.                 | READ/WRITE
          Use <TAB> or arrow keys to move, other keys to make changes.
```

Parameter	Description
Community Name	A community entry authorized for management access. Maximum string length : 19 characters
Access	Management access is restricted to Read Only or Read/ Write.
Status	Sets administrative status of entry to enabled or disabled.

Note: The default community strings are displayed on the screen.

4.4.3.2 Configuring IP Trap Managers

The following figure and table describe how to specify management stations that will receive authentication failure messages or other trap messages from the switch. Up to 5 trap managers may be entered.

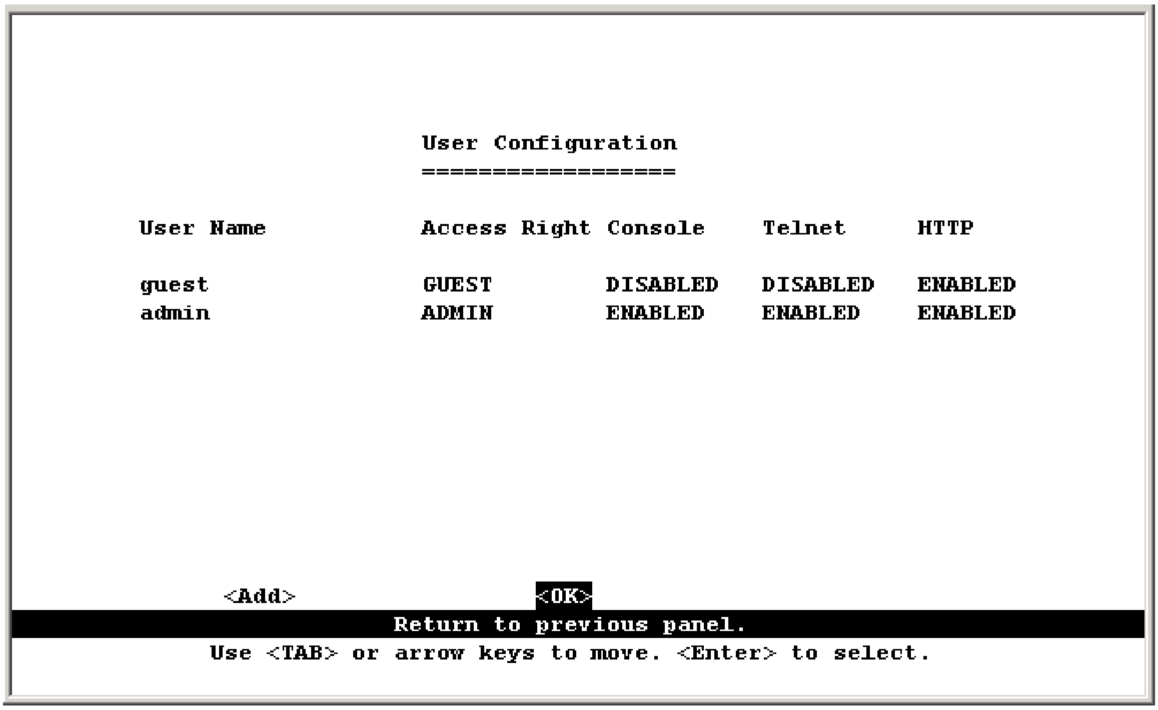


```
                  SNMP Configuration: IP Trap Manager
                  ==================

          IP Address          Community Name        Status

      1.  203.70.249.14       Public                ENABLED
      2.  0.0.0.0
      3.  0.0.0.0
      4.  0.0.0.0
      5.  0.0.0.0



          <Apply>              <OK>                  <Cancel>
          The administrative status of entry 1.              | READ/SELECT
     Use <TAB> or arrow keys to move, <Space> to scroll options.
```

Parameter	Description
IP Address	IP address of the trap manager.
Community Name	A community specified for trap management access.
Status	Sets administrative status of selected entry to enabled or disabled.

4.4.4 User Login Configuration

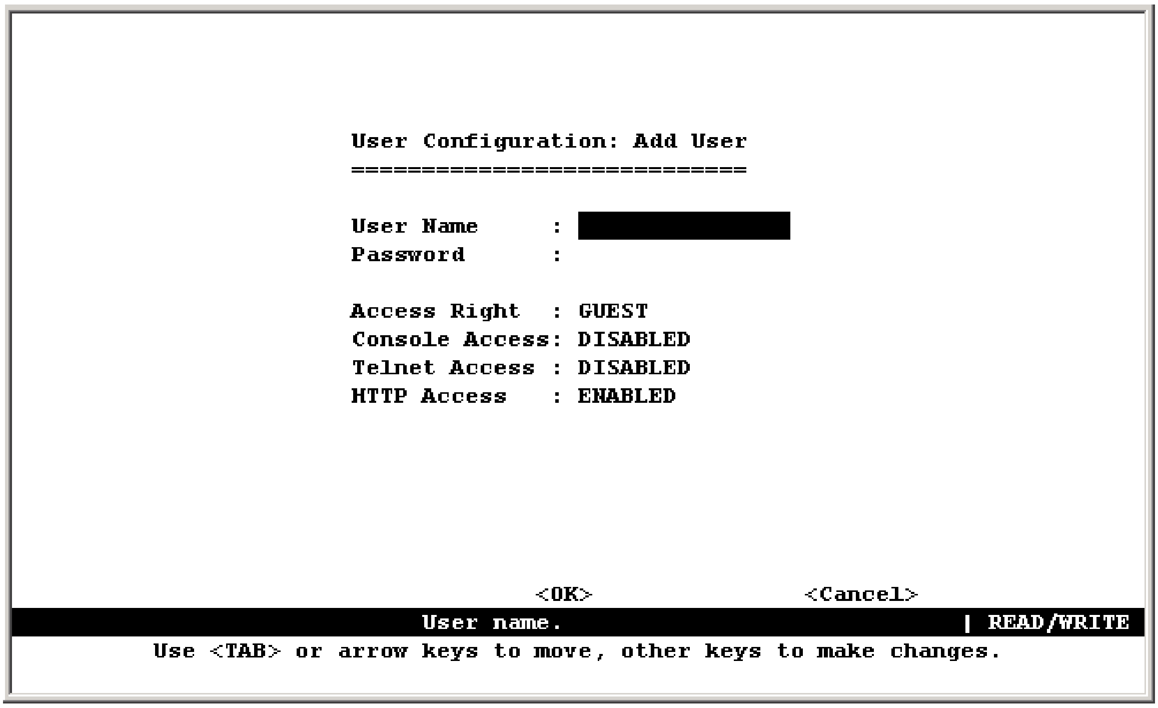
Use the User Configuration menu to restrict management access based on specified user names and passwords. There are two user types, Administrator and Guest. Only the Administrator has write access for parameters governing the SNMP agent. You should therefore assign a user name and password to the Administrator as soon as possible, and store it in a safe place. (If for some reason your password is lost, or you cannot gain access to the System Configuration Program, contact Technical Support for assistance.) The parameters shown on this screen are indicated in the following figure and table.



```
                        User Configuration
                        ==================

      User Name         Access Right Console    Telnet     HTTP

      guest             GUEST        DISABLED   DISABLED   ENABLED
      admin             ADMIN        ENABLED    ENABLED    ENABLED








           <Add>                <OK>
                        Return to previous panel.
                  Use <TAB> or arrow keys to move. <Enter> to select.
```

Parameter	Description
User Name	Specifies a user authorized management access to the switch via the console, Telnet or HTTP.
Access Right	There are two options.　ADMIN: Read/Write for all screens. GUEST: Read Only for all screens.
Console	Authorizes management via the console.
Telnet	Authorizes management via Telnet.
HTTP	Authorizes management via HTTP (that is, Microsoft Internet Explorer 4.0 or later version.　It does not support Netscape currently).

To add a new user, select <Add>. When you add a user, the following screen is displayed.



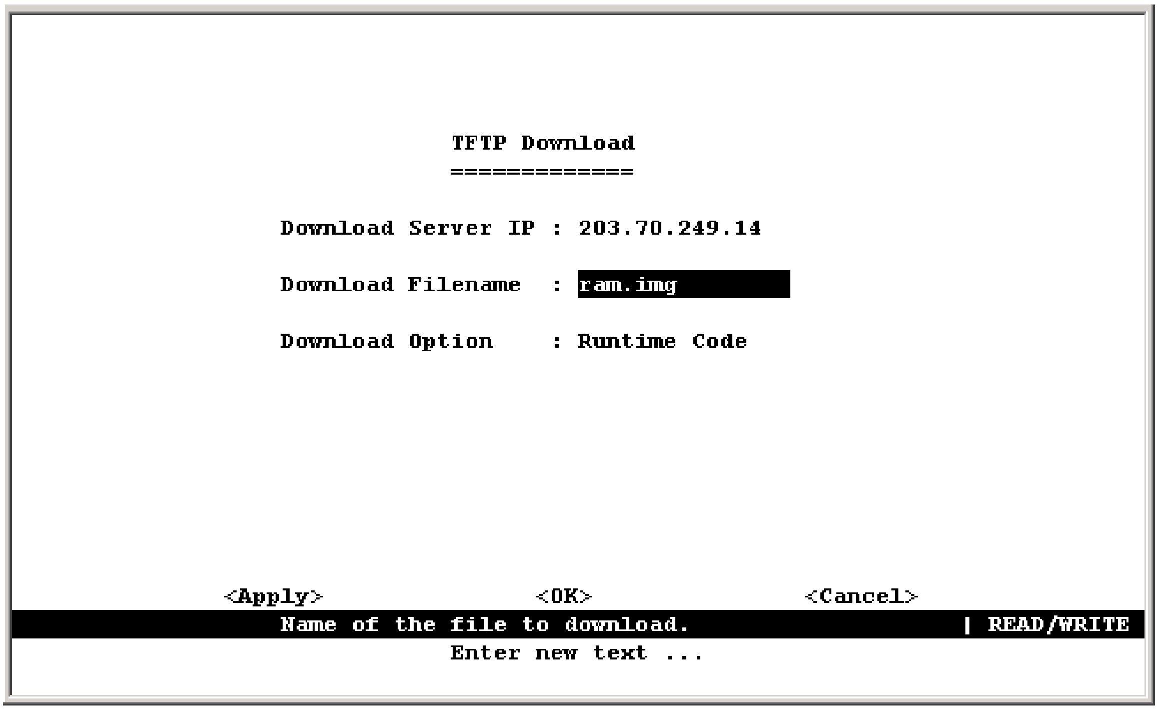
```
                       User Configuration: Add User
                       ============================

                       User Name     : 
                       Password      :

                       Access Right  : GUEST
                       Console Access: DISABLED
                       Telnet Access : DISABLED
                       HTTP Access   : ENABLED




                                   <OK>              <Cancel>
                            User name.                          | READ/WRITE
          Use <TAB> or arrow keys to move, other keys to make changes.
```

Parameter	Description
User Name*	Specifies a user authorized management access to the switch via the console, Telnet or HTTP.
Password*	Passwords can consist of up to 11 alphanumeric characters and are not case sensitive.
Access Right	ADMIN: Read/Write for all screens. GUEST: Read Only for all screens.
Console Access	Authorizes management via the console.
Telnet Access	Authorizes management via Telnet.
HTTP Access	Authorizes management via HTTP (that is, Microsoft Internet Explorer 4.0 or later version).

* These entries can consist of up to 15 alphanumeric characters and are not case sensitive.

4.4.5 Downloading System Software

Use the TFTP Download menu to load software updates to permanent flash ROM in the switch. The download file should be a 3 binary file or image file; otherwise the agent will not accept it. The success of the download operation depends on the accessibility of the TFTP server and the quality of the network connection. After downloading the new software, the agent will automatically restart itself. Parameters shown on this screen are indicated in the following figure and table.



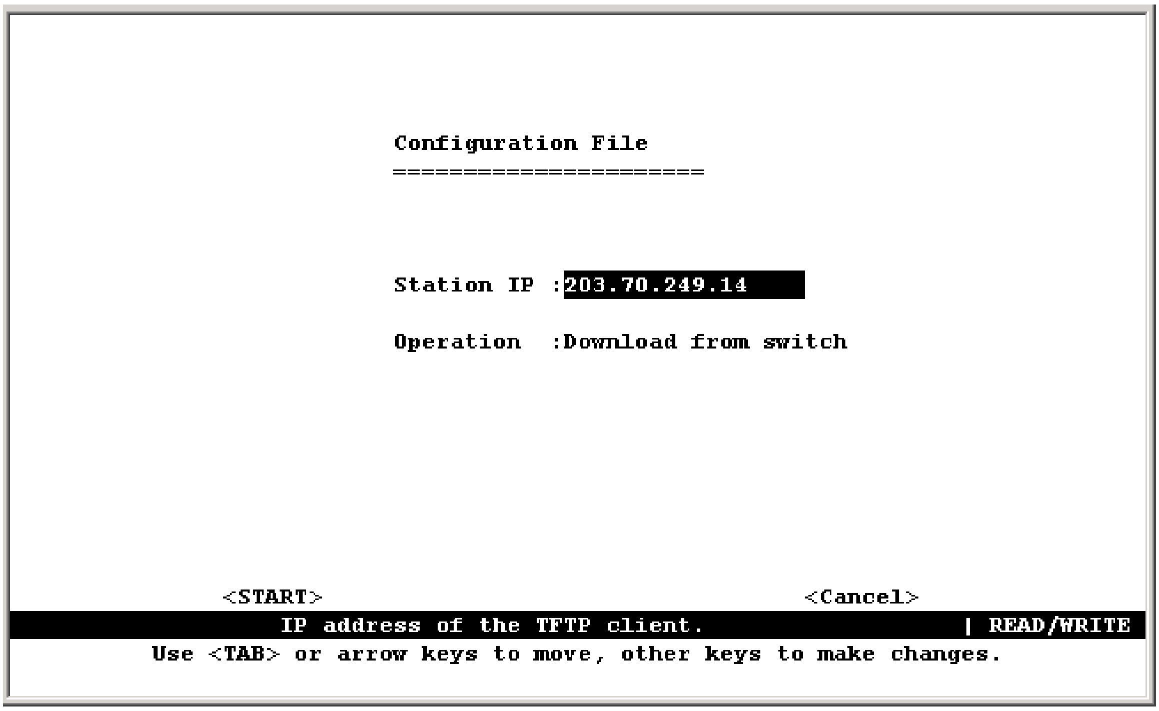
```
                         TFTP Download
                         =============

            Download Server IP : 203.70.249.14

            Download Filename  : ram.img

            Download Option    : Runtime Code



        <Apply>              <OK>              <Cancel>
            Name of the file to download.                | READ/WRITE
                         Enter new text ...
```

Parameter	Description
Download Server IP	IP address of a TFTP server.
Download Filename	The binary file to download.
Download Option	Specify the file to be Runtime code or POST code.

Note: You can also download firmware using the Web agent or by a direct console connection after a restart.

4.4.6 Saving or Restoring the System Configuration

Use the Configuration File menu to save the switch configuration settings to a file on a TFTP client. The file can be later downloaded to the switch to restore the switch's settings. The success of the operation depends on the accessibility of the TFTP client and the quality of the network connection. Parameters shown on this screen are indicated in the following figure and table.



```
                    Configuration File
                    ======================



                    Station IP :203.70.249.14

                    Operation  :Download from switch









       <START>                                  <Cancel>
                IP address of the TFTP client.                 | READ/WRITE
          Use <TAB> or arrow keys to move, other keys to make changes.
```

Parameter	Description
Station IP	IP address of a PC running TFTP client software.
Operation	Download from switch – Downloads the current switch configuration to a file on the client PC. Upload to switch – Uploads a configuration file to the switch from the client PC.

Note: Saving and restoring switch configuration settings can then be initiated by using any TFTP client utility, such as the command line utility included in Windows NT/2000/XP. For example, using Windows NT, from a DOS window command prompt, enter the TFTP command in the form:

TFTP [-i] host [GET : PUT] source [destination]

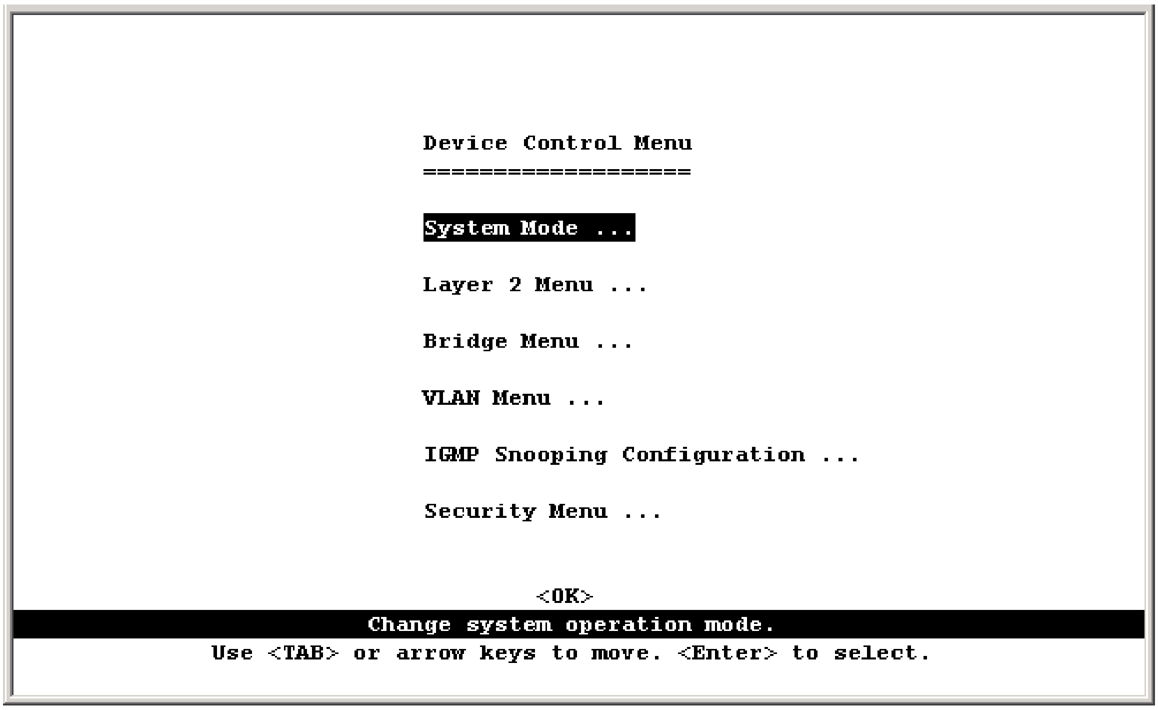
To transfer a file –

1. On Switch: Specify the IP address of the TFTP client, and select “Download from switch” or “Upload to Switch.” Then select <Start> from the menu to start.
2. On TFTP Client: Set the mode to <binary>, specify the IP address of the target switch and the directory path / name of the file to transfer. Then start transferring the configuration from the TFTP client or the switch and wait until the transfer completes.

For example, type “tftp -i 203.70.249.118 GET source wgs3.txt” on Windows 2000’s command prompt to download switch’s configuration and type “tftp –i 203.70.249.118 PUT wgs3.txt” to upload the configuration file to switch.

4.5 Device Control Menu

The Device Control menu is used to control a broad range of functions, including port mode, port mirroring, port trunking, Spanning Tree, Virtual LANs, IP subnets, multicast filtering, and routing protocols. Each of the setup screens provided by these configuration menus is described in the following sections.



```
                    Device Control Menu
                    ===================

                    System Mode ...

                    Layer 2 Menu ...

                    Bridge Menu ...

                    VLAN Menu ...

                    IGMP Snooping Configuration ...

                    Security Menu ...


                          <OK>
               Change system operation mode.
        Use <TAB> or arrow keys to move. <Enter> to select.
```

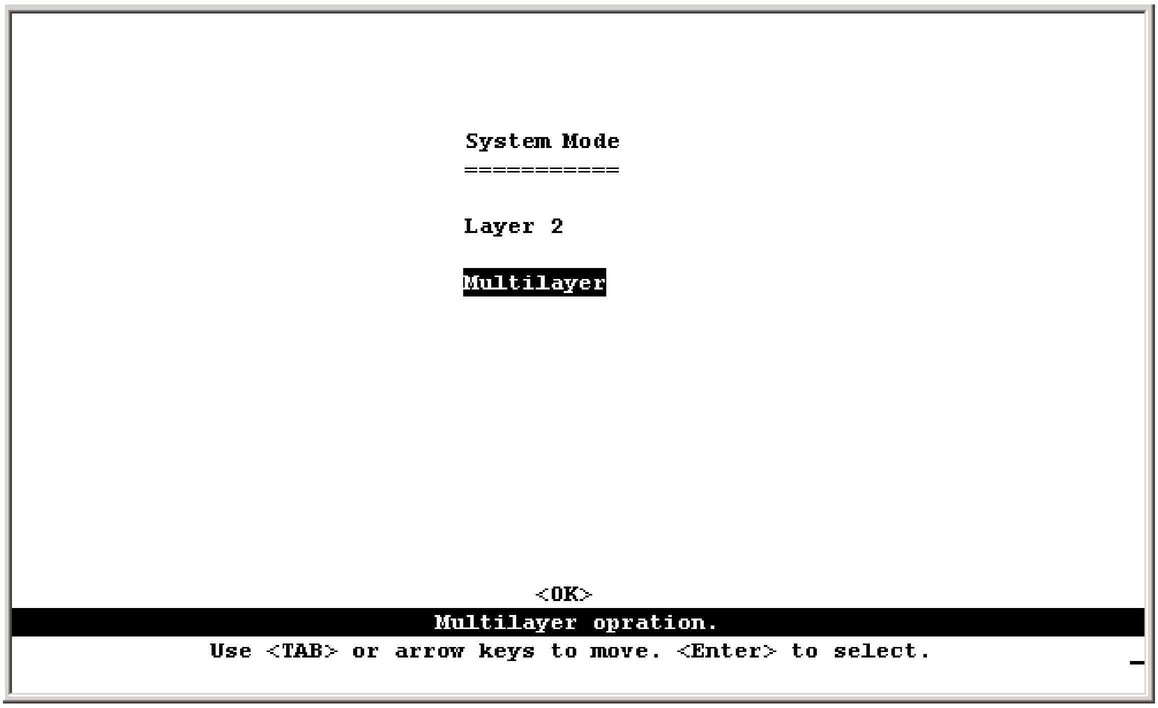
Menu	Description
System Mode	Sets the switch to operate as a Layer 2 switch or as a multilayer routing switch.
Layer 2 Menu	Configures port communication mode, mirror ports, and port trunking.
Bridge Menu	Configures the Spanning Tree Protocol for the bridge or for specific ports, GMRP and GVRP for automatic registration of multicast and VLAN groups, traffic class priority threshold, and address aging time.
VLAN Menu	Configures VLAN settings for specific ports, and defines the port membership for VLAN groups.
IGMP Snooping Configuration *1	Configures IGMP multicast filtering.
IP Menu *2	Configures the subnets for each VLAN group, global configuration for unicast and multicast routing protocols, IGMP snooping
Security	Restrict access through MAC address or IP address*2

1: Only displayed for Layer 2 mode.

2: Only displayed for Multilayer mode.

4.5.1 Setting the System Operation Mode

This switch can be set to operate as a Layer 2 switch, making all filtering and forwarding decisions based strictly on MAC addresses. Or it can be set to operate as a multilayer routing switch, whereby it switches packets for all non-IP protocols (such as NetBUEI, NetWare or AppleTalk) based on MAC addresses, and routes all IP packets based on the specified routing protocol. The System Mode menu is shown below. Note that the switch will be automatically rebooted whenever the system operation mode is changed.



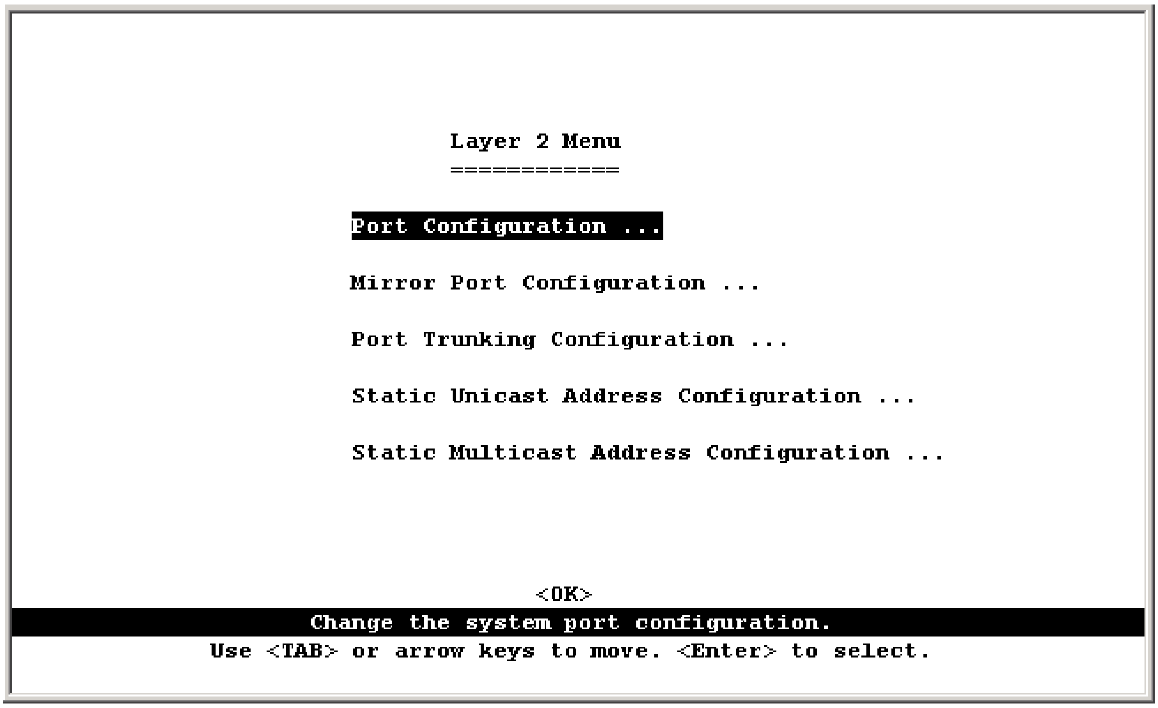
```
System Mode
===========

Layer 2

Multilayer

<OK>
Multilayer opration.
Use <TAB> or arrow keys to move. <Enter> to select.
```

Parameter	Description
Layer 2	Filtering and forwarding decision will be based on MAC addresses for all protocol traffic.
Multilayer	Switching based on MAC addresses will be used for all non-IP protocol traffic, and routing will be used for all IP protocol traffic.

Note: When the switch is set to multilayer mode, the IP menus are enabled, and the “IP Configuration (Layer 2 Mode)” menu is disabled. When operating in multilayer mode, you should configure an IP interface for each VLAN that needs to communicate with any device outside of the VLAN. (See “Subnet Configuration”)

4.5.2 Layer 2 Menu

The Layer 2 menu contains options for port configuration, port mirroring, port trunking and static unicast/multicast address configuration. These menu options are described in the following sections.

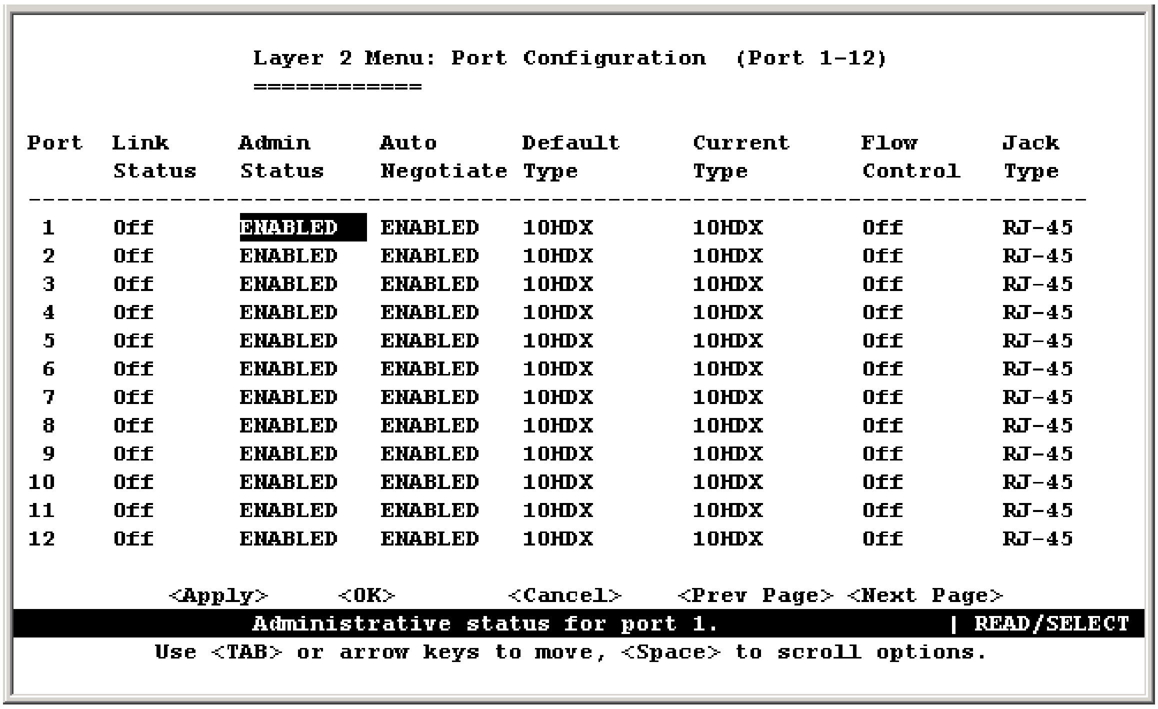


```
                    Layer 2 Menu
                    ============

                Port Configuration ...

                Mirror Port Configuration ...

                Port Trunking Configuration ...

                Static Unicast Address Configuration ...

                Static Multicast Address Configuration ...



                             <OK>
                 Change the system port configuration.
           Use <TAB> or arrow keys to move. <Enter> to select.
```

Menu	Description
Port Configuration	Enables any port, enables/disables flow control, and sets communication mode to auto-negotiation, full duplex or half duplex.
Mirror Port Configuration	Sets the source and target ports for mirroring.
Port Trunking Configuration	Specifies ports to group into aggregate trunks.
Static Unicast Address Configuration	Used to manually configure host MAC addresses in the unicast table.
Static Multicast Address Configuration	Used to manually configure host MAC addresses in the multicast table.

4.5.2.1 Configuring Port Parameters

Use the Port Configuration menu to display or set communication parameters for any port on the switch, including administrative status, auto-negotiation, default communication speed and duplex mode, as well as flow control in use.



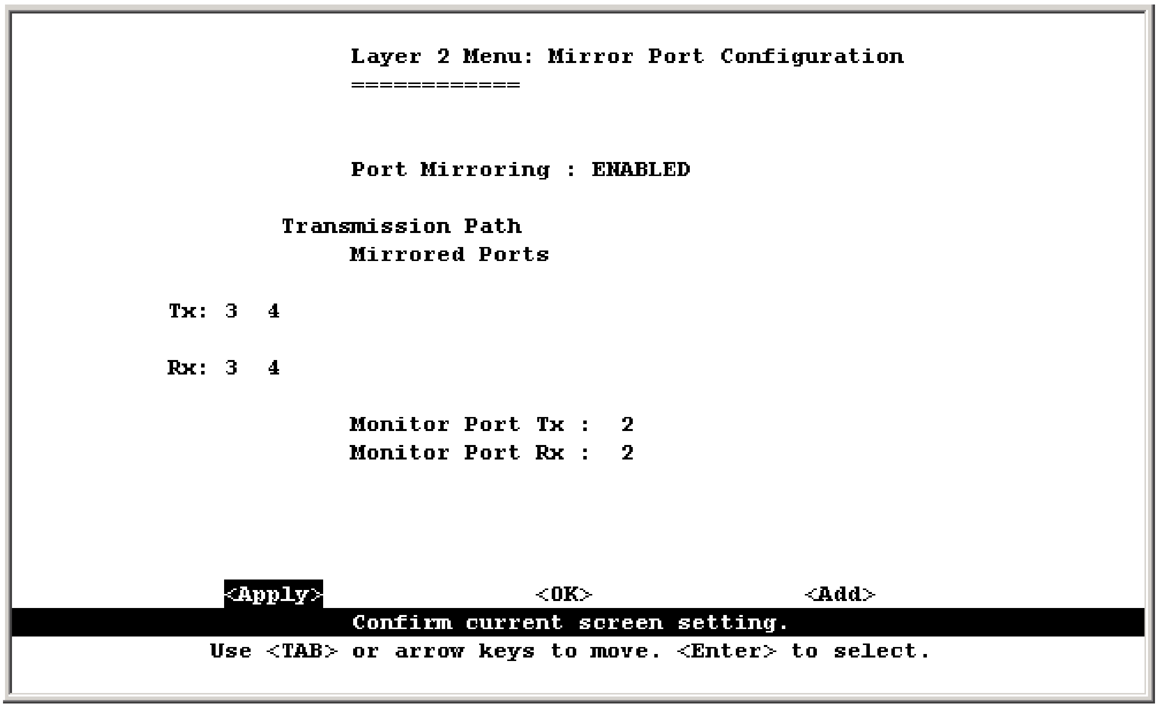
```
                 Layer 2 Menu: Port Configuration  (Port 1-12)
                 ============

Port  Link     Admin     Auto      Default     Current     Flow      Jack
      Status   Status    Negotiate Type        Type        Control   Type
---------------------------------------------------------------------------
 1    Off      ENABLED   ENABLED   10HDX       10HDX       Off       RJ-45
 2    Off      ENABLED   ENABLED   10HDX       10HDX       Off       RJ-45
 3    Off      ENABLED   ENABLED   10HDX       10HDX       Off       RJ-45
 4    Off      ENABLED   ENABLED   10HDX       10HDX       Off       RJ-45
 5    Off      ENABLED   ENABLED   10HDX       10HDX       Off       RJ-45
 6    Off      ENABLED   ENABLED   10HDX       10HDX       Off       RJ-45
 7    Off      ENABLED   ENABLED   10HDX       10HDX       Off       RJ-45
 8    Off      ENABLED   ENABLED   10HDX       10HDX       Off       RJ-45
 9    Off      ENABLED   ENABLED   10HDX       10HDX       Off       RJ-45
10    Off      ENABLED   ENABLED   10HDX       10HDX       Off       RJ-45
11    Off      ENABLED   ENABLED   10HDX       10HDX       Off       RJ-45
12    Off      ENABLED   ENABLED   10HDX       10HDX       Off       RJ-45

           <Apply>     <OK>        <Cancel>    <Prev Page> <Next Page>
                 Administrative status for port 1.              | READ/SELECT
            Use <TAB> or arrow keys to move, <Space> to scroll options.
```

Parameter	Default	Description
Link Status		Indicates if the port has a valid connection to an external device.
Admin Status	Enabled	Allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also disable a port for security reasons.
Auto Negotiate	Enabled	Enables or disables auto-negotiation for port speed, duplex mode, and flow control.
Default Type	10HDX	If auto-negotiation is disabled, the port will be set to the indicated speed and duplex mode.
Current Type		Indicates the current speed and duplex mode.
Flow Control	Off	Used to enable or disable flow control. Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half duplex and IEEE 802.3x for full duplex. Note that flow control should not be used if a port is connected to a hub.
Jack Type	RJ-45	Shows the jack type for each port.

4.5.2.2 Using a Mirror Port for Analysis

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner. When mirroring port traffic, note that the target port must be included in the same VLAN as the source port. (See “Configuring Virtual LANs”)

You can use the Port Mirror Configuration screen to mirror one or more ports to the monitor port as shown below.



```
                    Layer 2 Menu: Mirror Port Configuration
                    ============


                    Port Mirroring : ENABLED

                Transmission Path
                    Mirrored Ports

         Tx: 3  4

         Rx: 3  4

                    Monitor Port Tx :  2
                    Monitor Port Rx :  2



            <Apply>            <OK>            <Add>
                    Confirm current screen setting.
            Use <TAB> or arrow keys to move. <Enter> to select.
```

Parameter	Description
Enable Port	Mirror Enables or disables the mirror function.
Mirrored Ports (Tx/Rx)	The port whose transmitted or received traffic will be mirrored. Press Add to specify mirrored ports.
Monitor Port	The port that will duplicate the transmitted or received traffic appearing on the mirrored port.

Note: You can mirror multiple ports to a single port to view traffic. However, note that some packets may be dropped for moderate to heavy loading.

4.5.2.3 Configuring Port Trunks

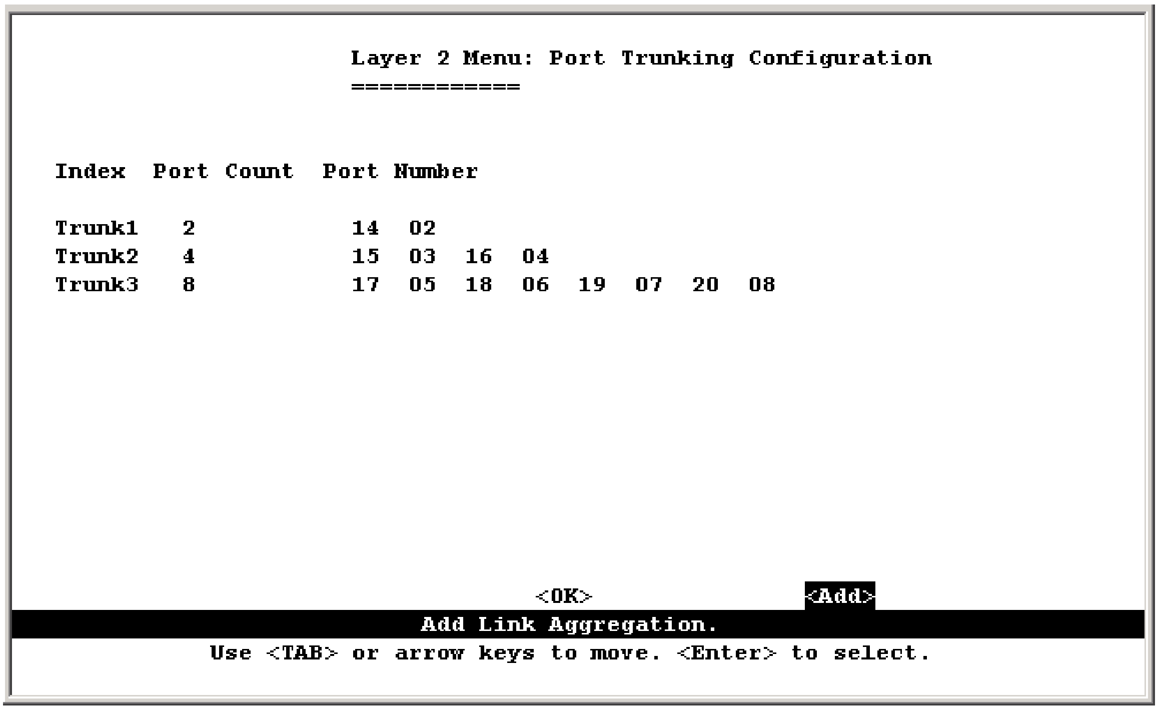
Ports can be combined into an aggregate link to increase the bandwidth of a network connection or ensure fault recovery. You can configure trunks between any two switches. The RJ-45 ports on this switch can be grouped into a trunk consisting of two, four or eight ports, creating an aggregate bandwidth up to 400, 800, 1600 or 4000 Mbps when operating at full duplex. Besides balancing the load across each port in the trunk, the additional ports provide redundancy by taking over the load if another port in the trunk should fail. However, before making any physical connections between devices, use the Port Trunking Configuration menu to specify the trunk on the devices at both ends. When using a port trunk, remember that::

• The ports used in a trunk must all be RJ-45. The ports that can be assigned to the same trunk are listed below:

Two ports as a trunk
<<13, 01>> <<14, 02>> <<15, 03>> <<16, 04>>
<<17, 05>> <<18, 06>> <<19, 07>> <<20, 08>>
<<21, 09>> <<22, 10>> <<23, 11>> <<24, 12>>
Four ports as a trunk
<<13, 01, 14, 02>> <<15, 03, 16, 04>>
<<17, 05, 18, 06>> <<19, 07, 20, 08>>
<<21, 09, 22, 10>> <<23, 11, 24, 12>>
Eight ports as a trunk
<<13, 01, 14, 02, 15, 03, 16, 04>>
<<17, 05, 18, 06, 19, 07, 20, 08>>
<<21, 09, 22, 10, 23, 11, 24, 12>>
Gigabit Ethernet Ports as a trunk
<<25, 26>>

- Ports can only be assigned to one trunk.
- The ports at both ends of a connection must be configured as trunk ports.
- The ports at both ends of a trunk must be configured in an identical manner, including communication mode, and VLAN assignments.
- None of the ports in a trunk can be configured as a mirror or monitor port.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- The Spanning Tree Algorithm will treat all the ports in a trunk as a whole.
- Enable the trunk prior to connecting any cable between the switches to avoid creating a loop.

You can use the Port Trunking Configuration screen to set up port trunks as shown below:



```
                     Layer 2 Menu: Port Trunking Configuration
                     ============

  Index  Port Count  Port Number

  Trunk1   2           14  02
  Trunk2   4           15  03  16  04
  Trunk3   8           17  05  18  06  19  07  20  08











                                   <OK>              <Add>
                            Add Link Aggregation.
              Use <TAB> or arrow keys to move. <Enter> to select.
```

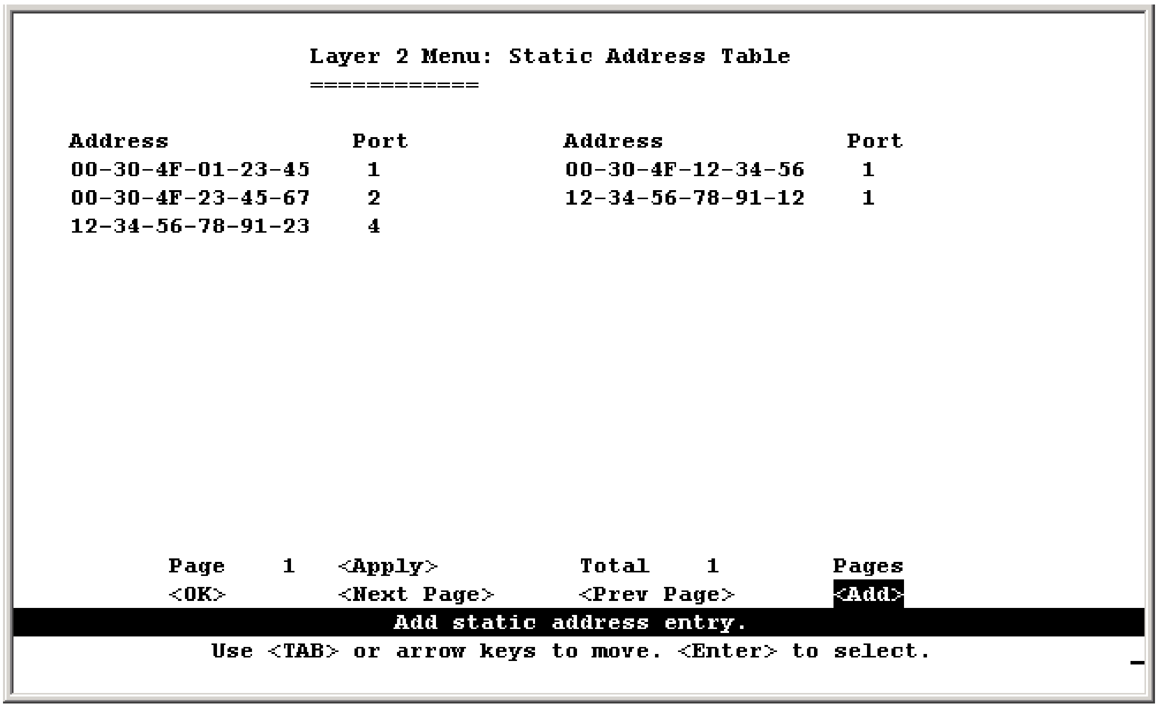
Parameter	Description
Trunk#	The trunk identifier.
Port Count	Trunks can contain 2, 4 or 8 ports.
Port Number	The ports assigned to each trunk.

To add a trunk, press <Add>. To delete a trunk, highlight the required entry and press Enter. Before disconnecting a port trunk, take the following steps:

- Before removing a port trunk via the configuration menu, you must disable all the ports in the trunk or remove all the network cables. Otherwise, a loop may be created.
- To disable a single link within a port trunk, you should first remove the network cable, and then disable both ends of the link via the configuration menu. This allows the traffic passing across that link to be automatically distributed to the other links in the trunk, without losing any significant amount of traffic.

4.5.2.4 Configuring the Static Unicast Address Table

The Static Unicast Address Table can be used to assign the MAC address for a host device to a specific port on this switch. Static unicast addresses are never aged out, and cannot be learned on another port. If any packets with a source address specified in this table enter another port, they will be dropped. The Static Unicast Address Table is described in the following figure and table.



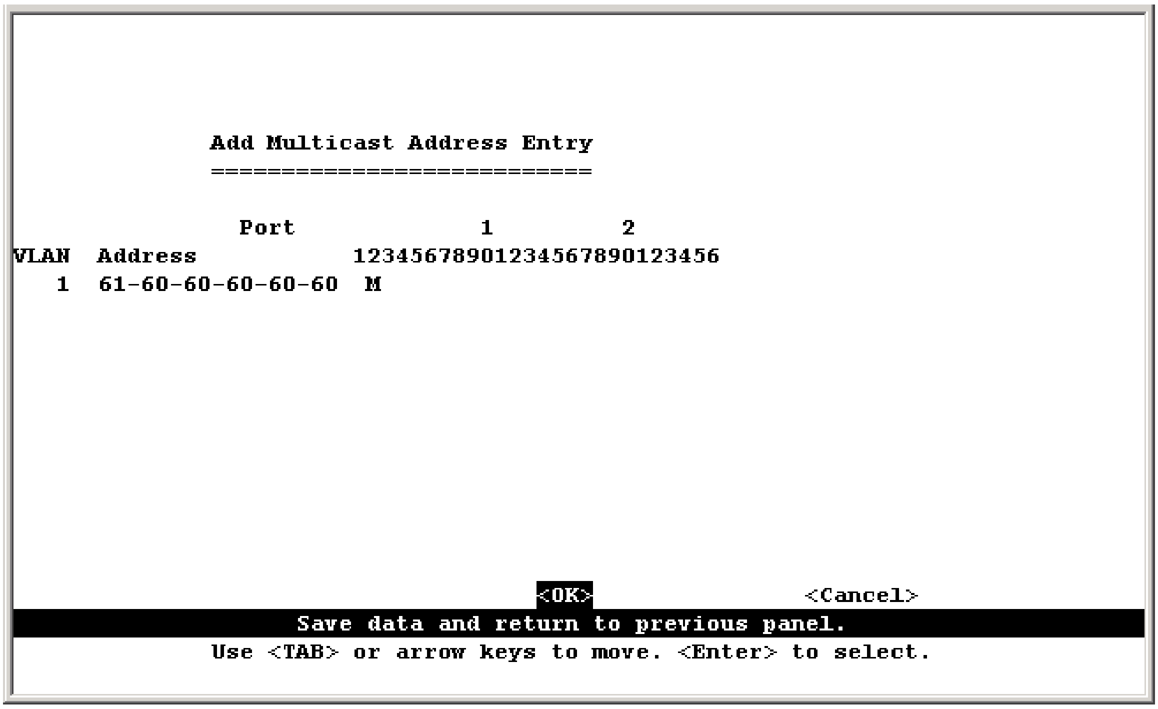
```
                    Layer 2 Menu: Static Address Table
                    ============

  Address             Port          Address             Port
  00-30-4F-01-23-45    1            00-30-4F-12-34-56    1
  00-30-4F-23-45-67    2            12-34-56-78-91-12    1
  12-34-56-78-91-23    4










          Page    1   <Apply>          Total    1        Pages
          <OK>        <Next Page>      <Prev Page>       <Add>
                           Add static address entry.
              Use <TAB> or arrow keys to move. <Enter> to select.
```

Parameter	Description
Address	The MAC address of a host device attached to this switch.
Port	The switch port the host device is attached to.

Note: To assign a MAC address to a specific port, use <Add>. To delete or modify an address, highlight it with the cursor and press Enter. To scroll through the address table, use the <Next Page> and <Prev Page> buttons. To display a specific page, set the page number in the Page field and then press <Apply>.

4.5.2.5 Configuring the Static Multicast Address Table

The Static Multicast Address Table can be used to assign a destination MAC address (and the corresponding ports) to the VLAN group used for a specific multicast service. Static multicast addresses are never aged out, and traffic with these addresses can only be forwarded to ports specified in this table.



```
              Add Multicast Address Entry
              ===========================

                Port            1         2
VLAN  Address          12345678901234567890123456
   1  61-60-60-60-60-60  M















                                     <OK>              <Cancel>
                    Save data and return to previous panel.
              Use <TAB> or arrow keys to move. <Enter> to select.
```

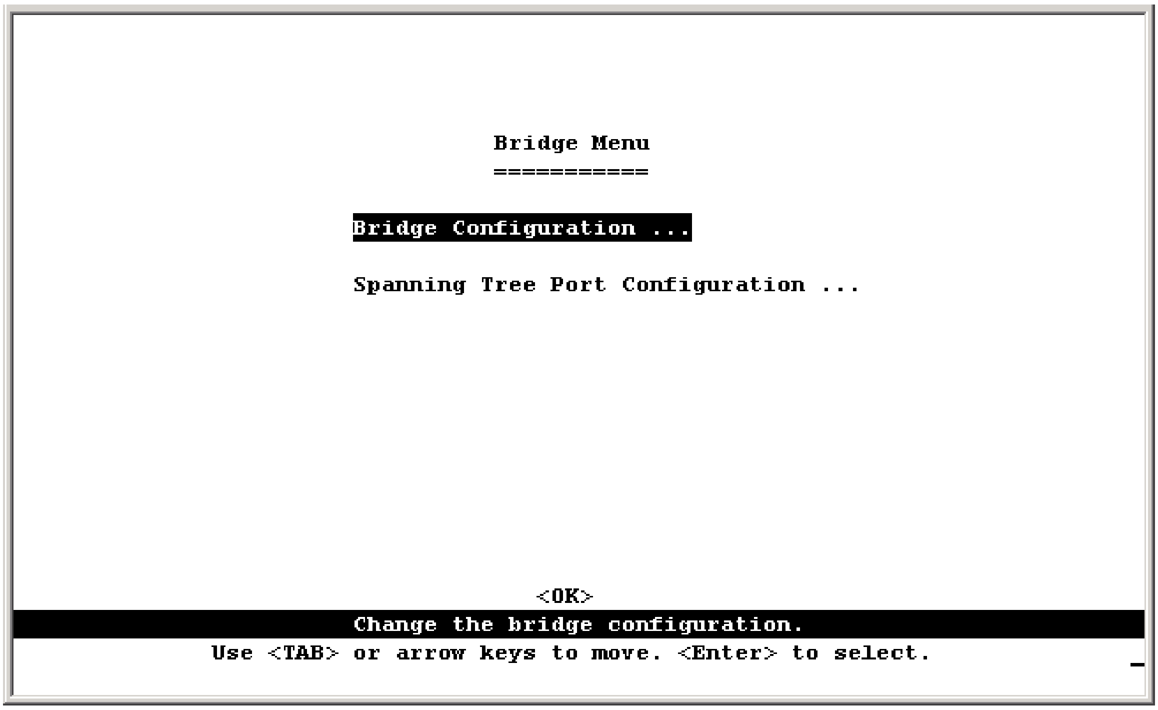
Parameter	Description
VLAN	The VLAN corresponding to this multicast service.
Address	The destination MAC address for a multicast service.
Port	The ports to which this multicast traffic can be forwarded.

Note: To assign a destination MAC address to one or more ports, use <Add>. To delete or modify an address, highlight it with the cursor and press Enter. To scroll through the address table, use the <Next Page> and <Prev Page> buttons. To display a specific page, set the page number in the Page field and then press <Apply>.

4.5.3 Using the Bridge Menu

The Bridge menu is used to display or configure settings for the Spanning Tree Algorithm, as well as the global bridge settings for GMRP (GARP Multicast Registration Protocol) and GVRP (GARP VLAN Registration Protocol), traffic classes priority threshold, and address aging time.

The Spanning Tree Algorithm can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links that automatically take over when a primary link goes down. For a more detailed description of how to use this algorithm, refer to “Spanning Tree Algorithm” on Chapter “Advanced Topics”.

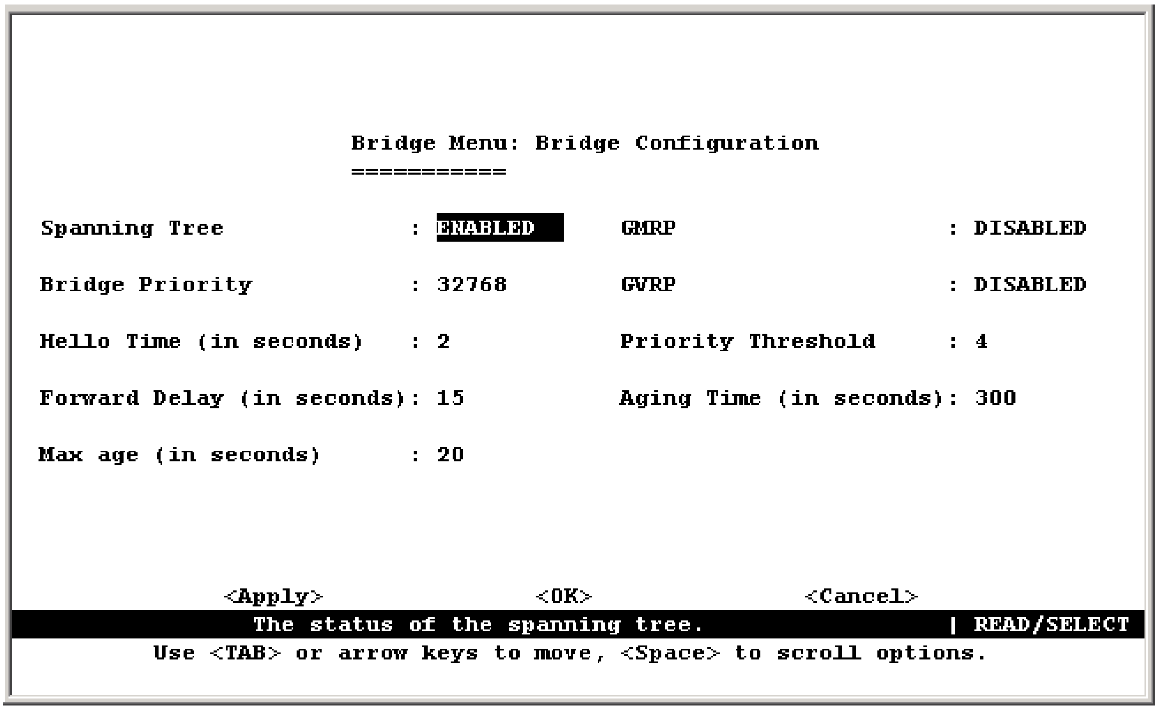


```
                         Bridge Menu
                         ===========

                    Bridge Configuration ...

                    Spanning Tree Port Configuration ...




                             <OK>
                 Change the bridge configuration.
          Use <TAB> or arrow keys to move. <Enter> to select.
```

Menu	Description
Bridge Configuration	Contains global bridge settings for STA (including bridge priority, hello time, forward delay, maximum message age), GMRP, GVRP, traffic class priority threshold, and address aging time.
Spanning Tree Port Configuration	Contains STA settings for individual ports, including port priority, path cost, and fast forwarding

4.5.3.1 Configuring Global Bridge Settings

The following figure and table describe bridge configuration for STA, GMRP, GVRP, priority threshold, and address aging time.



```
                    Bridge Menu: Bridge Configuration
                    ===========

 Spanning Tree            : ENABLED      GMRP                  : DISABLED

 Bridge Priority          : 32768        GVRP                  : DISABLED

 Hello Time (in seconds)  : 2            Priority Threshold    : 4

 Forward Delay (in seconds): 15          Aging Time (in seconds): 300

 Max age (in seconds)     : 20



              <Apply>              <OK>              <Cancel>
                 The status of the spanning tree.              | READ/SELECT
          Use <TAB> or arrow keys to move, <Space> to scroll options.
```

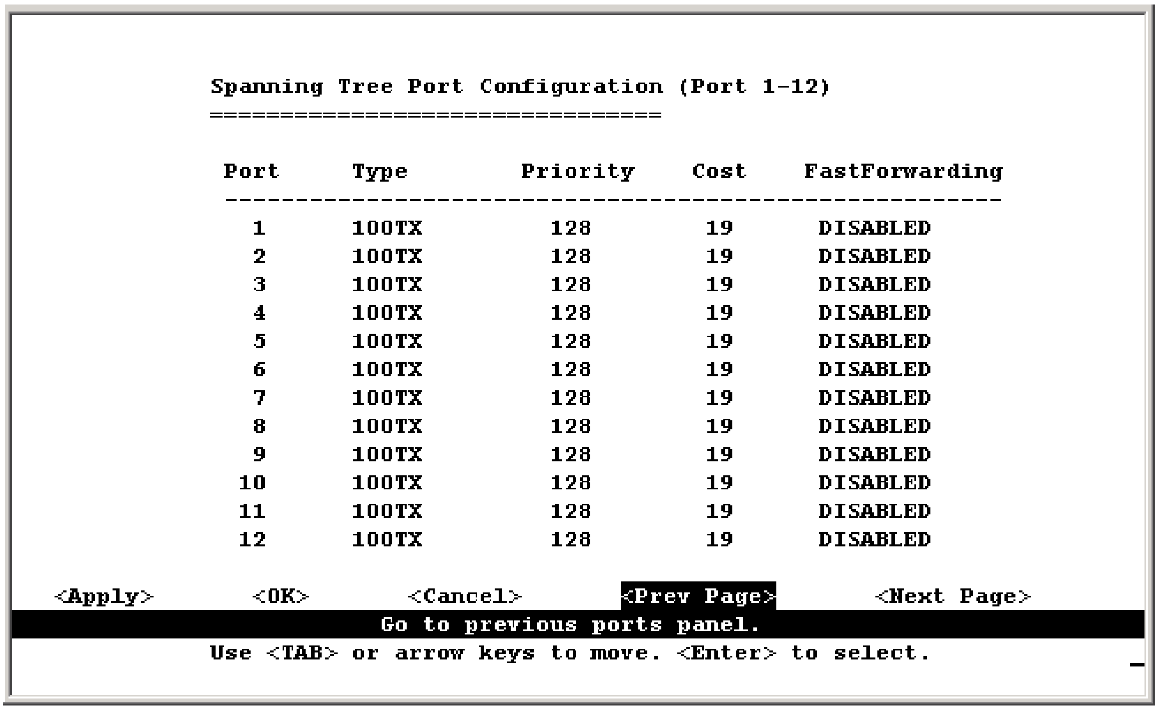
Parameter	Default	Description
Spanning Tree	Enabled	Enable this parameter to participate in a STA compliant network.
Bridge Priority	32,768	Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. Enter a value from 0 - 65535. Remember that the lower the numeric value, the higher the priority.
Hello Time	2	Time interval (in seconds) at which the root device transmits a configuration message. The minimum value is 1. The maximum value is the lower of 10 or [(Max. Message Age / 2) -1].
Forward Delay	15	The maximum time (in seconds) the root device will wait before changing states (that is, listening to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The maximum value is 30. The minimum value is the higher of 4 or [(Max. Message Age / 2) + 1].

Max (Message) Age	20	The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. The minimum value is the higher of 6 or [2 x (Hello Time + 1)]. The maximum value is the lower of 40 or [2 x (Forward Delay - 1)].
GMRP	Disabled	GARP Multicast Registration Protocol (GMRP) allows network devices to register end stations with multicast groups. If GMRP is globally enabled for the switch, then you can individually enable or disable GMRP for a specific port. See “4.5.4.1 VLAN Port Configuration”. IGMP and IGMP Snooping also provide multicast filtering. For multilayer mode, the full IGMP protocol set is automatically enabled/disabled along with DVMRP. (See “6.4.2 IGMP Protocol”, “ 4.5.6.1.5 Configuring DVMRP” and “4.5.5 Configuring IGMP Snooping” .)
GVRP	Disabled	GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. This function should be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch. If GVRP is globally enabled for the switch, then you can individually enable or disable GVRP for a specific port. See “4.5.4.1 VLAN Port Configuration”.
Priority Threshold*	4	This switch supports Quality of Service (QoS) by using two priority queues, with Weighted Fair Queuing for each port. Up to 8 separate traffic classes are defined in IEEE 802.1p. So any packets with a priority equal to or higher than this threshold are placed in the high priority queue.
(Address) Aging Time	300	Time-out period in seconds for aging out dynamically learned forwarding information. Range: 10 - 1000000 seconds

* You can use “ 4.5.4.1 VLAN Port Configuration” to configure the default priority for each port.

4.5.3.2 Configuring STA for Ports

The following figure and table describe port STA configuration.



```
              Spanning Tree Port Configuration (Port 1-12)
              ================================

               Port     Type        Priority    Cost    FastForwarding
               -------------------------------------------------------
                 1      100TX         128        19      DISABLED
                 2      100TX         128        19      DISABLED
                 3      100TX         128        19      DISABLED
                 4      100TX         128        19      DISABLED
                 5      100TX         128        19      DISABLED
                 6      100TX         128        19      DISABLED
                 7      100TX         128        19      DISABLED
                 8      100TX         128        19      DISABLED
                 9      100TX         128        19      DISABLED
                10      100TX         128        19      DISABLED
                11      100TX         128        19      DISABLED
                12      100TX         128        19      DISABLED

   <Apply>       <OK>       <Cancel>       <Prev Page>       <Next Page>
                         Go to previous ports panel.
              Use <TAB> or arrow keys to move. <Enter> to select.
```

Parameter	Default	Description
Type		Shows port type as: 100TX : 10BASE-T / 100BASE-TX 1000T : 1000BASE-T
Priority	128	Defines the priority for the use of a port in the STA algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (that is, lowest value) will be configured as an active link in the Spanning Tree. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. The range is 0 - 255.
(Path) Cost	100/19/4	This parameter is used by the STA algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) The default and recommended range is: Ethernet: 100 (50~600) Fast Ethernet: 19 (10~60) Gigabit Ethernet: 4 (3~10) The full range is 0 - 65535.
Fast Forwarding*	Disabled	This parameter is used to enable/disabled the Fast Spanning Tree mode for the selected port. In this mode, ports skip the Blocked, Listening and Learning states and proceed straight to Forwarding.

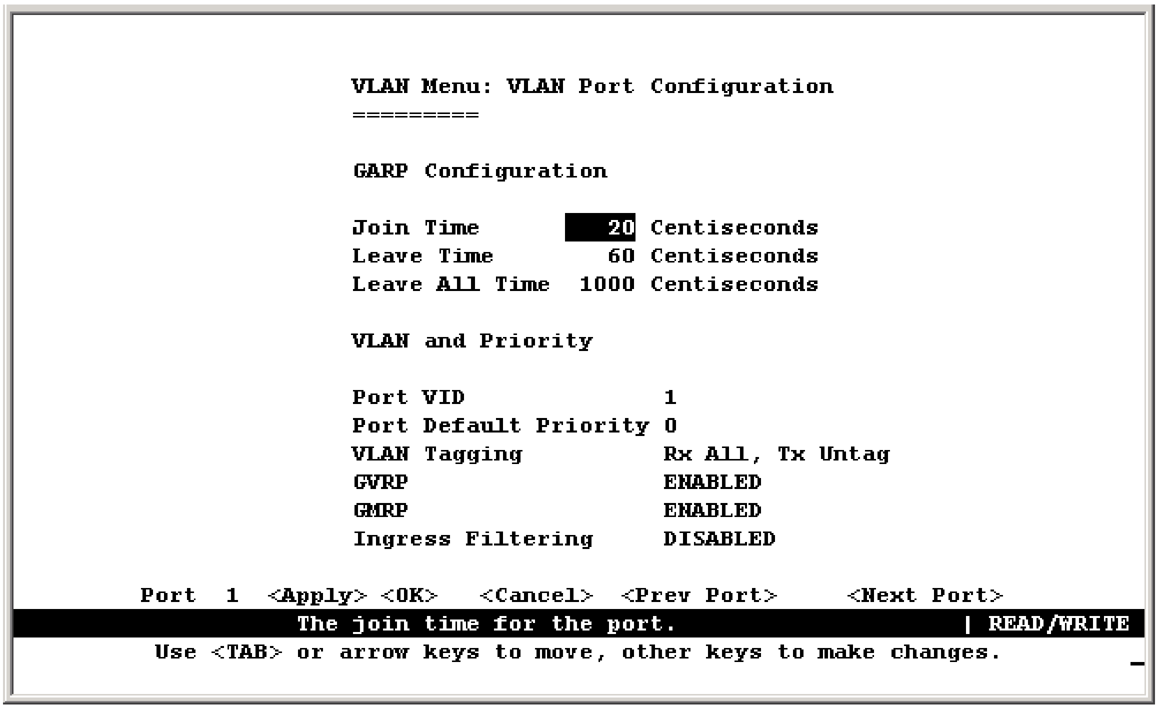
* Since end-nodes cannot cause forwarding loops, they can pass through the Spanning Tree state changes more quickly than allowed by standard convergence time. Fast Forwarding can achieve quicker convergence for end-node workstations and servers, and also overcome other STA related time-out problems. (Remember that Fast Forwarding should only be enabled for ports connected to an end-node device.)

4.5.4 Configuring Virtual LANs

You can use the VLAN configuration menu to assign any port on the switch to any of up to 256 Virtual LAN groups. In conventional networks with routers, broadcast traffic is split up into separate domains. Switches do not inherently support broadcast domains. This can lead to broadcast storms in large networks that handle traffic such as IPX or NetBEUI. By using IEEE 802.1Q compliant VLANs, you can organize any group of network nodes into separate broadcast domains, confining broadcast traffic to the originating group. This also provides a more secure and cleaner network environment. For more information on how to use VLANs, see “6.3 Virtual LANs”. The VLAN configuration screens are described in the following sections.

4.5.4.1 VLAN Port Configuration

You can use the VLAN Port Configuration screen to configure GARP, the default VLAN identifier, default port priority, VLAN tagging on the attached link, GVRP and GMRP status, and filtering of incoming frames for VLAN groups to which this port does not belong.



```
                    VLAN Menu: VLAN Port Configuration
                    =========

                    GARP Configuration

                    Join Time           20 Centiseconds
                    Leave Time          60 Centiseconds
                    Leave All Time    1000 Centiseconds

                    VLAN and Priority

                    Port VID              1
                    Port Default Priority 0
                    VLAN Tagging          Rx All, Tx Untag
                    GVRP                  ENABLED
                    GMRP                  ENABLED
                    Ingress Filtering     DISABLED

       Port  1  <Apply> <OK>   <Cancel>  <Prev Port>     <Next Port>
                  The join time for the port.                    | READ/WRITE
          Use <TAB> or arrow keys to move, other keys to make changes.
```

Parameter	Default	Description
GARP *1		Group Address Registration Protocol is used by GVRP and GMRP to register or deregister client attributes for client services within a bridged LAN.
Join Time	20	The interval (centiseconds) between transmitting requests/queries to participate in a group.
Leave Time	60	The interval (centiseconds) a port waits before leaving a group. This time should be set to more than twice the Join Time. This ensures that after a Leave or LeaveAll message has been issued, the applicants can re-join before the port actually leaves the group.
Leave All Time	1000	The interval (centiseconds) between sending out a LeaveAll query message for group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group.

1: The default values for the GARP timers are independent of the media access method or data rate. These values should not changed unless you are experiencing some difficulties with GMRP or GVRP registration/deregistration.

Parameter	Default	Description
VLAN and Priority		These fields set the default values for VLANs, port priority, GVRP and GMRP.
Port VID	1	The VLAN ID assigned to untagged frames received on this port.
Port Default Priority *2	0	Set the default ingress priority to any value beneath the priority threshold to specify the low priority queue, or to any value equal to or above this threshold to specify the high priority queue.
VLAN Tagging *3	Layer 2 - Rx All, Tx All Multilayer - Rx All, Tx Untag	Indicates whether or not VLAN tags will be included on frames passing through this port. The options include: Rx All: Accepts all frames, tagged or untagged. Rx Untag: Only accepts untagged frames. Tx All: If PVID and frame tag are same, sends tagged frame, otherwise sends untagged. Tx Untag: Sends only untagged frames.

2: This switch supports Quality of Service (QoS) by using two priority queues, with Weighted Fair Queuing for each port. Inbound frames that do not have VLAN tags are tagged with the input port' s default ingress user priority, and then placed in the appropriate priority queue at the output port. The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in the low priority queue of the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.)

3: If you want to create a small port-based VLAN for just one or two switches, you can assign ports to the same untagged VLAN (and use a separate connection where a VLAN crosses the switches). However, to participate in a VLAN group that extends beyond this switch, we recommend using the VLAN ID for that group (using VLAN tagging for Layer 2 mode, or a common PVID for multilayer mode).

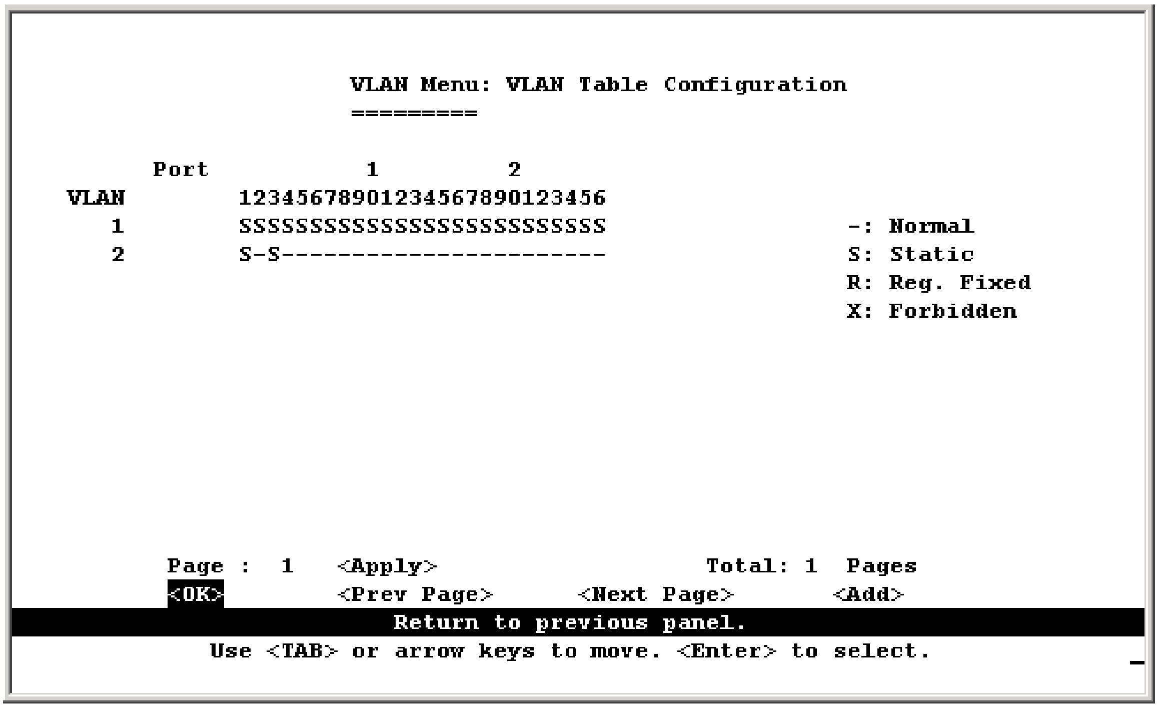
When operating the switch in Layer 2 mode, ports assigned to a large VLAN group that crosses several switches must use VLAN tagging. But when operating in multilayer mode, this switch does not currently support tagging, so you should set the PVID to the same value at both ends of the link (if the device you are attaching to is VLAN-aware), and configure an IP interface for this VLAN if you need to connect it to other group. (This limitation will be removed for future firmware versions.)

Parameter	Default	Description
GVRP	Enabled	Enables or disables GVRP for this port. When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports. Note that GVRP must be enabled globally for the switch before this setting can take effect. (See "4.5.3.1 Configuring Global Bridge Settings")
GMRP	Enabled	Enables or disables GMRP for this port. When enabled, this port will allow end stations to register with multicast groups using GMRP. Note that GMRP must be enabled for the switch before this setting can take effect. IGMP and IGMP Snooping also provide multicast filtering. (See "6.4.2 IGMP Protocol")
Ingress Filtering *4	Disabled	If enabled, incoming frames for VLANs which do not include this ingress port in their member set will be discarded at the ingress port.

4: This control does not affect VLAN independent BPDU frames, such as GVRP or STP. However, they do affect VLAN dependent BPDU frames, such as GMRP.

4.5.4.2 VLAN Table Configuration

Use this screen to create a new VLAN or modify the settings for an existing VLAN.



```
                        VLAN Menu: VLAN Table Configuration
                        =========

          Port           1         2
    VLAN        12345678901234567890123456
       1        SSSSSSSSSSSSSSSSSSSSSSSSSS                    -: Normal
       2        S-S-----------------------                    S: Static
                                                              R: Reg. Fixed
                                                              X: Forbidden










           Page :  1   <Apply>                   Total: 1  Pages
           <OK>        <Prev Page>      <Next Page>       <Add>
                           Return to previous panel.
              Use <TAB> or arrow keys to move. <Enter> to select.
```

Parameter	Description
VLAN	The ID for the VLAN currently displayed. Range: 1-4094
Port	Port entries may be marked as: - : (Normal) Uses GVRP to determine port membership. S : (Static) Adds port as a static entry. GVRP protocol is disabled. R : (Registration Fixed) Adds port as a static entry. GVRP protocol messages are still forwarded through this port. X : (Forbidden) Disables GVRP for this VLAN on the specified port. If a removed port is no longer assigned to any other group as an untagged port, it will automatically be assigned to VLAN group 1 as untagged.

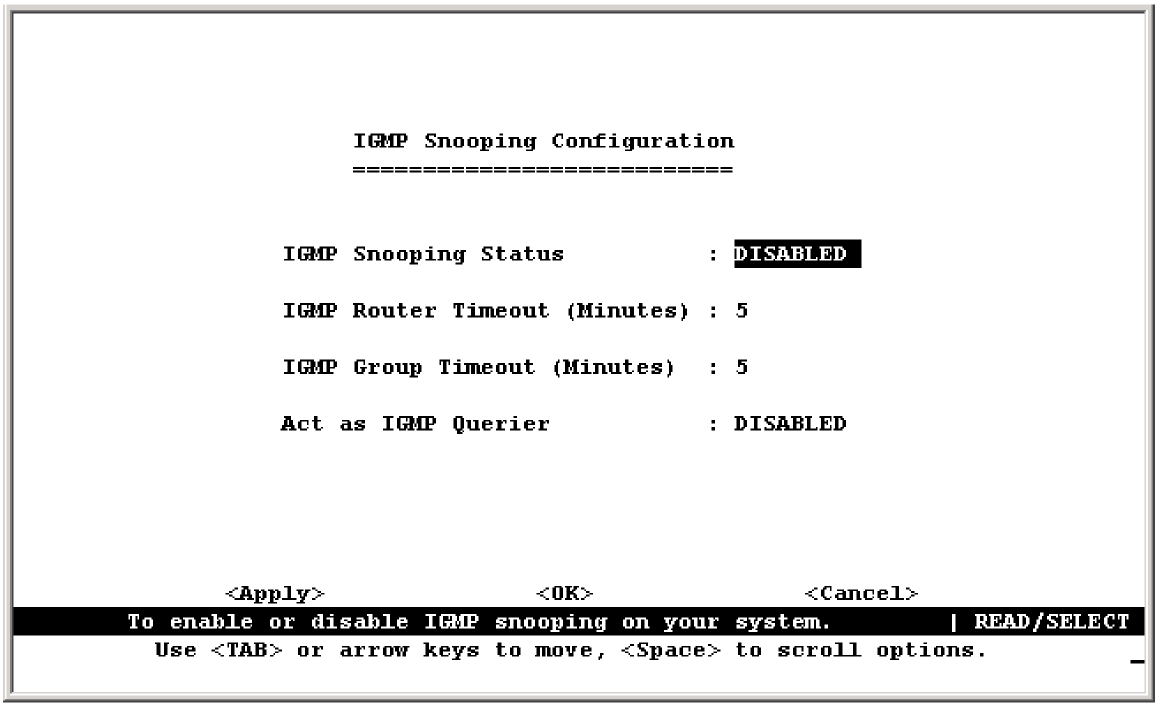
Note: Use the <Next Page> and <Prev Page> buttons to scroll through the table. To display a specific page, set the page number in the Page field and press <Apply>. To modify a VLAN group, highlight the entry in the table and press Enter. To add a VLAN group, press <Add>.

4.5.5 Configuring IGMP Snooping

Multicasting is used to support real-time applications such as video conferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network; and any hosts which want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast switch/router it passes through to ensure that traffic is only passed on to the hosts which subscribed to this service.

This switch uses IGMP (Internet Group Management Protocol) Snooping to monitor any attached hosts which want to receive a specific multicast service. It looks up the IP Multicast Group used for this service, and adds any port which received a similar request to that group.

You can use the IGMP Snooping Configuration screen to configure multicast filtering shown below.



```
                    IGMP Snooping Configuration
                    ===========================

               IGMP Snooping Status          : DISABLED

               IGMP Router Timeout (Minutes) : 5

               IGMP Group Timeout (Minutes)  : 5

               Act as IGMP Querier           : DISABLED


          <Apply>              <OK>               <Cancel>
      To enable or disable IGMP snooping on your system.        | READ/SELECT
        Use <TAB> or arrow keys to move, <Space> to scroll options.
```

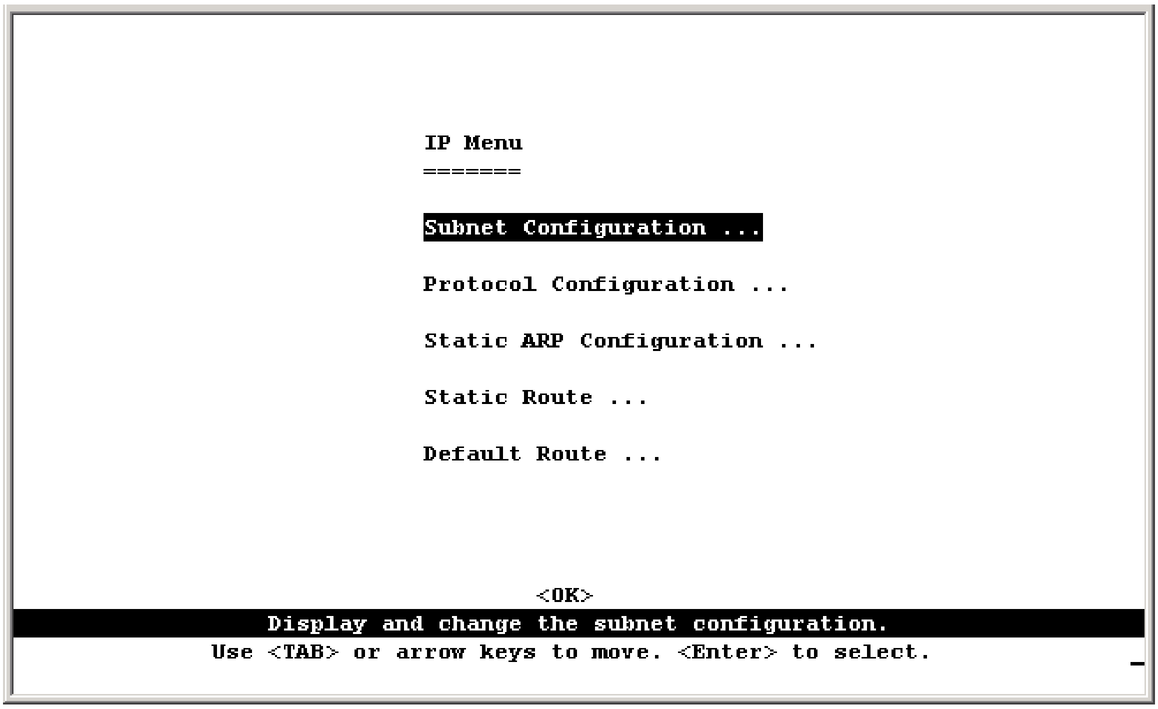
Parameter	Default	Description
IGMP Snooping Status*1	Disabled	If enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. This is also referred to as IGMP Snooping.
IGMP Router Timeout	5	A switch port that stops receiving multicast protocol packets for this interval will be removed from the IGMP forwarding list. Range: 3 - 5 minutes
IGMP Group Timeout	5	The time between last spotting an IGMP Report message for an IP multicast address on a specific port and the switch removing that entry from its list. Range: 3 - 5 minutes
Act as IGMP Querier*2	Disabled	If enabled, the switch can serve as the “querier,” which is responsible for asking hosts is they want to receive multicast traffic.

1: This item is only displayed for Layer 2 mode. For multilayer mode, the full IGMP protocol set is automatically enabled/disabled along with DVMRP. (See “6.4 Multicast Filtering” and “4.5.6.1.5 Configuring DVMRP”.)

2: This item is only displayed for Layer 2 mode. When IGMP is enabled for multilayer mode, the switch will always serve as the querier if elected.

4.5.6 Configuring IP Settings

If this switch is set to multilayer mode (see 4.5.1 Setting the System Operation Mode), the IP Menu will be displayed. Use this menu to configure the IP subnets for each VLAN on your switch, the unicast and multicast routing protocols, static ARP entries, static IP routes, and the default IP Route.

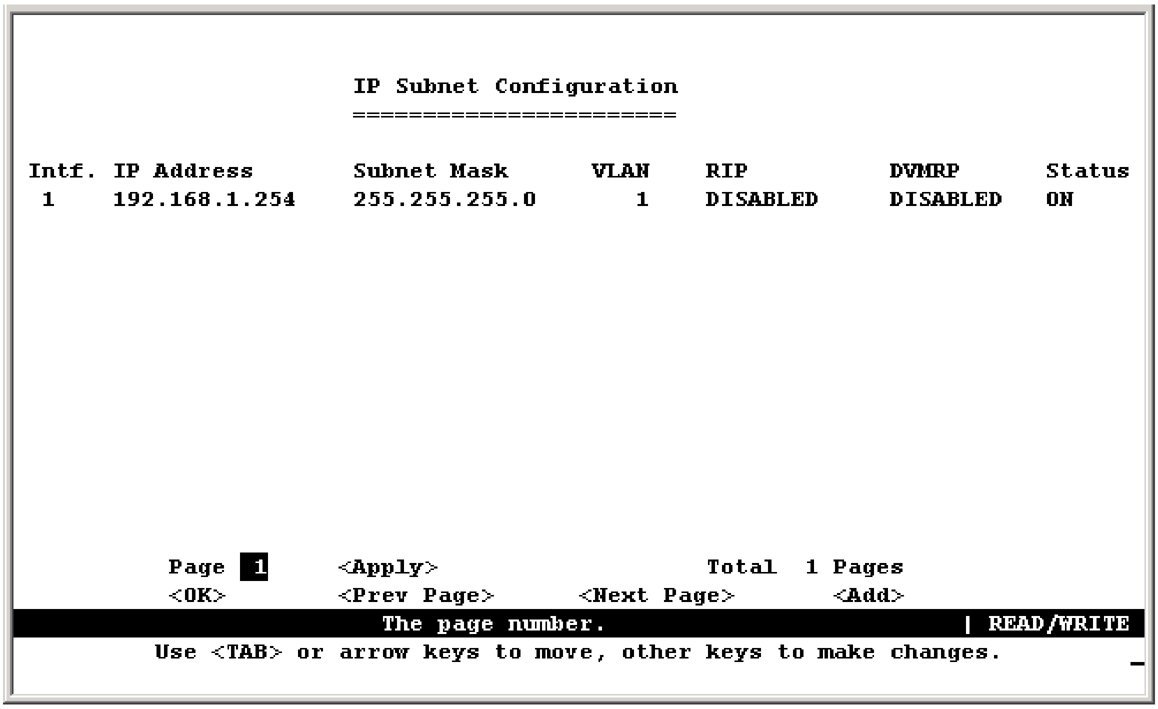


```
IP Menu
=======

Subnet Configuration ...

Protocol Configuration ...

Static ARP Configuration ...

Static Route ...

Default Route ...

<OK>
Display and change the subnet configuration.
Use <TAB> or arrow keys to move. <Enter> to select.
```

Parameter	Description
Subnet Configuration	Specifies the IP interface for VLANs configured on this switch, including the subnet address and routing Protocols
Protocol Configuration	Configures ARP timeout, enables Proxy ARP, sets the preferred servers for BOOTP/DHCP Relay, as well as enabling/configuring unicast and multicast protocols globally for this switch.
Static ARP Configuration	Used to map an IP address to a specific physical MAC address
Static Route	Used to configure static routes to other IP networks, subnetworks, or hosts.
Default Route	Defines the router to which this switch will forward all traffic for unknown networks.

4.5.6.1 Subnet Configuration

Use this menu to specify an IP interface for any VLAN configured on this switch that needs to communicate with a device outside of its own group (that is, another network segment). You also need to define a VLAN for each IP subnet connected directly to this switch. Note that you must first create a VLAN as described under “Configuring Virtual LANs” before configuring the corresponding subnet. If you need to manage the switch in-band then you must define the IP subnet address for at least one VLAN.



```
                      IP Subnet Configuration
                      =======================

Intf. IP Address        Subnet Mask       VLAN    RIP          DVMRP       Status
 1    192.168.1.254     255.255.255.0        1    DISABLED     DISABLED    ON









          Page 1      <Apply>                     Total  1 Pages
          <OK>        <Prev Page>      <Next Page>        <Add>
                        The page number.                         | READ/WRITE
         Use <TAB> or arrow keys to move, other keys to make changes.
```

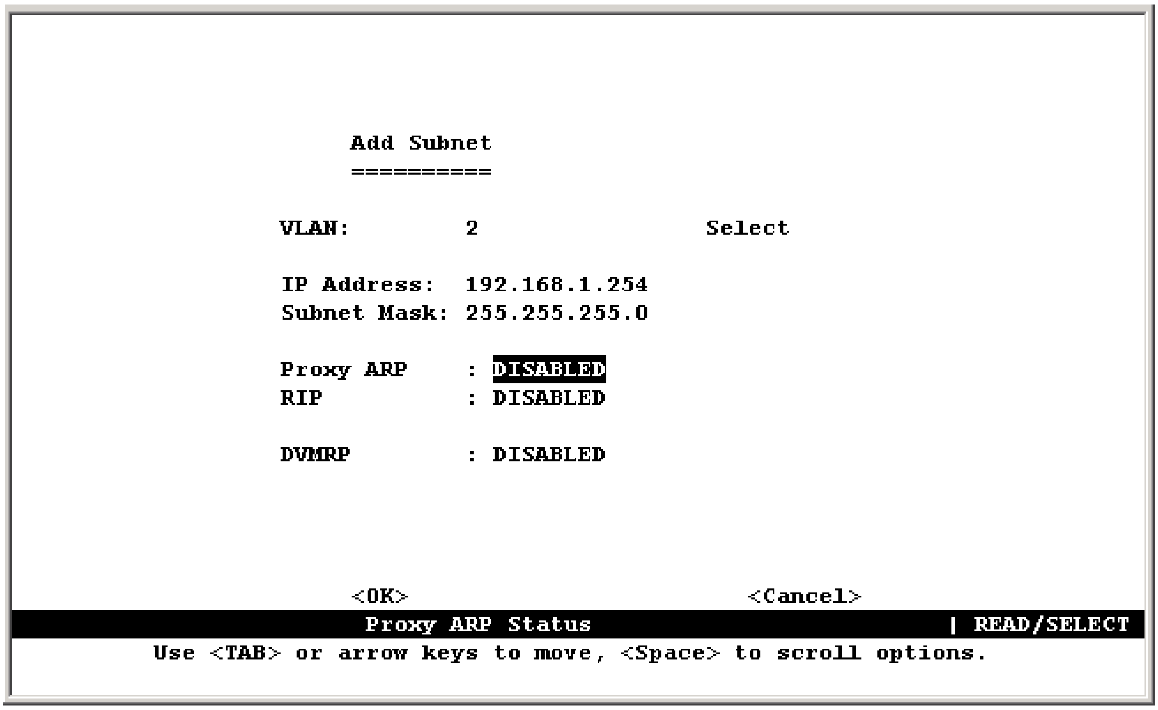
Parameter	Description
IP Address	The IP address associated with the specified VLAN interface. In general, it is the router IP address for the specified VLAN members. By convention, the last three digits should be set to “254” to readily distinguish this device as a router port.
Subnet Mask	A template that identifies the address bits in the host address used for routing to specific subnets. Each bit that corresponds to a “1” is part of the network / subnet number; and each bit that corresponds to “0” is part of the host number.
VLAN	The VLAN associated with this IP interface.
RIP	Routing Information Protocol for unicast routing.
DVMRP	Distance-Vector Multicast Routing Protocol.

Note: Use the <Next Page> and <Prev Page> buttons to scroll through the subnet configuration table. To display a specific page, set the page number in the Page field and then press <Apply>. To modify an IP interface, highlight the entry in the table and press Enter. To add an IP interface, press <Add>.

4.5.6.1.1 Adding an IP Interface

Select <Add> on the Subnet Configuration menu to add an IP interface. When the Add Subnet screen opens as shown below, assign a VLAN group to this interface, configure the IP address, and then enable the required routing protocols. You can specify a VLAN that has already been configured on this switch or press “Select” to open the Port Group Configuration screen and create or modify a VLAN group.

To configure the unicast or multicast routing protocols, select the IP address for a specific interface from the Subnet Configuration menu, and then select “Advanced” configuration from the Modify Subnet screen.

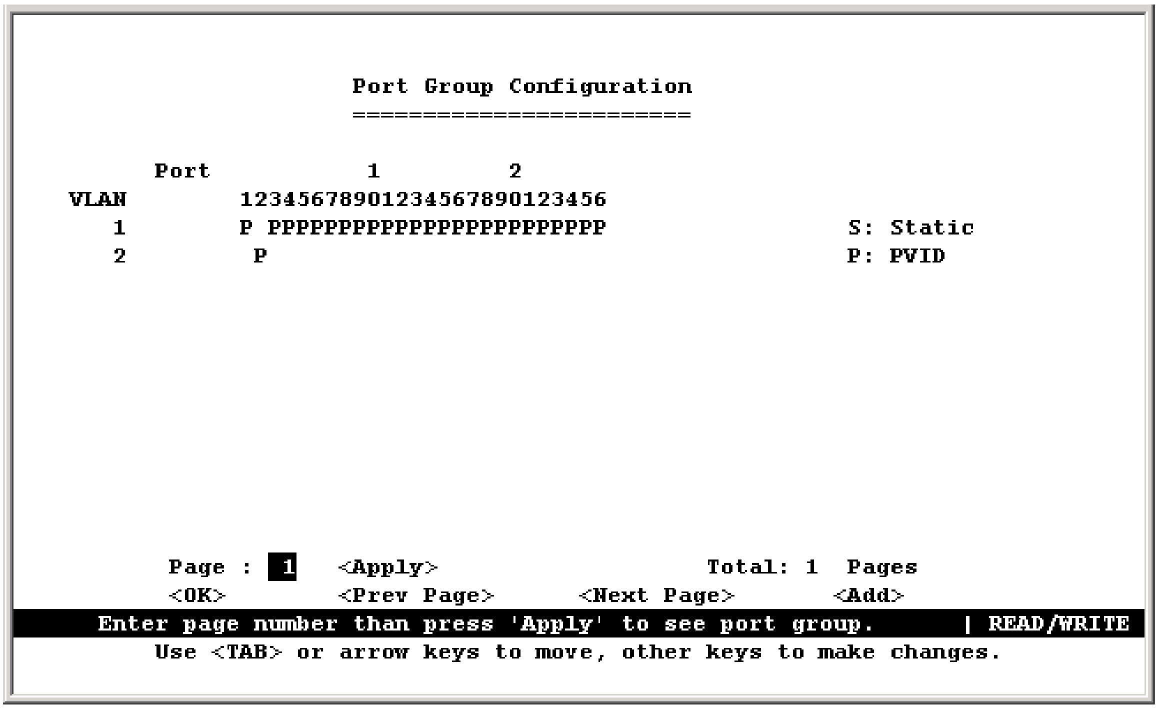


```
                    Add Subnet
                    ==========

               VLAN:        2                Select

               IP Address:  192.168.1.254
               Subnet Mask: 255.255.255.0

               Proxy ARP    : DISABLED
               RIP          : DISABLED

               DVMRP        : DISABLED



                    <OK>                        <Cancel>
                     Proxy ARP Status                       | READ/SELECT
          Use <TAB> or arrow keys to move, <Space> to scroll options.
```

Parameter	Description
VLAN	The VLAN associated with this IP interface.
Select	Use this option to create or modify a VLAN under the “Port Group Configuration” menu.
IP Address	The IP address associated with the specified VLAN interface. In general, it is the router IP address for the specified VLAN members.
Subnet Mask	A template that identifies the address bits in the host address used for routing to specific subnets. Each bit that corresponds to a “1” is part of the network / subnet number; and each bit that corresponds to“0” is part of the host number.
Proxy ARP	Enables or disables Proxy ARP for the interface. This feature allows the switch forward an ARP request from a node in the attached subnetwork (that does not have routing or a default gateway configured) to a remote subnetwork. (See “6.2.5 Proxy ARP”.) Note that Proxy ARP must be enabled globally for the switch before this setting can take effect. (See “ 4.5.6.2 Protocol Configuration”.)
RIP	Routing Information Protocol for unicast routing.
DVMRP	Distance-Vector Multicast Routing Protocol.

4.5.6.1.2 Configuring Port Groups

You can create a new VLAN group or modify the members of an existing group by pressing "Select" on the Add Subnet screen.



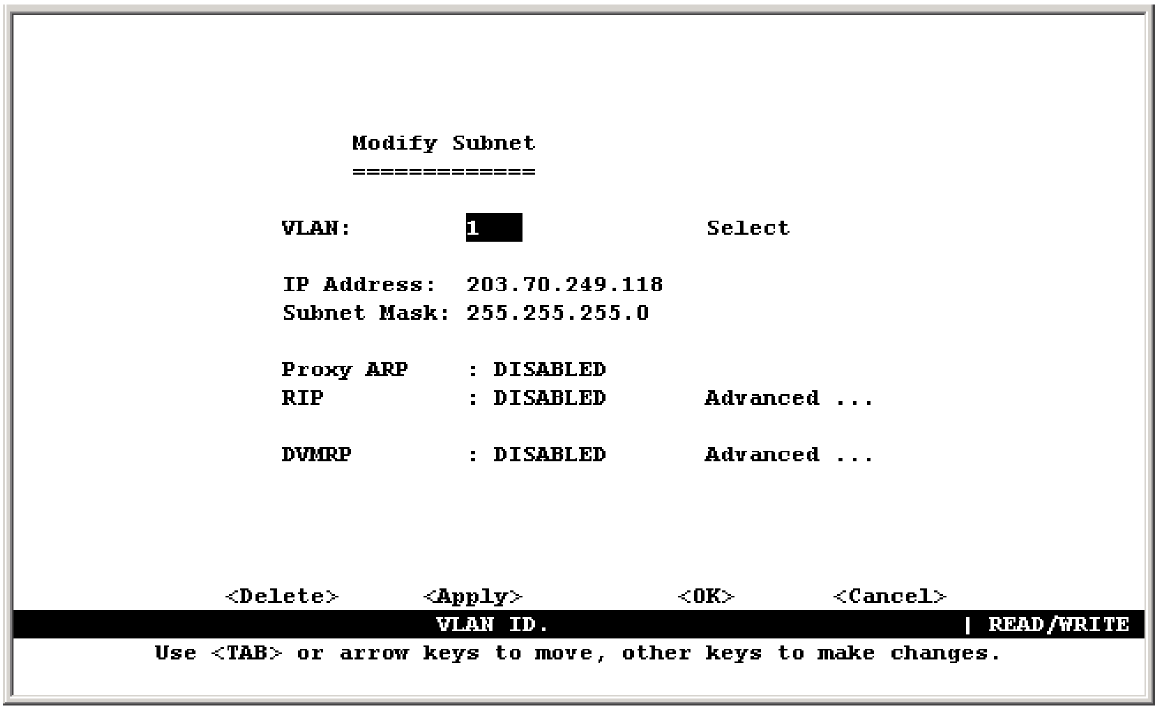
```
                    Port Group Configuration
                    ========================

          Port            1         2
     VLAN        12345678901234567890123456
        1        P PPPPPPPPPPPPPPPPPPPPPPPP                S: Static
        2         P                                        P: PVID









           Page :  1    <Apply>                 Total: 1  Pages
           <OK>         <Prev Page>      <Next Page>       <Add>
     Enter page number than press 'Apply' to see port group.       | READ/WRITE
          Use <TAB> or arrow keys to move, other keys to make changes.
```

Parameter	Description
VLAN	A VLAN already configured on this switch.
Port	Port entries may be marked as: S : Adds port as a static entry. P : Adds port as a static entry, and sets the port's PVID to this VLAN ID.

Note: Use the <Next Page> and <Prev Page> buttons to scroll through the table. To display a specific page, set the page number in the Page field and then press <Apply>. To modify a VLAN, highlight the entry in the table and press Enter. To add a new VLAN, press <Add>.

4.5.6.1.3 Modifying an IP Interface

To modify an IP interface, first highlight the IP address in the Subnet Configuration menu, and then press Enter. The Modify Subnet screen is nearly the same as the Add Subnet screen. However, it also includes an “Advanced” option that allows you to configure the unicast and multicast routing protocols as described in the following sections.

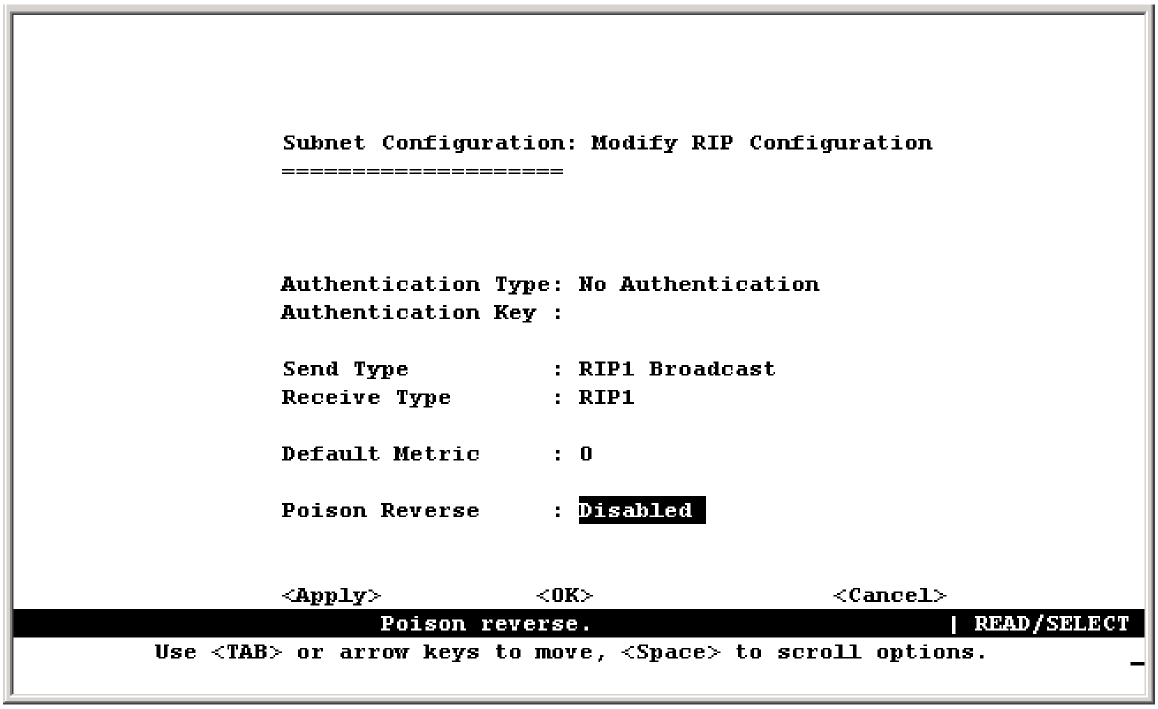


```
                    Modify Subnet
                    =============

               VLAN:         1               Select

               IP Address:   203.70.249.118
               Subnet Mask:  255.255.255.0

               Proxy ARP    : DISABLED
               RIP          : DISABLED       Advanced ...

               DVMRP        : DISABLED       Advanced ...



          <Delete>      <Apply>          <OK>       <Cancel>
                             VLAN ID.                           | READ/WRITE
        Use <TAB> or arrow keys to move, other keys to make changes.
```

4.5.6.1.4 Configuring RIP

The Routing Information Protocol is used to specify how routers exchange routing table information. (See "RIP and RIP-2 Dynamic Routing Protocols" on Chapter "Advanced Topics".) When RIP is enabled on this routing switch, it broadcasts RIP messages to all devices in the network every 30 seconds, and updates its own routing table when RIP messages are received from other routers. RIP messages contain both the IP address and a metric for each destination network it knows about, where the metric indicates the number of hops from this device to the destination network.

You can use the following menu to specify authentication, the protocol used for sending or receiving routing messages on this port, the default metric used in calculating the best path, and enable or disable Poison Reverse.



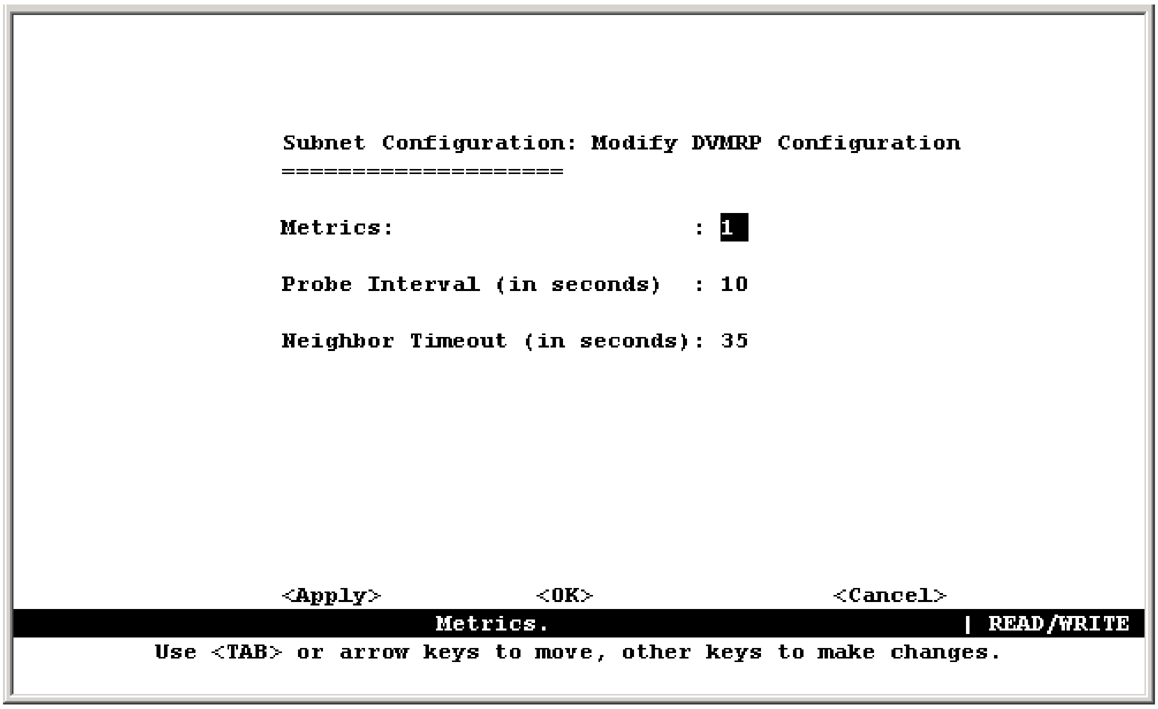
```
                   Subnet Configuration: Modify RIP Configuration
                   ====================



                   Authentication Type: No Authentication
                   Authentication Key :

                   Send Type          : RIP1 Broadcast
                   Receive Type       : RIP1

                   Default Metric     : 0

                   Poison Reverse     : Disabled


                   <Apply>          <OK>                  <Cancel>
                         Poison reverse.                         | READ/SELECT
              Use <TAB> or arrow keys to move, <Space> to scroll options.
```

Parameter	Description
Authentication Type	Authentication can be used to ensure that routing information comes from a valid source.
Authentication Key	A simple password must be provided if authentication is enabled. (An authentication string is case sensitive, and can be up to 16 characters.)
Send Type	The protocol used for traffic sent out this port: RIP1 Broadcast —Route information is broadcast to other routers on the network using RIPv1. RIP2 Broadcast —Route information is broadcast to other routers on the network using RIPv2. RIP2 Multicast —Route information is multicast to other routers on the network using RIPv2. Do Not Send —The switch will passively monitor route information advertised by other routers attached to the network.
Receive Type	The routing protocol messages accepted on this port includes RIP1, RIP2, RIP1/RIP2, or Disabled (i.e., none received).
Default Metric	A “metric” indicates the number of hops between the switch and the destination network. The “default metric” is used for the default route in RIP updates originated on this interface. A value of zero indicates that no default route should be originated; in this case, a default route via another router may be propagated. Range: 0-15
Poison Reverse*	Propagates routes back to an interface port from which they have been acquired, but sets the distance vector metrics to infinity.

* This is a method of preventing routing information from looping back to the source. Note that Split Horizon is also enabled on this switch for this purpose. (See “6.2.6.1 RIP and RIP-2 Dynamic Routing Protocols”.)

4.5.6.1.5 Configuring DVMRP

Distance Vector Multicast Routing Protocol is used to route multicast traffic to nodes which have requested a specific multicast service via IGMP. (See "6.4.4 DVMRP Routing Protocol") To configure DVMRP, you must specify the routing metric, probe interval, and neighbor router timeout.



```
Subnet Configuration: Modify DVMRP Configuration
====================

Metrics:                      : 1

Probe Interval (in seconds)   : 10

Neighbor Timeout (in seconds): 35
```

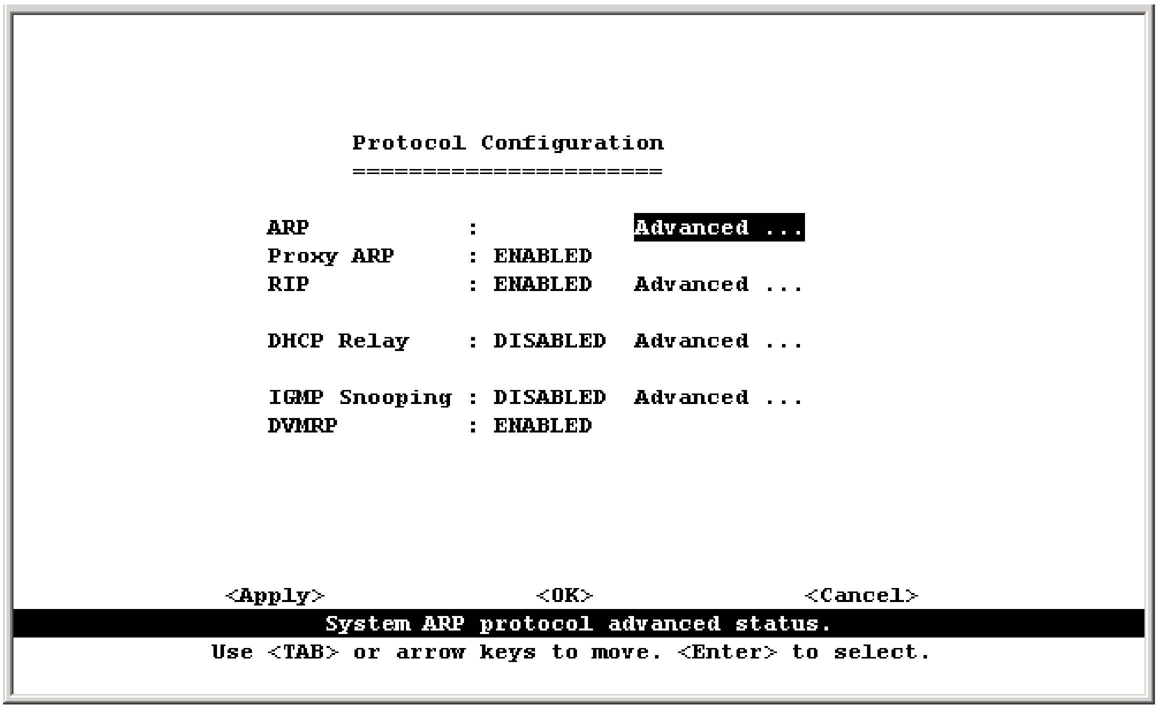
<Apply>
<OK>
<Cancel>
Metrics.
| READ/WRITE
Use <TAB> or arrow keys to move, other keys to make changes.

Parameter	Default	Description
Metrics	1 hop	This value is used to select the best reverse path to networks that are connected directly to an interface on this switch. Range: 1-31 hops
Probe Interval	10 seconds	The interval between sending neighbor probe messages to the multicast group address for all DVMRP routers. Range: 5-30 seconds
Neighbor Timeout	35 seconds	The interval to wait without hearing from a DVMRP neighbor before declaring it dead. This is used for timing out routes, and for setting the children and leaf flags. Range: 10-8000 seconds

Note: IGMP is automatically enabled/disabled along with DVMRP. (See "6.4.2 IGMP Protocol".)

4.5.6.2 Protocol Configuration

Use the Protocol Configuration screen to globally enable or disable unicast or multicast routing protocols for the switch.



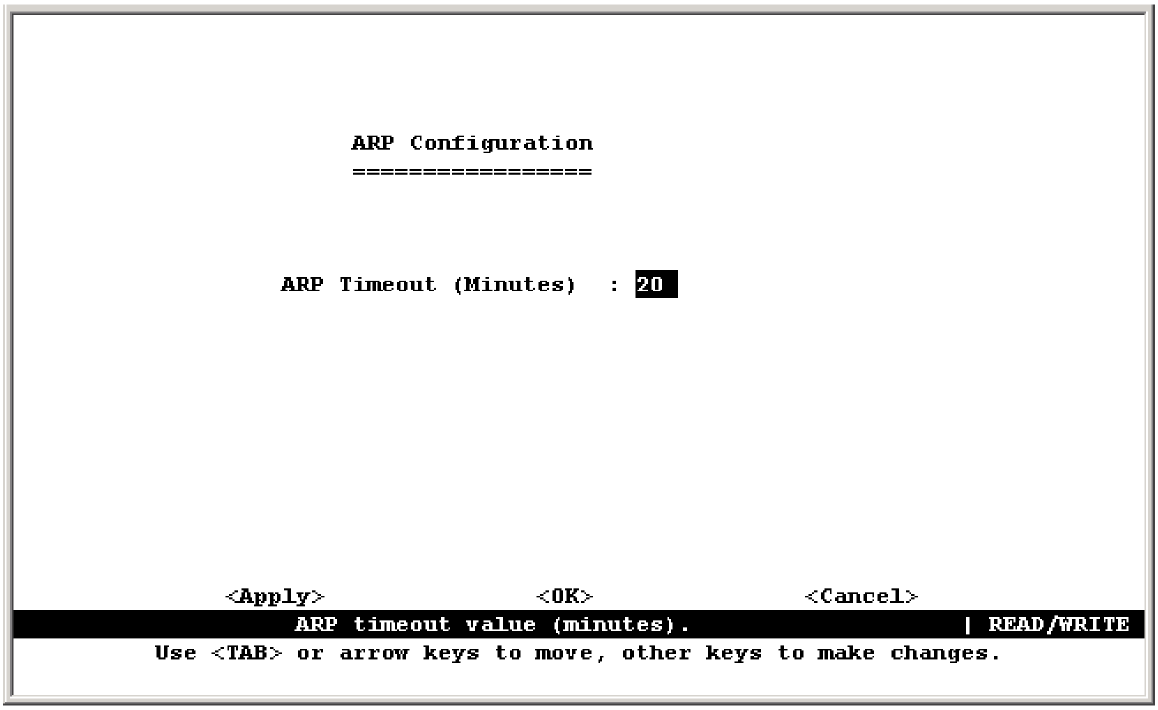
```
                    Protocol Configuration
                    ======================

              ARP           :            Advanced ...
              Proxy ARP     : ENABLED
              RIP           : ENABLED    Advanced ...

              DHCP Relay    : DISABLED   Advanced ...

              IGMP Snooping : DISABLED   Advanced ...
              DVMRP         : ENABLED




             <Apply>              <OK>              <Cancel>
                  System ARP protocol advanced status.
            Use <TAB> or arrow keys to move. <Enter> to select.
```

Parameter	Description
ARP	Sets the aging time for dynamic ARP entries.
Proxy ARP	Enables or disables Proxy ARP globally for the switch. This feature allows the switch to forward an ARP request from a node in the attached subnetwork (that does not have routing or a default gateway configured) to a remote subnetwork. (See “6.2.5 Proxy ARP”.) If Proxy ARP is globally enabled for the switch, then you can enable or disable it for a specific interface. See “4.5.6.1.1 Adding an IP Interface”, or “4.5.6.1.3 Modifying an IP Interface”.
RIP	Enables or disables the Routing Information Protocol. The Advanced menu sets the interval at which the switch advertises known routes, and also enables/disables advertising for static routes or the default route.
DHCP Relay	Enables or disables BOOTP/DHCP Relay. The Advanced menu defines the preferred servers or the outbound subnetworks for broadcasting a BOOTP/DHCP request.
IGMP Snooping	Enables or disables IGMP Snooping. The Advanced menu sets the timeout for inactive multicast ports or for specific multicast flows when there are no longer any clients.
DVMRP	Enables or disables the Distance-Vector Multicast Routing Protocol.

Note: Once RIP and DVMRP have been globally enabled, you can enable or disable them for any specific subnet via the Subnet Configuration menu.

4.5.6.2.1 Setting the ARP Timeout

You can use the following configuration screen to modify the aging time for dynamically learned entries in the ARP cache.

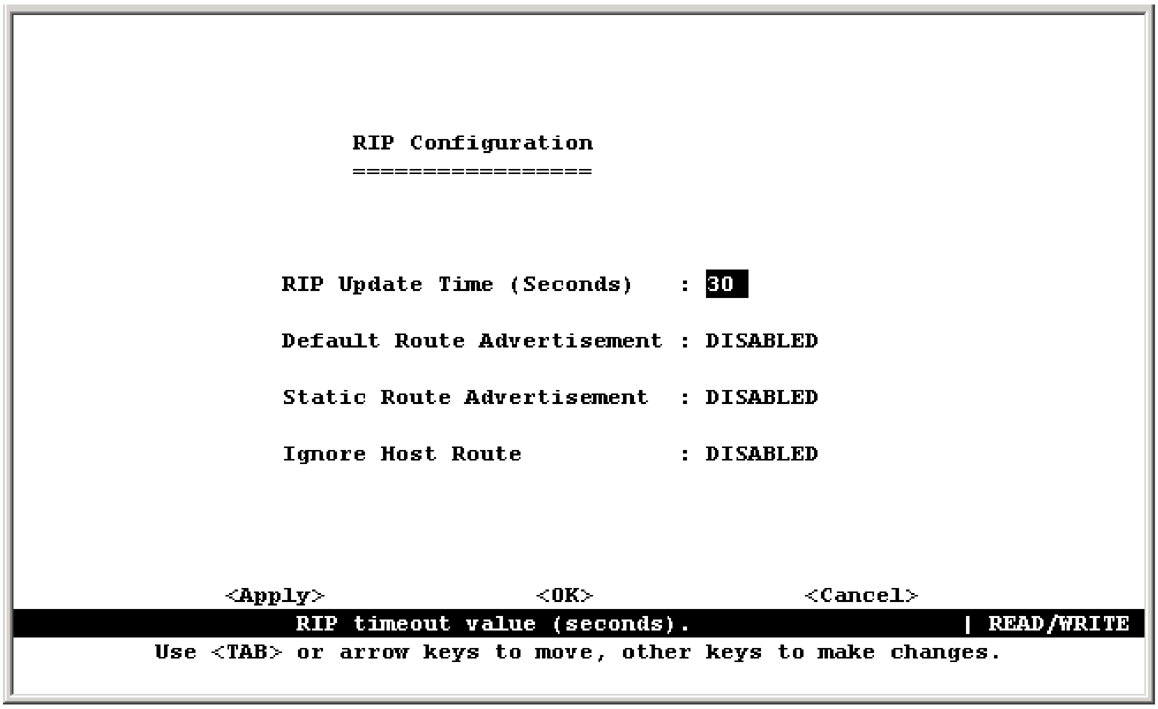


```
                    ARP Configuration
                    =================


              ARP Timeout (Minutes)   : 20









              <Apply>               <OK>              <Cancel>
                   ARP timeout value (minutes).                    | READ/WRITE
         Use <TAB> or arrow keys to move, other keys to make changes.
```

Parameter	Default	Description
ARP Timeout	20 minutes	The time that dynamically learned entries are retained in the ARP cache. Range: 0-999 minutes, where 0 disables aging

4.5.6.2.2 Setting the RIP Advertisement Policy

You can use the following configuration screen to set the timing interval and policies RIP uses to advertise route information.



```
                    RIP Configuration
                    =================


                RIP Update Time (Seconds)    : 30

                Default Route Advertisement : DISABLED

                Static Route Advertisement  : DISABLED

                Ignore Host Route           : DISABLED



            <Apply>              <OK>              <Cancel>
                 RIP timeout value (seconds).                | READ/WRITE
          Use <TAB> or arrow keys to move, other keys to make changes.
```

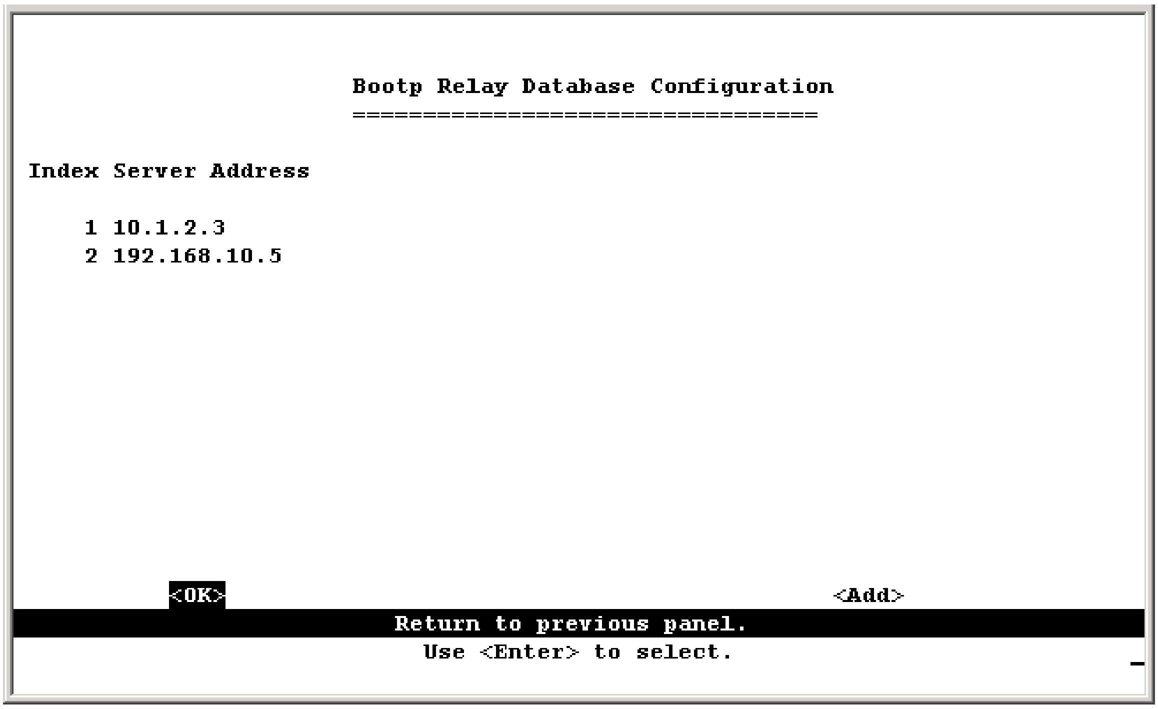
Parameter	Default	Description
RIP Update Time	30 seconds	The interval at which RIP advertises known route information. Range: 0-999 seconds, where 0 disables route advertisements
Default Route Advertisement	Disabled	Enables or disables advertising this switch as a default router.
Static Route Advertisement	Disabled	Enables or disables advertisement of static routes.
Ignore Host Route	Disabled	If enabled, the switch will not import a default route from other routers.

4.5.6.2.3 Configuring BOOTP/DHCP Relay

If a DHCP/BOOTP server is not located in the same subnet with a host, you can configure this switch to forward any host configuration queries to a server located on another subnet or on another network. Depending on the configuration setup, the switch either:

- Forwards the packet to a preferred server as defined in the switch configuration using unicast routing, or
- Broadcasts the DHCP Request again to another directly attached IP subnet specified in the switch configuration.

Specify the address for any DHCP server, or specify the subnet address for an outbound IP interface already configured on this switch as described in the following screens.

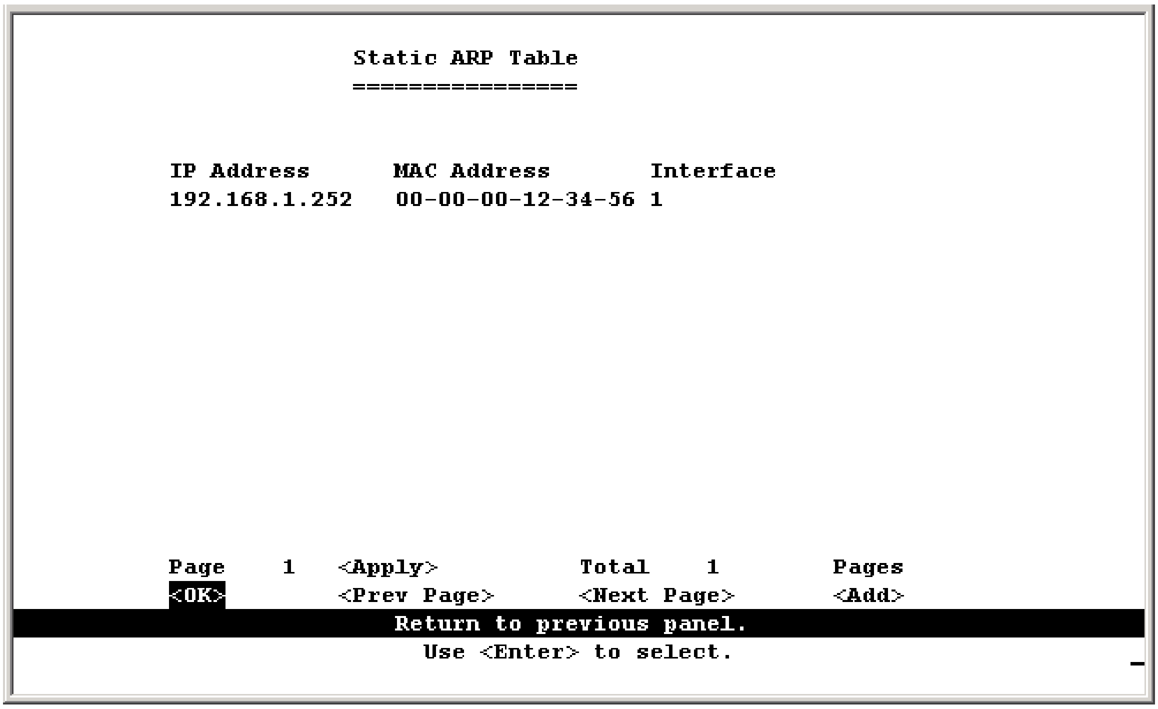


```
                        Bootp Relay Database Configuration
                        ==================================

Index Server Address

    1 10.1.2.3
    2 192.168.10.5









          <OK>                                              <Add>
                           Return to previous panel.
                             Use <Enter> to select.
```

Parameter	Description
Index Server Address	Used to define any preferred DHCP servers or the outbound subnetwork for relaying a DHCP request broadcast. (Up to five entries are permitted.)

4.5.6.3 Static ARP Configuration

Use the following screen to display or edit entries in the Static ARP Table. Entries added to this table are retained until the associated IP interface is deleted or the switch is reset to the factory defaults.



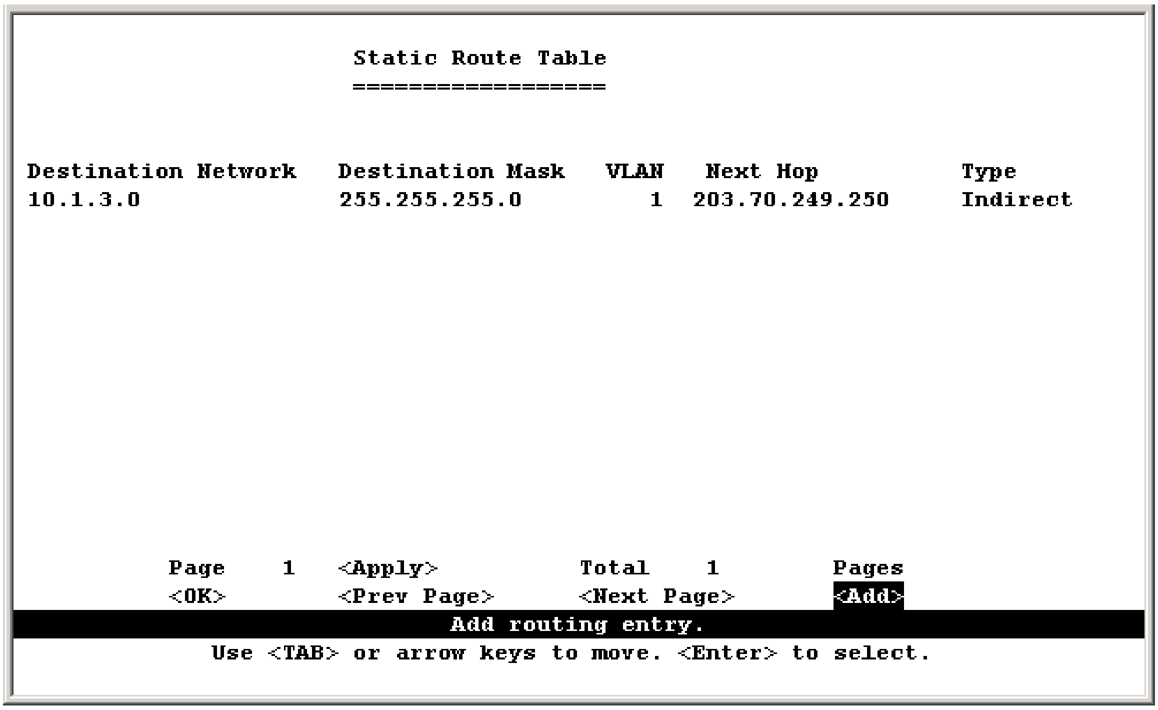
```
                    Static ARP Table
                    ================


         IP Address       MAC Address        Interface
         192.168.1.252    00-00-00-12-34-56  1













         Page     1    <Apply>          Total     1         Pages
         <OK>          <Prev Page>      <Next Page>         <Add>
                          Return to previous panel.
                            Use <Enter> to select.
```

Parameter	Description
IP Address	IP address statically mapped to a physical MAC address.
MAC Address	MAC address statically mapped to the corresponding IP address.
Interface	The index number of the IP interface that will use this static ARP entry. (Port "0" refers to the CPU.)

4.5.6.4 Static Route Configuration

This switch can be configured to dynamically learn the routes to other IP networks, subnets or hosts using unicast or multicast routing protocols. If the route to a specific destination cannot be learned via these protocols or you wish to restrict the path used for transmitting traffic to a destination, then it can be statically configured using the Static Route Table.

Before defining a static route, remember that you must first configure at least one IP interface on this switch. Static routes take precedence over dynamically learned routes, and remain in the table until you remove them or the corresponding IP interface from this switch.

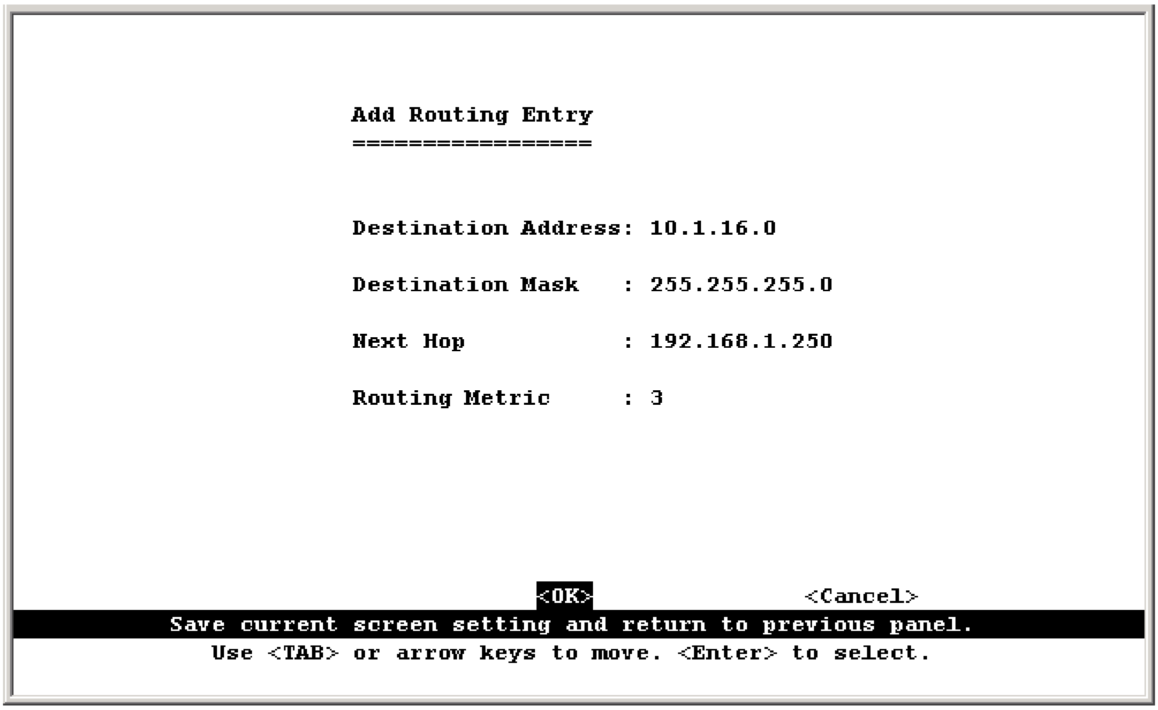


```
                       Static Route Table
                       ==================


Destination Network    Destination Mask    VLAN   Next Hop          Type
10.1.3.0               255.255.255.0          1   203.70.249.250    Indirect











          Page    1    <Apply>          Total    1         Pages
          <OK>         <Prev Page>      <Next Page>        <Add>
                              Add routing entry.
              Use <TAB> or arrow keys to move. <Enter> to select.
```

Parameter	Description
Destination Network	A destination network, subnet or host.
Destination Mask	The subnet mask that specifies the bits to match. A routing entry will be used for a packet if the bits in the address set by the destination mask match the Destination Network.
VLAN	The VLAN within which the gateway or destination address resides.
Next Hop	The IP address of the router at the next hop. Note that the network portion of the next hop must match that used for one of the subnet IP interfaces configured on this switch. (See “4.5.6.1 Subnet Configuration”)
Type	The IP route type for the destination network. This switch supports the following types: Direct - A directly connected subnetwork. Indirect - A remote IP subnetwork or host address.

Note: Use the <Next Page> and <Prev Page> buttons to scroll through the static route table. To display a specific page, set the page number in the Page field and then press <Apply>. To modify a static route, highlight the entry in the table and press Enter. To add a static route, press <Add>.

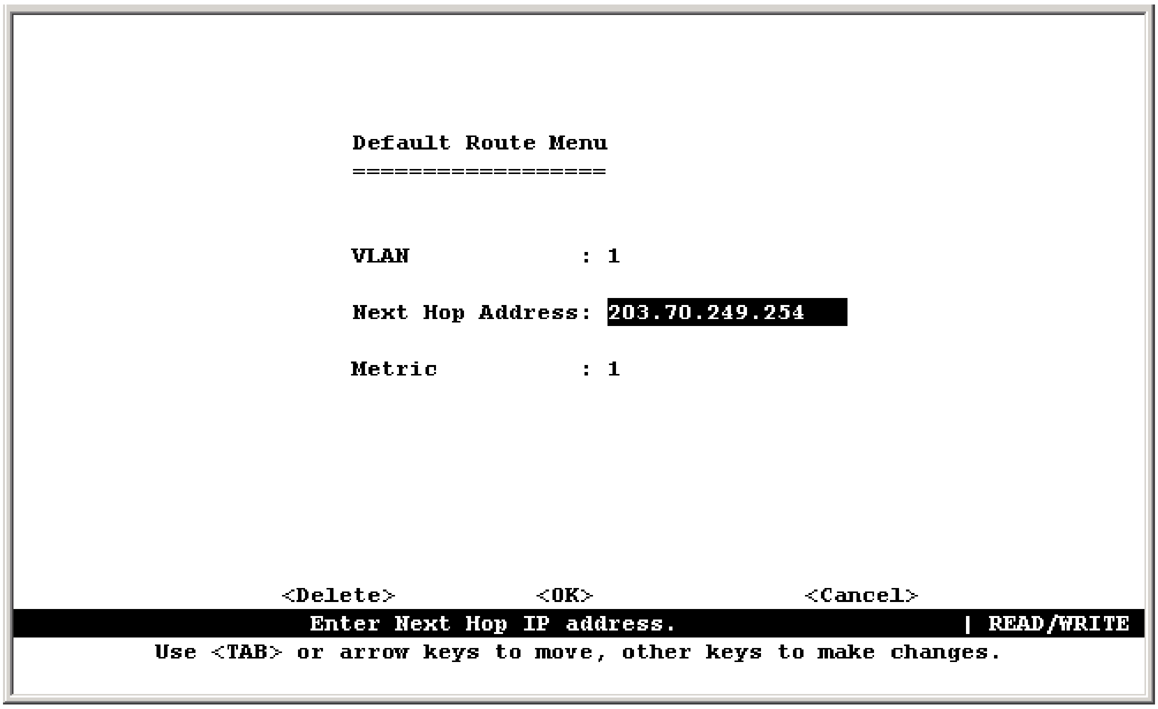
Adding a Static Route - The same screen is displayed for modifying or adding a static route. You must provide route information as described in the preceding table, plus the routing metric used to indicate the number of hops to the destination network.



```
                    Add Routing Entry
                    =================


                    Destination Address: 10.1.16.0

                    Destination Mask   : 255.255.255.0

                    Next Hop           : 192.168.1.250

                    Routing Metric     : 3





                               <OK>               <Cancel>
           Save current screen setting and return to previous panel.
              Use <TAB> or arrow keys to move. <Enter> to select.
```

4.5.6.5 Configuring the Default Route

Defines the router to which this switch will forward all traffic for unknown networks. The default route can be learned from RIP protocol (See “4.5.6.1.4 Configuring RIP”) or manually configured. If the switch does not contain a default route, any packet that does not match an entry in the routing table will be dropped. To manually configure a default route, enter the next hop in the following table.

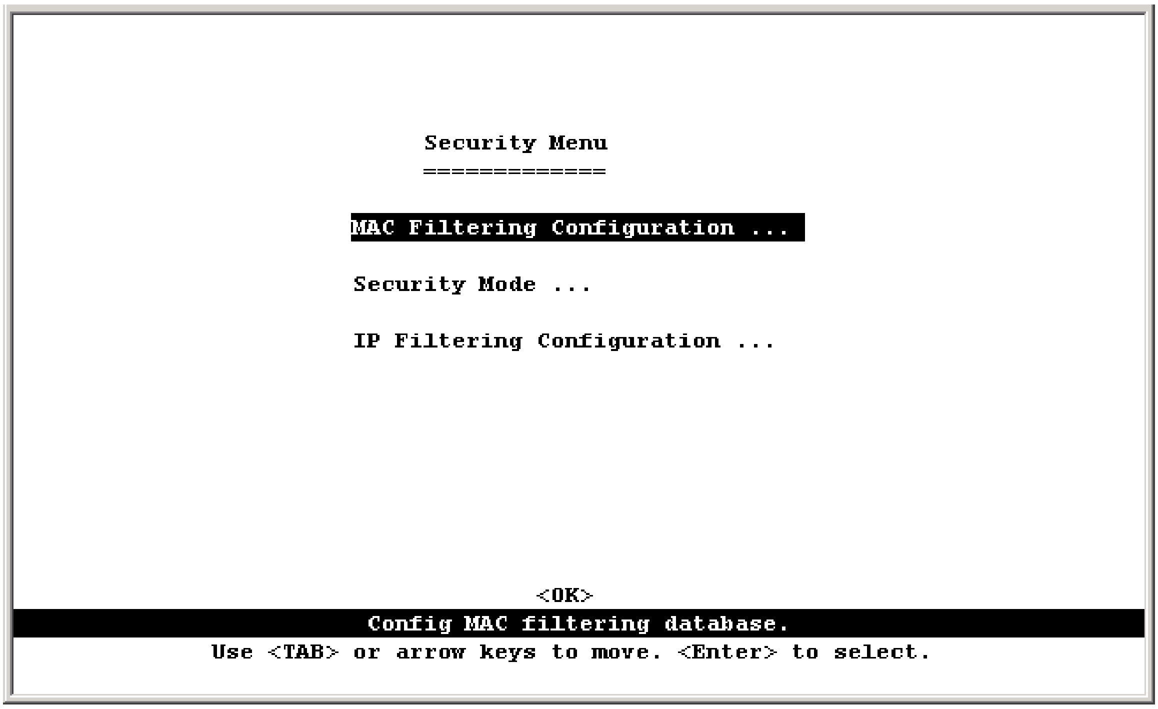


```
                 Default Route Menu
                 ==================

                 VLAN             : 1

                 Next Hop Address: 203.70.249.254

                 Metric           : 1



             <Delete>         <OK>              <Cancel>
                  Enter Next Hop IP address.                 | READ/WRITE
          Use <TAB> or arrow keys to move, other keys to make changes.
```

Parameter	Description
VLAN	The VLAN which has the IP interface to the default router.
Next Hop Address	The IP address of the default router.
Metric	The number of hops required to reach the default router.

4.5.7 Security Menu

The Security menu contains options to filter specified MAC or IP addresses. These menu options are described in the following sections.



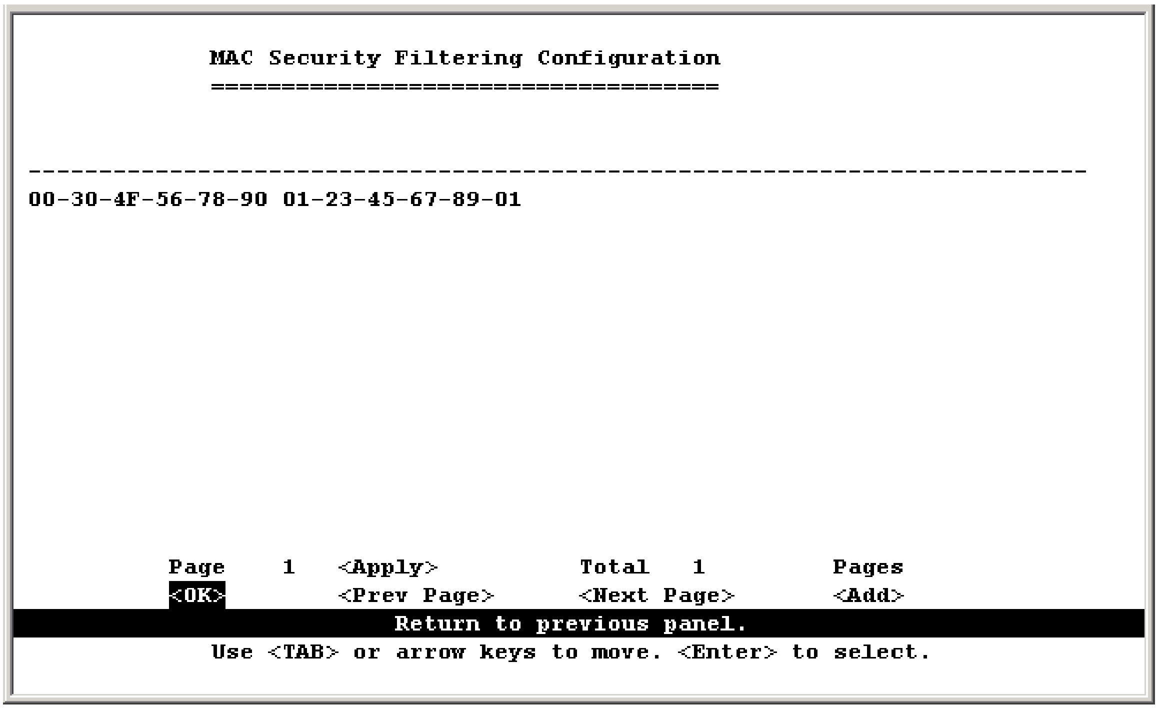
```
                    Security Menu
                    =============

              MAC Filtering Configuration ...

              Security Mode ...

              IP Filtering Configuration ...




                         <OK>
              Config MAC filtering database.
       Use <TAB> or arrow keys to move. <Enter> to select.
```

Menu	Description
MAC Filtering Configuration	Specifies the source or destination MAC address for any traffic to be filtered from the switch for security reasons.
IP Filtering Configuration *	Specifies the source or destination IP address for any traffic to be filtered from the switch for security reasons.

* This menu item is only displayed for multilayer mode.

4.5.7.1 Configuring MAC Address Filters

Any node that presents a security risk or is functioning improperly can be filtered from this switch. You can drop all the traffic from a host device based on a specified MAC address. Traffic with either a source or destination address listed in the Security Filtering Configuration table will be filtered.

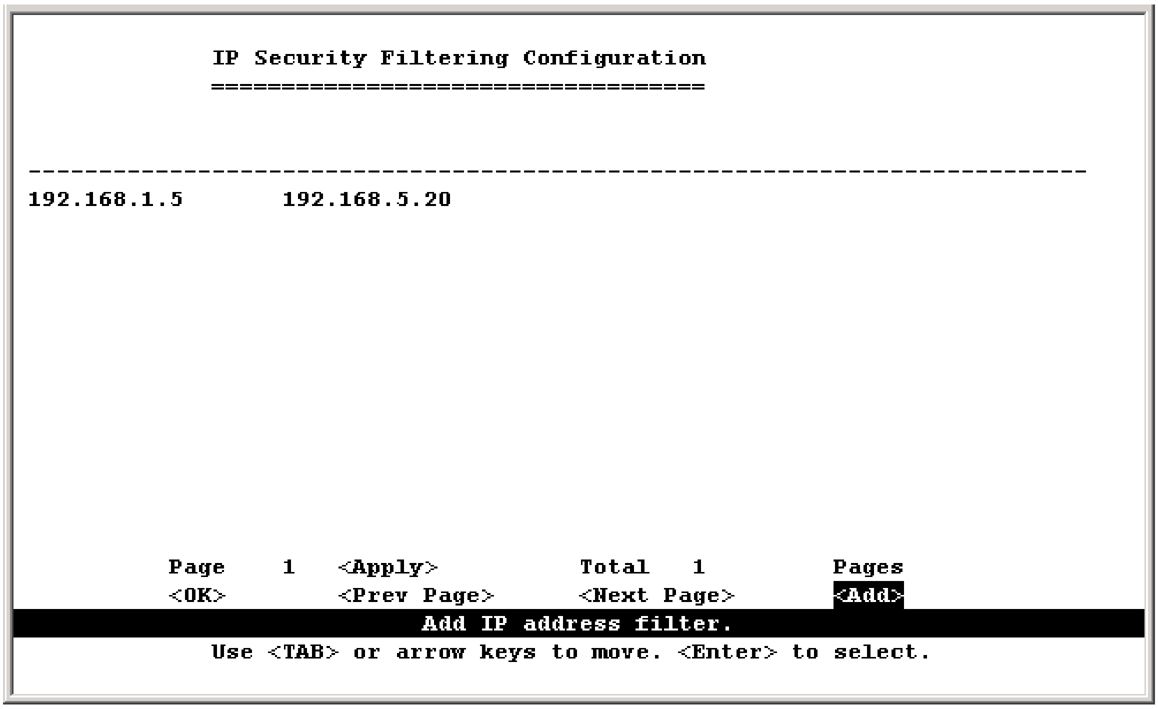


```
             MAC Security Filtering Configuration
             ====================================


------------------------------------------------------------------------
00-30-4F-56-78-90 01-23-45-67-89-01










          Page    1   <Apply>          Total   1         Pages
          <OK>        <Prev Page>      <Next Page>       <Add>
                              Return to previous panel.
             Use <TAB> or arrow keys to move. <Enter> to select.
```

Note: To add a MAC address to the security filtering, use <Add>. To delete an address, highlight it with the cursor and press Enter. To scroll through the address table, use the <Next Page> and <Prev Page> buttons. To display a specific page, set the page number in the Page field and then press <Apply>.

4.5.7.2 IP Filtering Configuration

If any node presents a security risk, you can filter all traffic for this node by entering its address into the IP Security Filter. Any packet passing through the switch that has a source or destination IP address matching an entry in this table will be filtered.

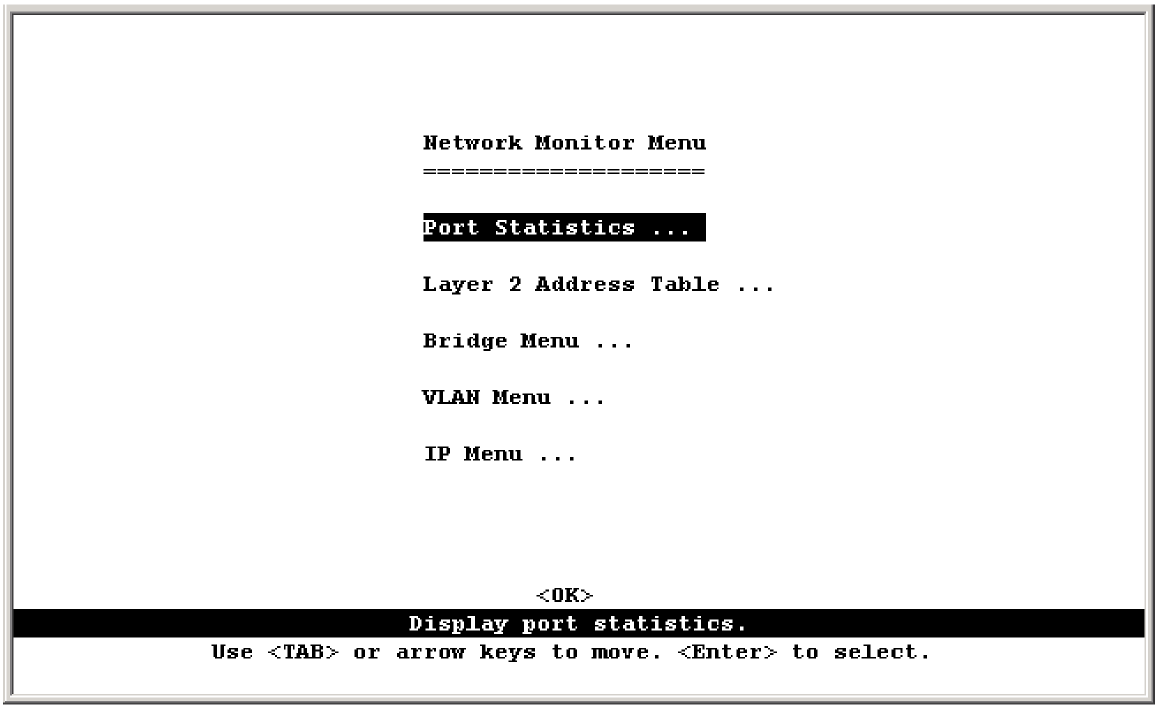


```
              IP Security Filtering Configuration
              ===================================


-----------------------------------------------------------------------------
192.168.1.5       192.168.5.20









           Page     1   <Apply>          Total    1         Pages
           <OK>         <Prev Page>      <Next Page>        <Add>
                           Add IP address filter.
              Use <TAB> or arrow keys to move. <Enter> to select.
```

Note: To add a IP address to the security filter, use <Add>. To delete an address, highlight it with the cursor and select Enter. Use the <Next Page> and <Prev Page> buttons to scroll through the table. To display a specific page, set the page number in the Page field and then press <Apply>. To add an entry, press <Add>.

4.6 Monitoring the Switch

The Network Monitor Menu provides access to port statistics, address tables, STA information, VLANs registration and forwarding information, multicast groups. Each of the screens provided by these menus is described in the following sections.



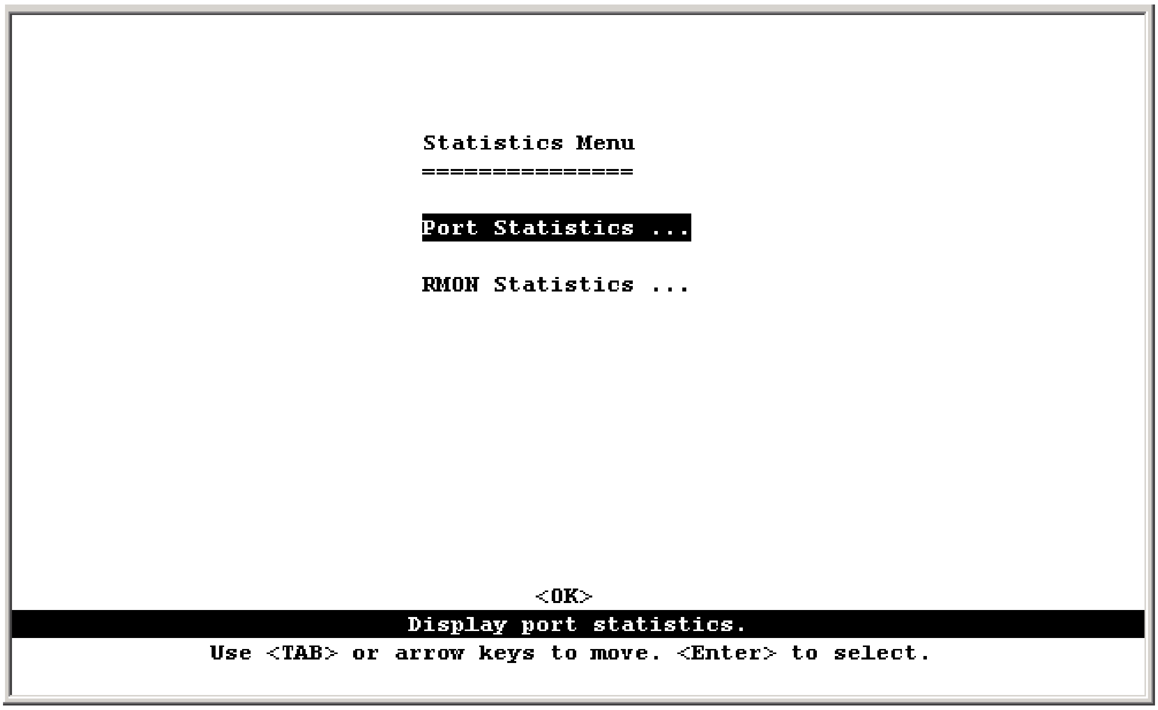
```
Network Monitor Menu
====================

Port Statistics ...

Layer 2 Address Table ...

Bridge Menu ...

VLAN Menu ...

IP Menu ...



              <OK>
       Display port statistics.
Use <TAB> or arrow keys to move. <Enter> to select.
```

Menu	Description
Port Statistics	Displays statistics on port traffic, including information from the Interfaces Group, Ethernet-like MIB, and RMON MIB.
Layer 2 Address Table	Contains the unicast address table.
Bridge Menu	Displays Spanning Tree settings for the overall switch and for specific ports.
VLAN Menu	Displays ports dynamically learned through GMRP or GVRP, and ports that are currently forwarding VLAN traffic.
IP Multicast Registration Table *1	Displays all the multicast groups active on this switch, including the multicast IP address and the corresponding VLANs.
IP Menu * 2	Displays all the IP subnets used on this switch, as well as the corresponding VLANs and ports. Also contains the ARP table, routing table and multicast menu.

1: This menu is only displayed if the switch is set to Layer 2 mode.
2: This menu is only displayed if the switch is set to multilayer mode.

4.6.1 Displaying Port Statistics

Port Statistics display standard statistics on network traffic from the Interfaces Group and Ethernet-like MIBs, as well as a detailed breakdown of traffic based on the RMOM MIB.



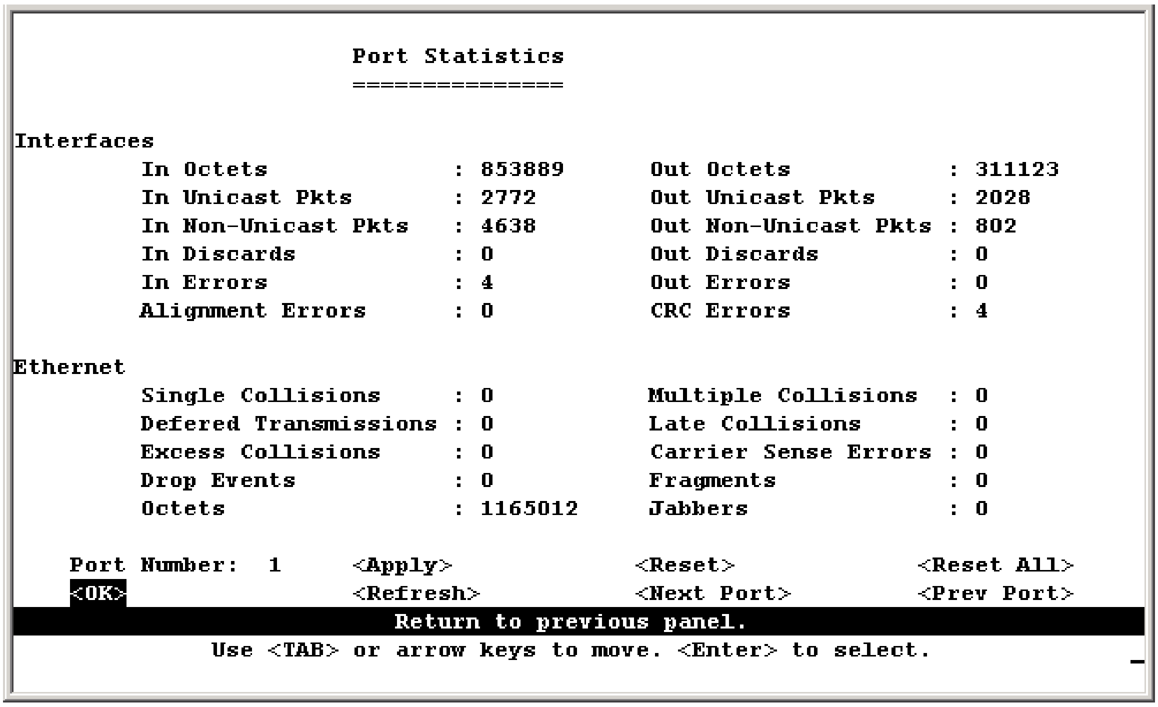
```
Statistics Menu
===============

Port Statistics ...

RMON Statistics ...


                    <OK>
           Display port statistics.
  Use <TAB> or arrow keys to move. <Enter> to select.
```

Menu	Description
Port Statistics	Displays statistics on network traffic passing through the selected port.
RMON Statistics	Displays detailed statistical information for the selected port such as packet type and frame size counters.

4.6.1.1 Displaying Ethernet Port Statistics

Port Statistics display key statistics from the Interfaces Group and Ethernet MIBs for each port. Error statistics on the traffic passing through each port are displayed. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading). The values displayed have been accumulated since the last system reboot.

Select the required port. The statistics displayed are indicated in the following figure and table.



```
                        Port Statistics
                        ===============

Interfaces
         In Octets            : 853889      Out Octets           : 311123
         In Unicast Pkts      : 2772        Out Unicast Pkts     : 2028
         In Non-Unicast Pkts  : 4638        Out Non-Unicast Pkts : 802
         In Discards          : 0           Out Discards         : 0
         In Errors            : 4           Out Errors           : 0
         Alignment Errors     : 0           CRC Errors           : 4

Ethernet
         Single Collisions    : 0           Multiple Collisions  : 0
         Defered Transmissions : 0          Late Collisions      : 0
         Excess Collisions    : 0           Carrier Sense Errors : 0
         Drop Events          : 0           Fragments            : 0
         Octets               : 1165012     Jabbers              : 0

    Port Number:  1     <Apply>             <Reset>             <Reset All>
    <OK>                <Refresh>           <Next Port>         <Prev Port>
                           Return to previous panel.
              Use <TAB> or arrow keys to move. <Enter> to select.
```

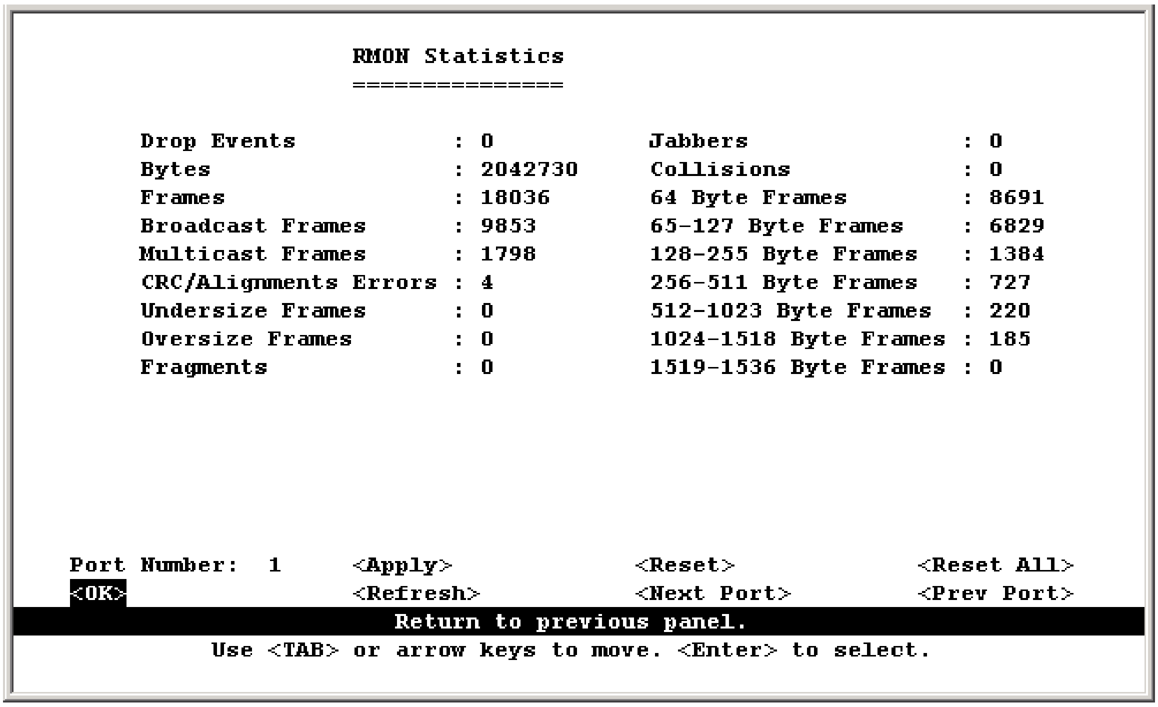
Parameter	Description
Interfaces Group	
In Octets	The total number of octets received on the interface, including framing characters.
In Unicast Pkts	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
In Non-Unicast Pkts	The number of non-unicast (that is, subnetwork- broadcast or subnetwork-multicast) packets delivered to a higher-layer protocol.
In Discards	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
In Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Alignment Errors	The number of alignment errors (mis-synchronized data packets).
Out Octets	The total number of octets transmitted out of the interface, including framing characters.
Out Unicast Pkts	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Out Non-Unicast	The total number of packets that higher-level protocols requested be transmitted to a non- unicast (that is, a subnetwork-broadcast or

Pkts	subnetwork-multicast) address, including those that were discarded or not sent.
Out Discards	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Out Errors	The number of outbound packets that could not be transmitted because of errors.
CRC Errors	Number of Ethernet Cyclic Redundancy Check errors detected by this device.
Ethernet-Like	
Single Collisions	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Excessive Collisions	The number of frames for which transmission failed due to excessive collisions.
Drop Events	The total number of events in which packets were dropped due to lack of resources
Octets	Number of octets passing through this port.
Multiple Collisions	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
Carrier Sense Errors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.

Note: Statistics are refreshed every 10 seconds by default (See “4.4.2 Configuring the Serial Port”).

4.6.1.2 Displaying RMON Statistics

Use the RMON Statistics screen to display key statistics for each port from RMON group 1. (RMON groups 2, 3 and 9 can only be accessed using SNMP management software.) The following screen displays the overall statistics on traffic passing through each port. RMON statistics provide access to a broad range of statistics, including a total count of different frame types and sizes passing through each port. Values displayed have been accumulated since the last system reboot.



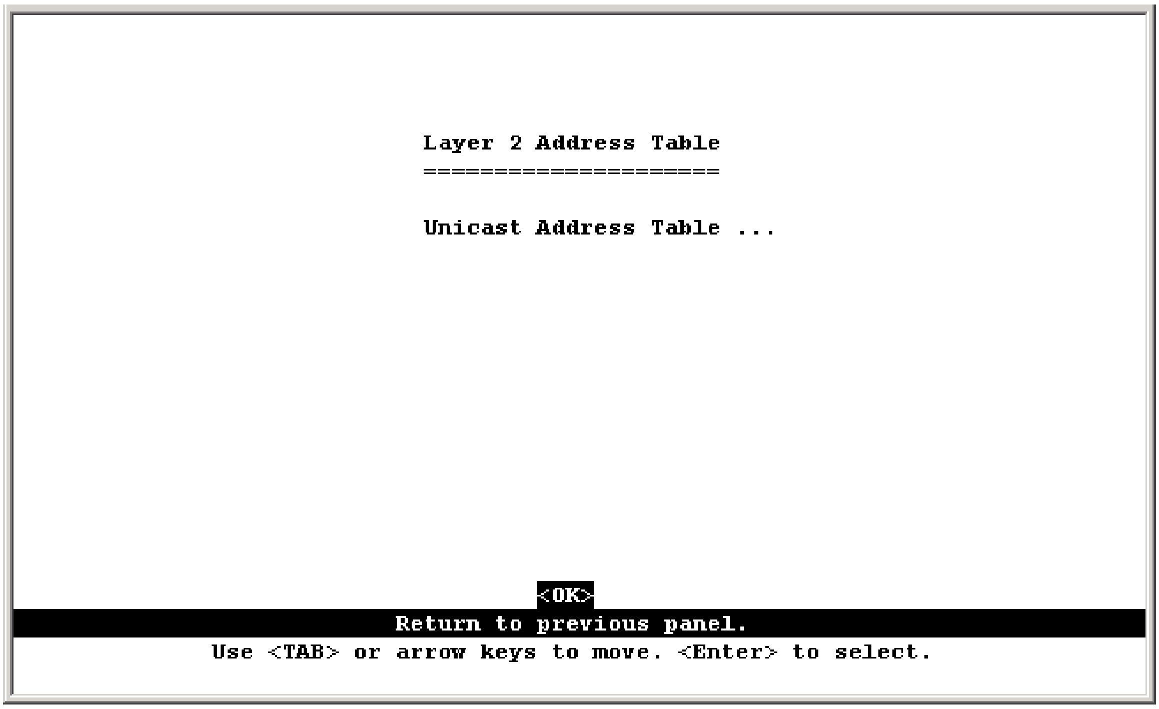
```
                    RMON Statistics
                    ===============

        Drop Events            : 0           Jabbers               : 0
        Bytes                  : 2042730     Collisions            : 0
        Frames                 : 18036       64 Byte Frames        : 8691
        Broadcast Frames       : 9853        65-127 Byte Frames    : 6829
        Multicast Frames       : 1798        128-255 Byte Frames   : 1384
        CRC/Alignments Errors  : 4           256-511 Byte Frames   : 727
        Undersize Frames       : 0           512-1023 Byte Frames  : 220
        Oversize Frames        : 0           1024-1518 Byte Frames : 185
        Fragments              : 0           1519-1536 Byte Frames : 0




    Port Number:  1     <Apply>             <Reset>             <Reset All>
    <OK>                <Refresh>           <Next Port>         <Prev Port>
                           Return to previous panel.
              Use <TAB> or arrow keys to move. <Enter> to select.
```

Parameter	Description
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Bytes	Total number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Frames	The total number of frames (bad, broadcast and multicast) received.
Broadcast Frames	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Frames	The total number of good frames received that were directed to this multicast address.
CRC/Alignment Errors	The number of CRC/alignment errors (FCS or alignment errors).
Undersize Frames	The total number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed. Oversize Frames The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
64 Byte Frames	The total number of frames (including bad packets) received and transmitted that were 64 octets in length(excluding framing bits but including FCS octets).
65-127 Byte Frames 128-255 Byte Frames 256-511 Byte Frames 512-1023 Byte Frames 1024-1518 Byte Frames 1519-1536 Byte Frames	The total number of frames (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).

Note: Statistics are refreshed every 10 seconds by default (See “4.4.2 Configuring the Serial Port”).

4.6.2 Layer 2 Address Tables

This menu includes the unicast address table.

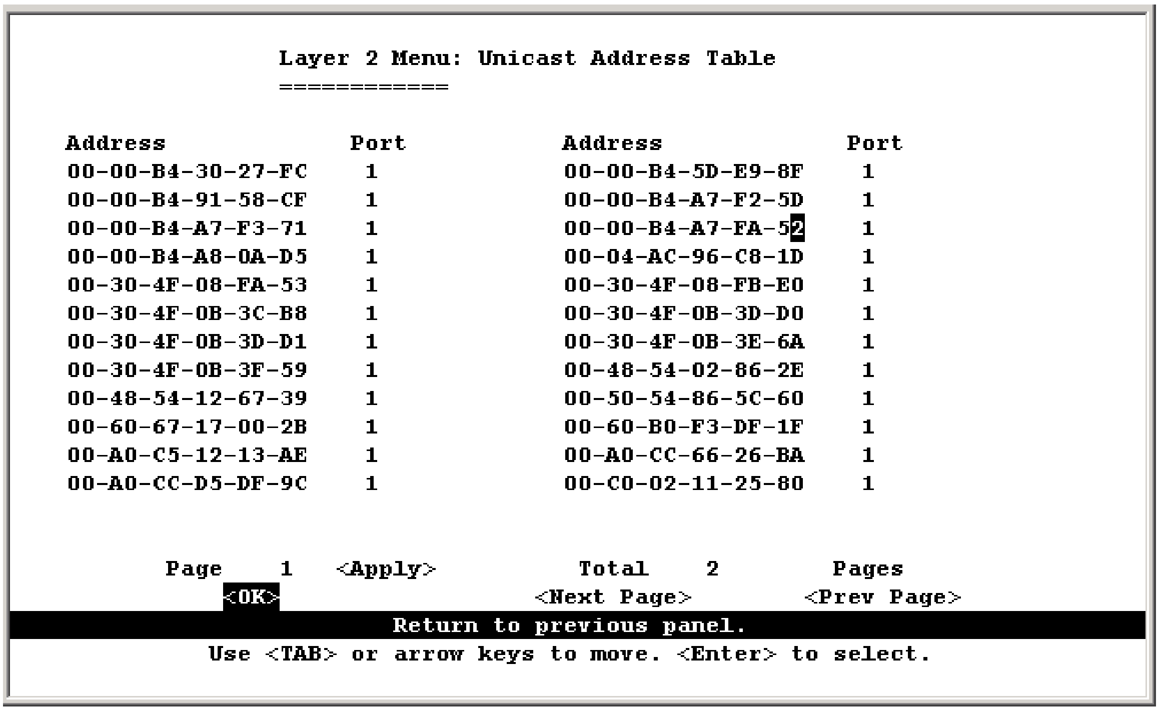


```
Layer 2 Address Table
=====================

Unicast Address Table ...



<OK>
Return to previous panel.
Use <TAB> or arrow keys to move. <Enter> to select.
```

Menu	Description
Unicast Address Table	Provides a full listing for unicast addresses

4.6.2.1 Displaying the Unicast Address Table

The Unicast Address Table contains the MAC addresses associated with each port (that is, the source port associated with the address). The information displayed in the Address Table is indicated in the following figure and table.



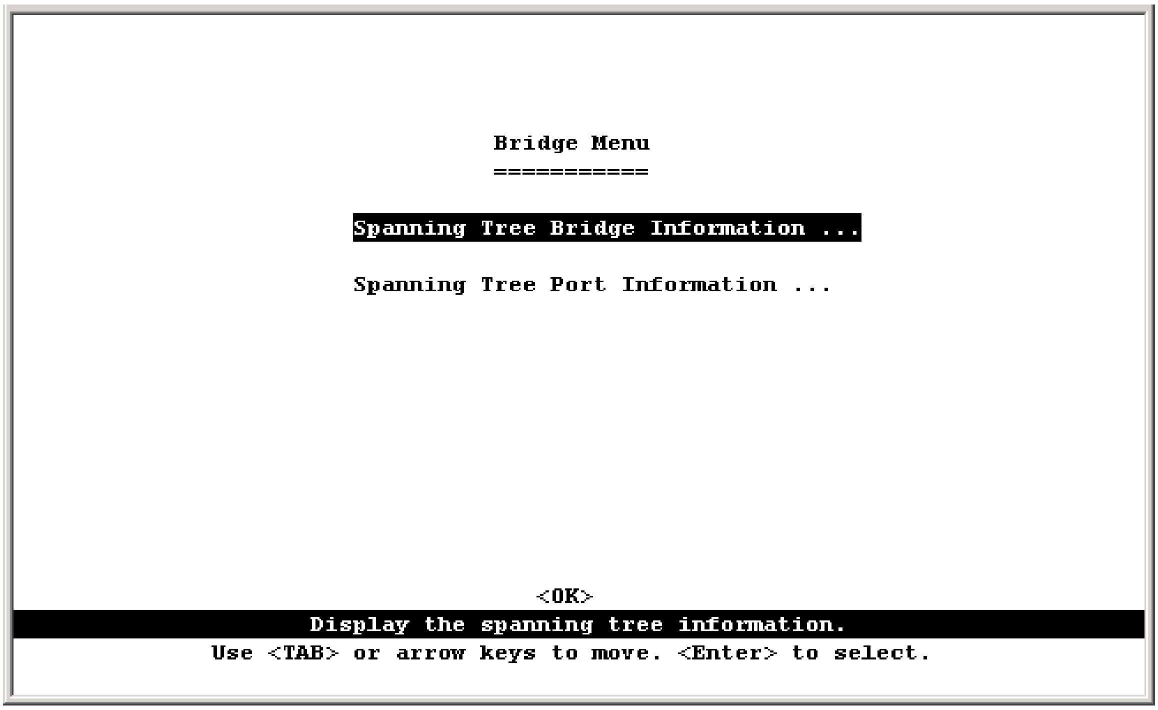
```
                   Layer 2 Menu: Unicast Address Table
                   ============

    Address              Port           Address              Port
    00-00-B4-30-27-FC     1             00-00-B4-5D-E9-8F     1
    00-00-B4-91-58-CF     1             00-00-B4-A7-F2-5D     1
    00-00-B4-A7-F3-71     1             00-00-B4-A7-FA-52     1
    00-00-B4-A8-0A-D5     1             00-04-AC-96-C8-1D     1
    00-30-4F-08-FA-53     1             00-30-4F-08-FB-E0     1
    00-30-4F-0B-3C-B8     1             00-30-4F-0B-3D-D0     1
    00-30-4F-0B-3D-D1     1             00-30-4F-0B-3E-6A     1
    00-30-4F-0B-3F-59     1             00-48-54-02-86-2E     1
    00-48-54-12-67-39     1             00-50-54-86-5C-60     1
    00-60-67-17-00-2B     1             00-60-B0-F3-DF-1F     1
    00-A0-C5-12-13-AE     1             00-A0-CC-66-26-BA     1
    00-A0-CC-D5-DF-9C     1             00-C0-02-11-25-80     1


            Page    1   <Apply>         Total    2        Pages
                <OK>                 <Next Page>        <Prev Page>
                           Return to previous panel.
              Use <TAB> or arrow keys to move. <Enter> to select.
```

Parameter	Description
Address	The MAC address of a node seen on this switch.
Port	The port whose address table includes this MAC address.

Note: Use the <Next Page> and <Prev Page> buttons to scroll through the address table. To display a specific page, set the page number in the Page field and then press <Apply>.

4.6.3 Displaying Bridge Information

The Bridge menu is used to display settings for the Spanning Tree Algorithm. For a more detailed description of how to use this algorithm, refer to “6.1.3 Spanning Tree Algorithm”.

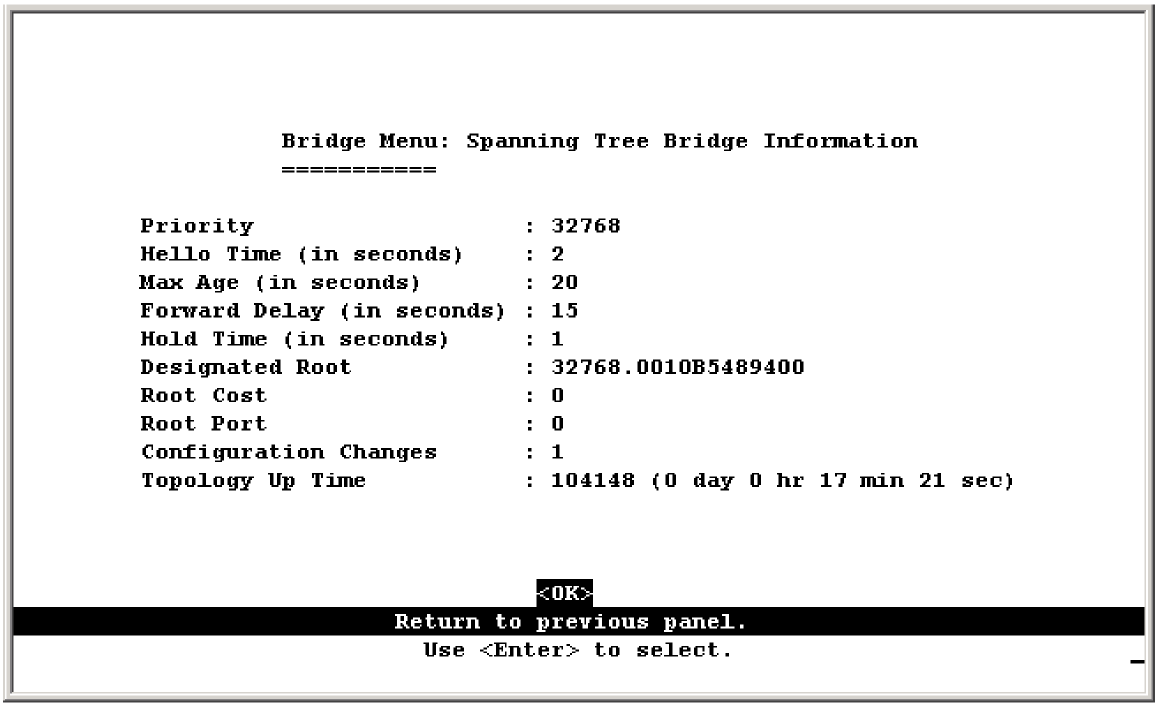


```
                         Bridge Menu
                         ===========

              Spanning Tree Bridge Information ...

              Spanning Tree Port Information ...








                             <OK>
                Display the spanning tree information.
          Use <TAB> or arrow keys to move. <Enter> to select.
```

Menu	Description
Spanning Tree Bridge Information	Displays a full list of STA values used for the bridge.
Spanning Tree Port Information	Displays a list of STA values used for each port, including status, designated cost, designated bridge, and designated port.

4.6.3.1 Viewing the Current Spanning Tree Bridge Information

The STA Bridge Information screen displays a summary of STA information for the overall bridge. To make any changes to these parameters, use the Bridge STA Configuration menu. The parameters shown in the following figure and table describe the current bridge STA settings.

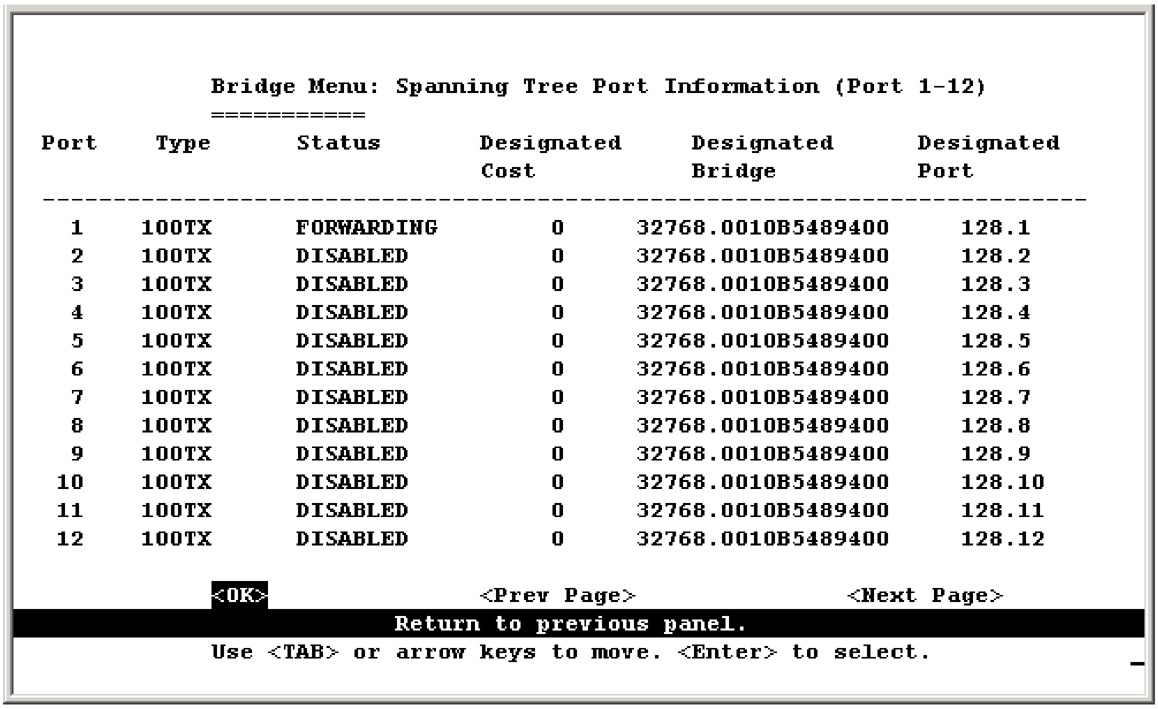


```
                    Bridge Menu: Spanning Tree Bridge Information
                    ===========

          Priority                   : 32768
          Hello Time (in seconds)    : 2
          Max Age (in seconds)       : 20
          Forward Delay (in seconds) : 15
          Hold Time (in seconds)     : 1
          Designated Root            : 32768.0010B5489400
          Root Cost                  : 0
          Root Port                  : 0
          Configuration Changes      : 1
          Topology Up Time           : 104148 (0 day 0 hr 17 min 21 sec)


                                     <OK>
                           Return to previous panel.
                             Use <Enter> to select.
```

Parameter	Description
Priority	Device priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.
Hello Time	The time interval (in seconds) at which the root device transmits a configuration message.
Max Age	The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure.
Forward Delay	The maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding).
Hold Time	The minimum interval between the transmission of consecutive Configuration BPDUs
Designated Root	The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.
Root Cost	The path cost from the root port on this switch to the root device.
Root Port	The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.
Configuration Changes	The number of times the Spanning Tree has been reconfigured.
Topology Up Time	The time since the Spanning Tree was last reconfigured.

4.6.3.2 Displaying the Current Spanning Tree Port information

The parameters shown in the following figure and table are for spanning tree port Information.

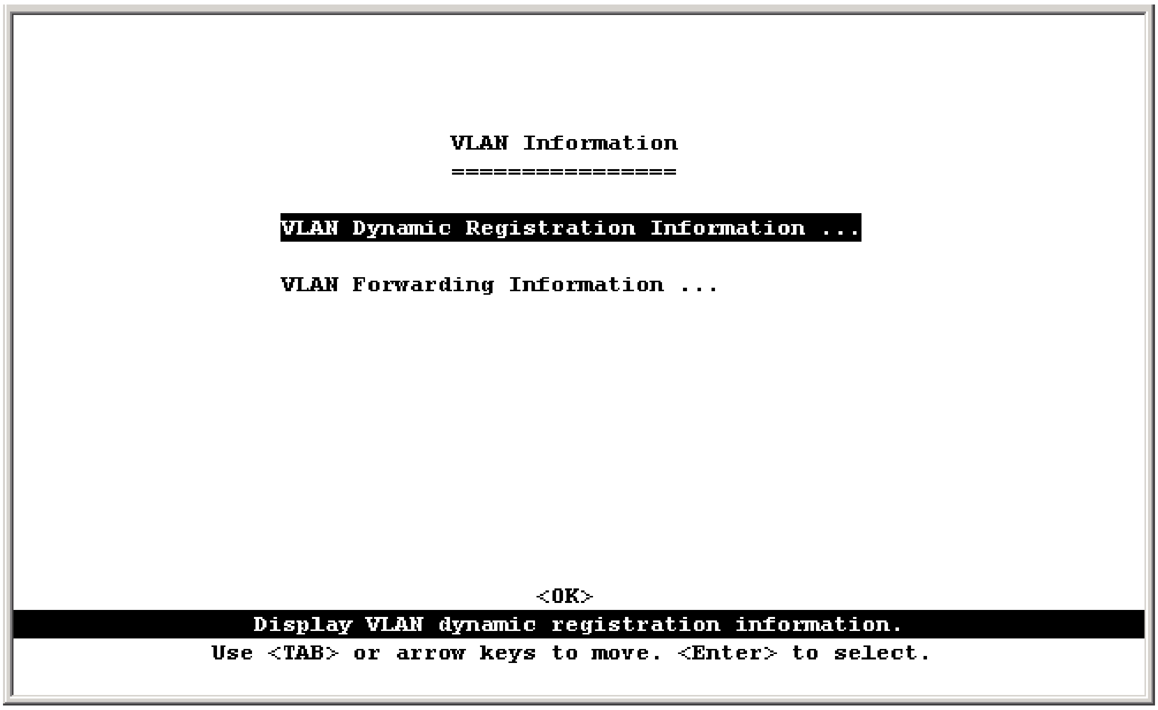


```
             Bridge Menu: Spanning Tree Port Information (Port 1-12)
             ===========
 Port    Type      Status      Designated     Designated      Designated
                               Cost           Bridge          Port
 --------------------------------------------------------------------------
   1    100TX     FORWARDING        0     32768.0010B5489400     128.1
   2    100TX     DISABLED          0     32768.0010B5489400     128.2
   3    100TX     DISABLED          0     32768.0010B5489400     128.3
   4    100TX     DISABLED          0     32768.0010B5489400     128.4
   5    100TX     DISABLED          0     32768.0010B5489400     128.5
   6    100TX     DISABLED          0     32768.0010B5489400     128.6
   7    100TX     DISABLED          0     32768.0010B5489400     128.7
   8    100TX     DISABLED          0     32768.0010B5489400     128.8
   9    100TX     DISABLED          0     32768.0010B5489400     128.9
  10    100TX     DISABLED          0     32768.0010B5489400     128.10
  11    100TX     DISABLED          0     32768.0010B5489400     128.11
  12    100TX     DISABLED          0     32768.0010B5489400     128.12

             <OK>                <Prev Page>               <Next Page>
                             Return to previous panel.
             Use <TAB> or arrow keys to move. <Enter> to select.
```

Parameter	Description
Type	Shows port type as: 100TX : 10BASE-T/ 100BASE-TX 1000T : 1000BASE-T
Status	Displays current state of this port within the Spanning Tree: **Disabled** - No link has been established on this port. Otherwise, the port has been disabled by the user or has failed diagnostics. Blocking - Port receives STA configuration messages, but does not forward packets. **Listening** - Port will leave blocking state due to a topology change, starts transmitting configuration messages, but does not yet forward packets. **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses. **Forwarding** - The port forwards packets, and continues the learning addresses. The rules defining port status are: • A port on a network segment with no other STA compliant bridging device is always forwarding. • If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is blocked. • All ports are blocked when the switch is booted, then some of them change state to listening, to learning, and then to forwarding.
Designated Cost	The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.
Designated Bridge (ID)	The priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.
DesignatedPort (ID)	The priority and number of the port on the designated bridging device through which this switch must communicate with the root of the Spanning Tree.

4.6.4 Displaying VLAN Information

These menus display information on the ports that have been automatically learned via GVRP; and all those ports that have been configured by dynamic or static means to forward VLAN traffic.

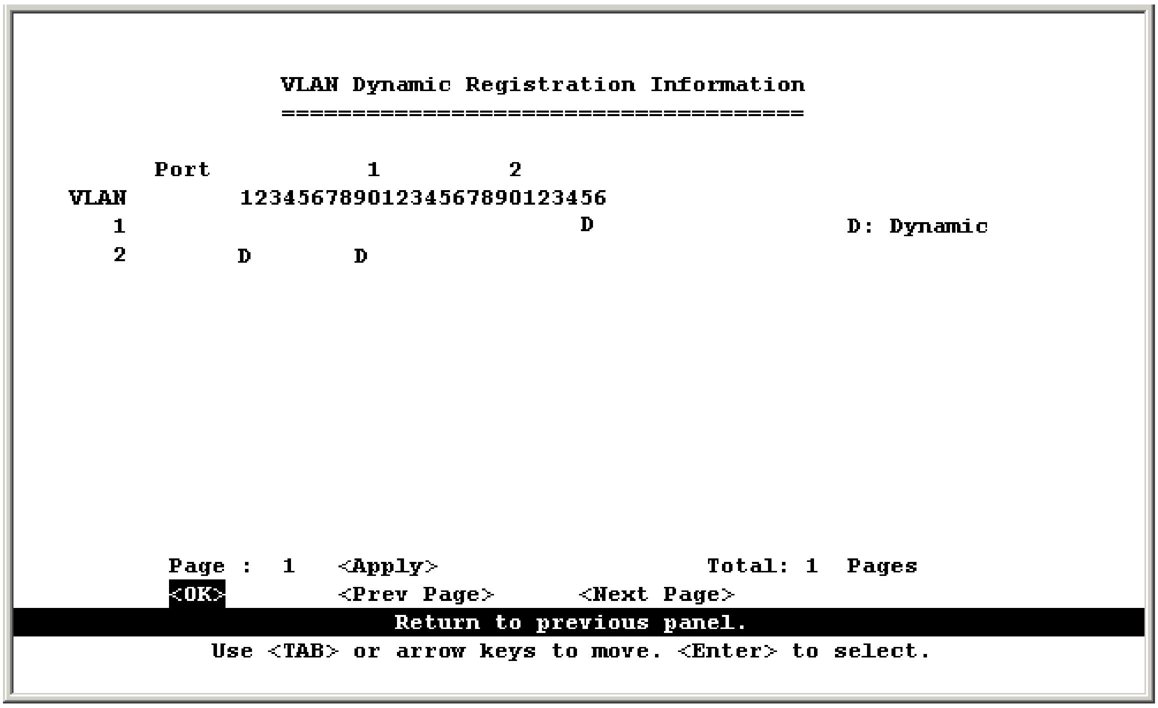


```
                         VLAN Information
                         ================

             VLAN Dynamic Registration Information ...

             VLAN Forwarding Information ...




                              <OK>
            Display VLAN dynamic registration information.
          Use <TAB> or arrow keys to move. <Enter> to select.
```

Menu	Description
VLAN Dynamic Registration Information	Shows the ports that have been automatically learned via GVRP.
VLAN Forwarding Information	Shows all those ports that have been configured by either dynamic or static means to forward VLAN traffic.

4.6.4.1 VLAN Dynamic Registration Information

This table shows the ports that have been automatically learned via GVRP.

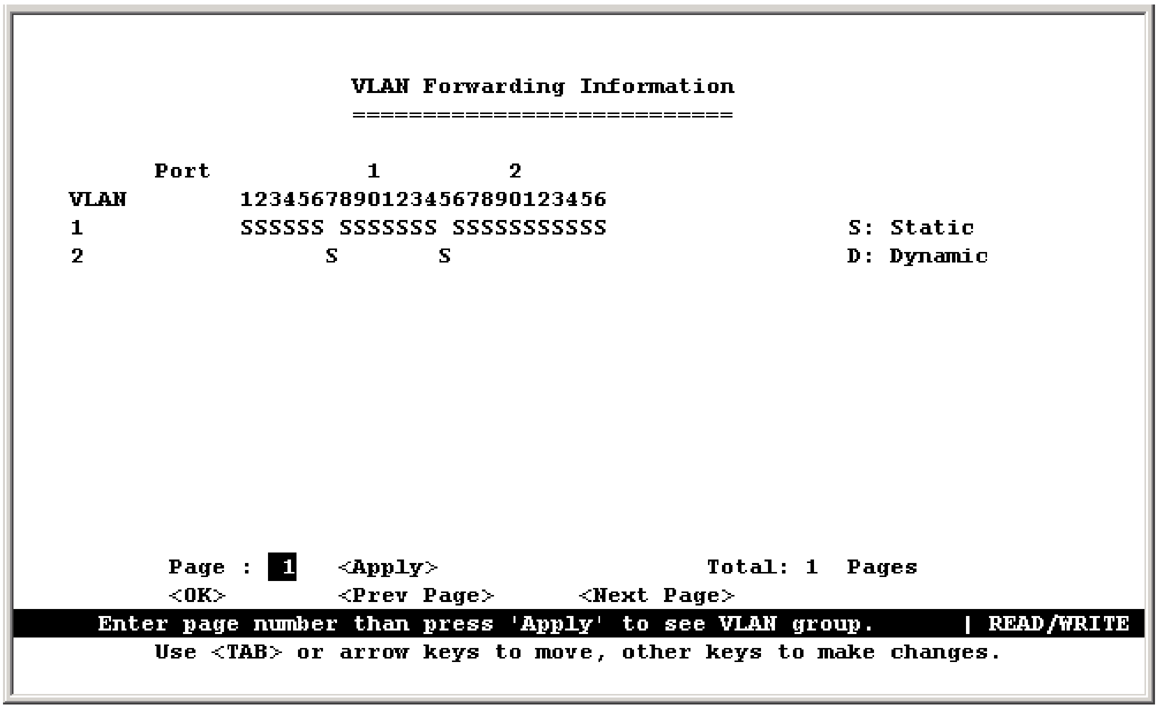


```
                   VLAN Dynamic Registration Information
                   =====================================

          Port           1         2
    VLAN        12345678901234567890123456
       1                                D                  D: Dynamic
       2        D       D











           Page :  1   <Apply>                   Total: 1  Pages
           <OK>        <Prev Page>      <Next Page>
                           Return to previous panel.
              Use <TAB> or arrow keys to move. <Enter> to select.
```

Note: To scroll through the dynamic registration table, use the <Next Page> and <Prev Page> buttons. To display a specific page, set the page number in the Page field and then press <Apply>.

4.6.4.2 VLAN Forwarding Information

Shows all those ports that have been configured by either dynamic or static means to forward VLAN traffic.

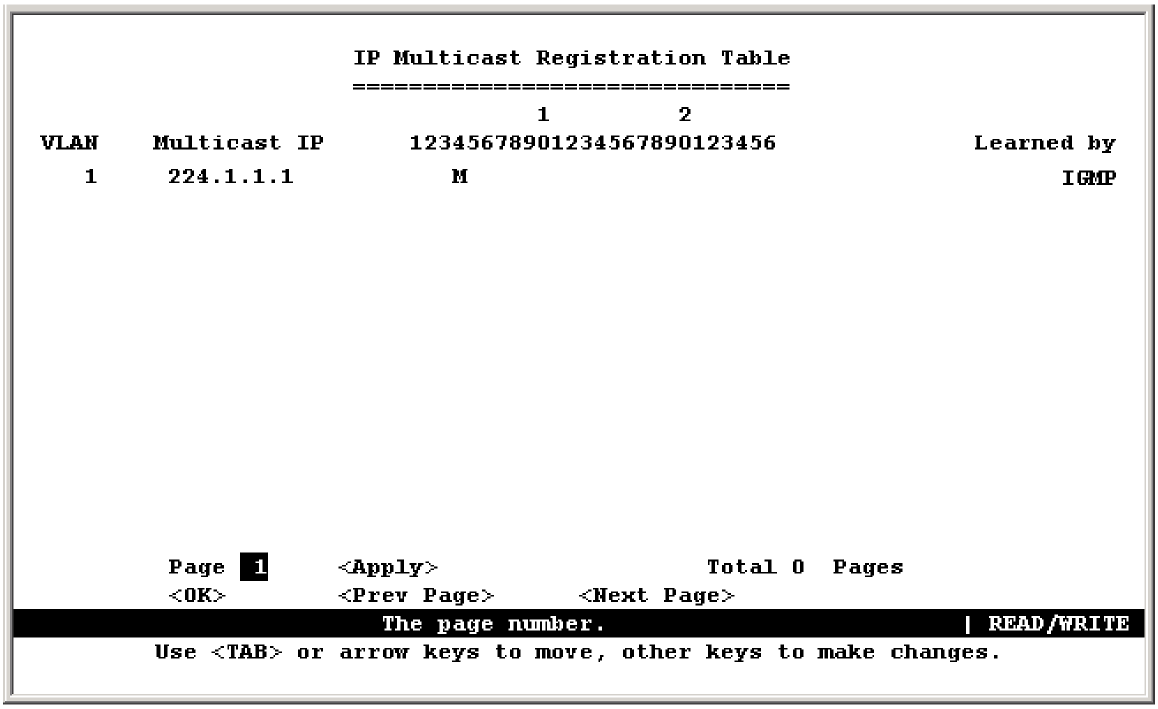


```
                        VLAN Forwarding Information
                        ===========================

          Port           1         2
    VLAN        12345678901234567890123456
    1           SSSSSS SSSSSSS SSSSSSSSSSS                S: Static
    2                 S       S                           D: Dynamic









           Page :  1   <Apply>                   Total: 1  Pages
           <OK>        <Prev Page>      <Next Page>
      Enter page number than press 'Apply' to see VLAN group.       | READ/WRITE
          Use <TAB> or arrow keys to move, other keys to make changes.
```

Note: To scroll through the dynamic registration table, use the <Next Page> and <Prev Page> buttons. To display a specific page, set the page number in the Page field and then press <Apply>.

4.6.5 IP Multicast Registration Table

This table displays all the multicast groups active on the switch, including the multicast IP address and the corresponding VLANs.



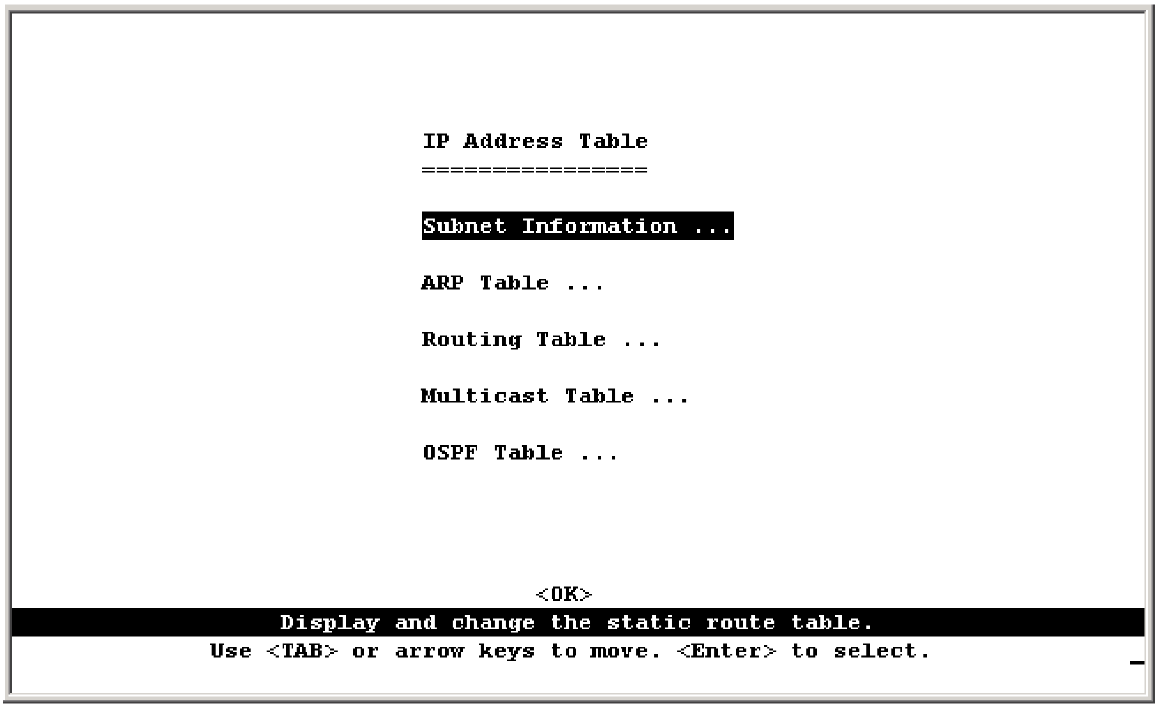
```
                        IP Multicast Registration Table
                        ===============================
                                     1         2
  VLAN    Multicast IP      12345678901234567890123456            Learned by
     1     224.1.1.1           M                                        IGMP











           Page  1     <Apply>                   Total 0  Pages
           <OK>        <Prev Page>      <Next Page>
                          The page number.                         | READ/WRITE
          Use <TAB> or arrow keys to move, other keys to make changes.
```

Parameter	Description
VLAN	A VLAN with host members that have asked to receive the indicated multicast service.
Multicast IP	A source IP address that represents a specific multicast service.
(Multicast Group Port Lists)	The ports that belong to the indicated VLAN group.
Learned by	Shows if this entry was learned dynamically or via IGMP Snooping. An entry is learned dynamically if a multicast packet was seen crossing the port, or via IGMP Snooping if an IGMP registration packet was seen crossing the port.

Note: To scroll through the address table, use the <Next Page> and <Prev Page> buttons. To display a specific page, set the page number in the Page field and then press <Apply>.

4.6.6 IP Address Tables

This menu contains IP subnet information, the ARP cache, routing table, as well as multicast groups and multicast routing information.

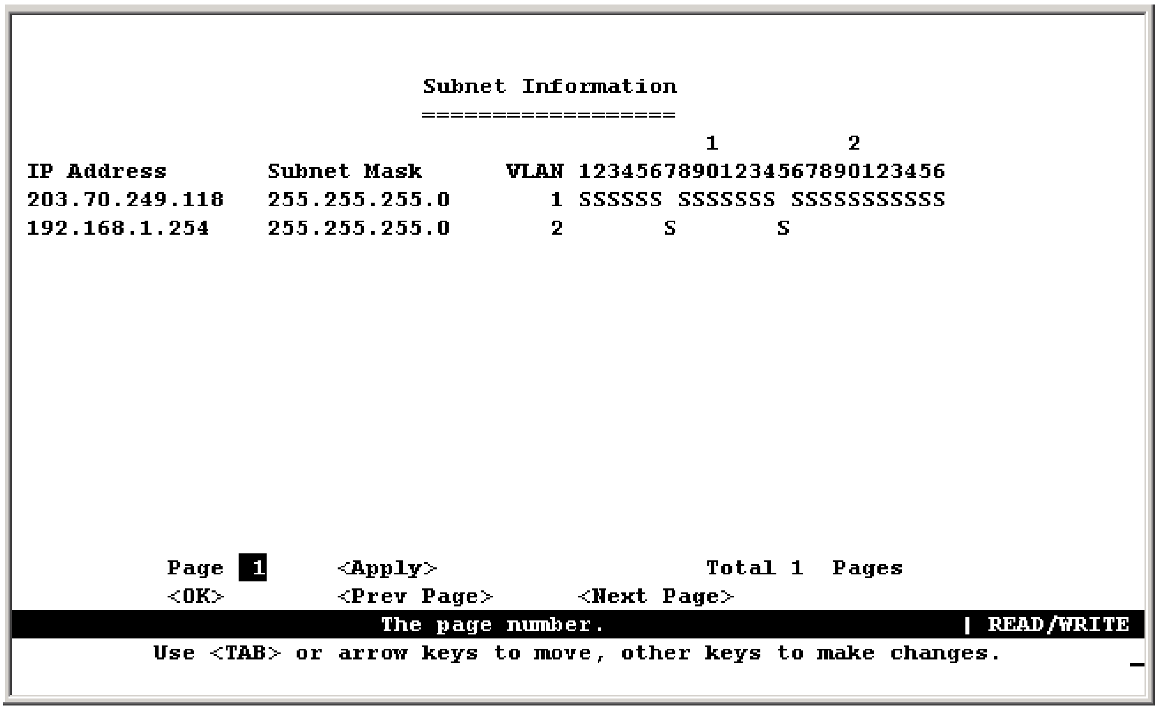


```
IP Address Table
================

Subnet Information ...

ARP Table ...

Routing Table ...

Multicast Table ...

OSPF Table ...



                  <OK>
      Display and change the static route table.
   Use <TAB> or arrow keys to move. <Enter> to select.
```

Menu	Description
Subnet Information	Displays a list of all the IP interfaces configured on this switch.
ARP Table	Shows the IP-to-MAC addresses discovered by ARP.
Routing Table	Shows the routes through which all recognized Ethernet networks (and the corresponding VLAN) can be reached.
Multicast Table	Displays all the multicast groups active on this switch, including the multicast IP address and the corresponding VLANs. Also includes the IGMP registration table, the multicast forwarding cache, and DVMRP routing information.

4.6.6.1 Displaying Subnet Information

You can display a list of all the IP interfaces configured on this switch. This table includes the gateway address, corresponding VLAN, and member ports that use this address.



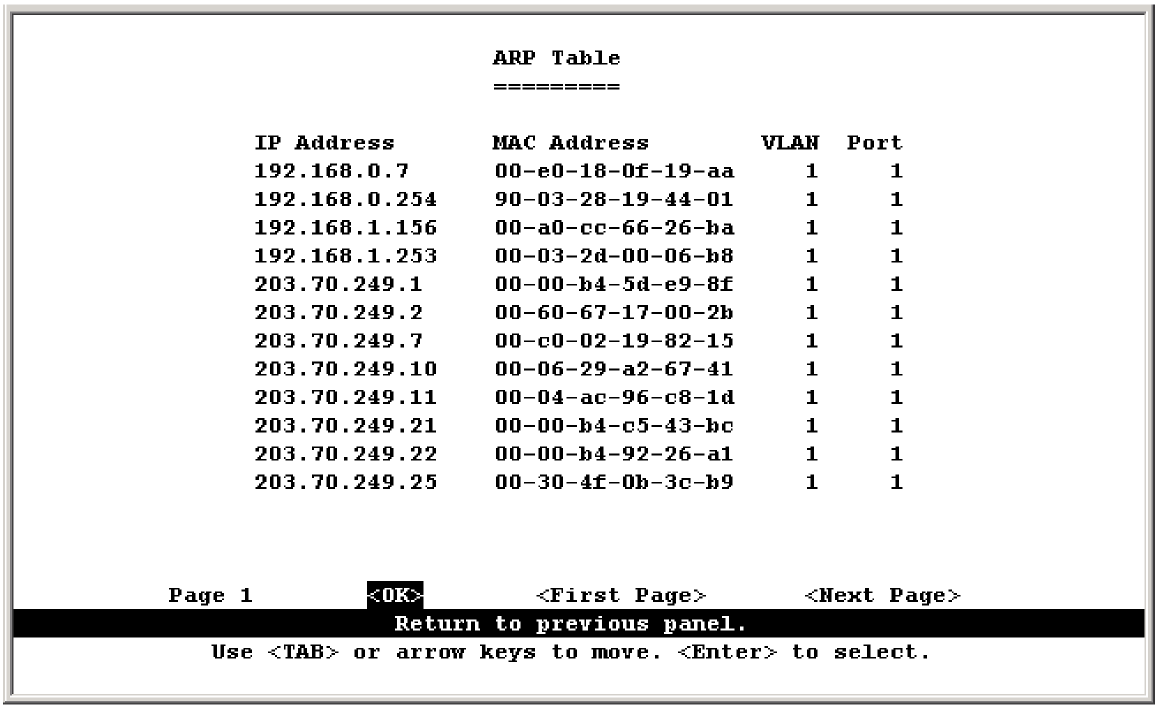
```
                            Subnet Information
                            ==================
                                                1         2
IP Address       Subnet Mask      VLAN 12345678901234567890123456
203.70.249.118   255.255.255.0       1 SSSSSS SSSSSSS SSSSSSSSSSS
192.168.1.254    255.255.255.0       2       S       S









          Page 1     <Apply>                    Total 1  Pages
          <OK>       <Prev Page>      <Next Page>
                         The page number.                         | READ/WRITE
         Use <TAB> or arrow keys to move, other keys to make changes.
```

Parameter	Description
IP Address	The address for an IP interface on this switch.
Subnet Mask	A template that identifies the address bits in the host address used for routing to specific subnets. Each bit that corresponds to a “1” is part of the network / subnet number; and each bit that corresponds to “0” is part of the host number.
VLAN	The VLAN group associated with this IP interface.
(Port Members)	The ports that can be reached through this IP interface.

Note: To scroll through the table, use the <Next Page> and <Prev Page> buttons. To display a specific page, set the page number in the Page field and then select <Apply>.

4.6.6.2 ARP Table

Address Resolution Protocol (ARP) defines a method for finding a host's Ethernet address from its Internet address. This table shows the IP-to-MAC address cache discovered via ARP.



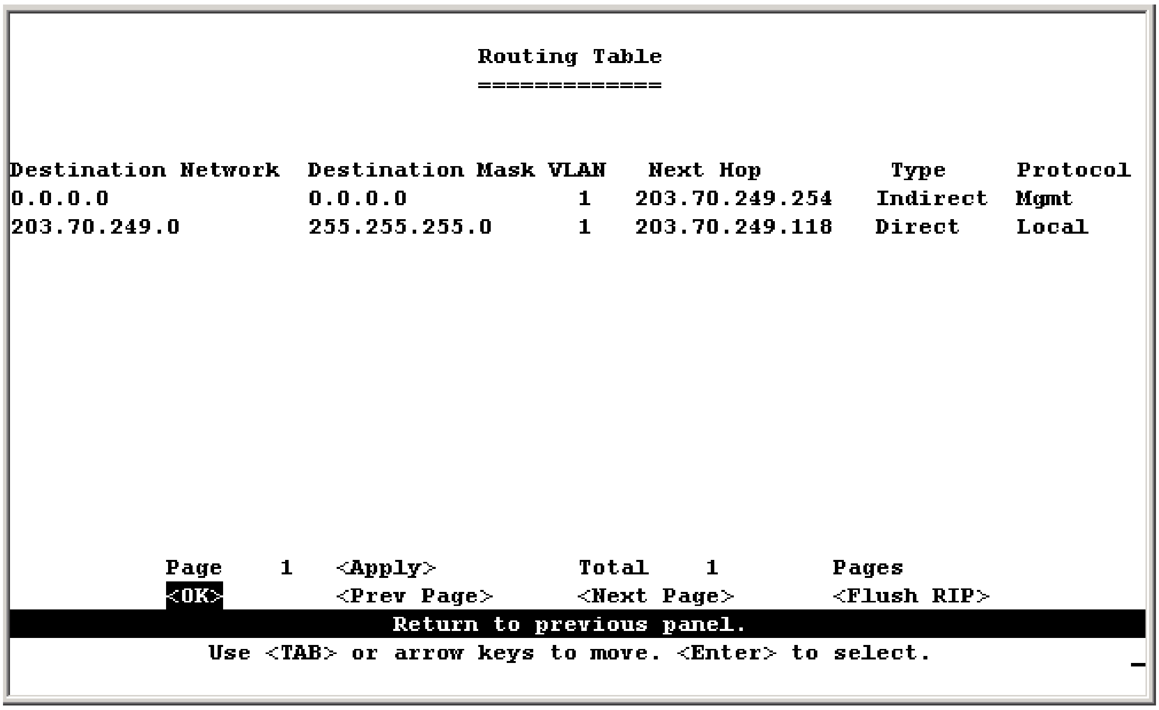
```
                              ARP Table
                              =========

                IP Address       MAC Address        VLAN  Port
                192.168.0.7      00-e0-18-0f-19-aa     1     1
                192.168.0.254    90-03-28-19-44-01     1     1
                192.168.1.156    00-a0-cc-66-26-ba     1     1
                192.168.1.253    00-03-2d-00-06-b8     1     1
                203.70.249.1     00-00-b4-5d-e9-8f     1     1
                203.70.249.2     00-60-67-17-00-2b     1     1
                203.70.249.7     00-c0-02-19-82-15     1     1
                203.70.249.10    00-06-29-a2-67-41     1     1
                203.70.249.11    00-04-ac-96-c8-1d     1     1
                203.70.249.21    00-00-b4-c5-43-bc     1     1
                203.70.249.22    00-00-b4-92-26-a1     1     1
                203.70.249.25    00-30-4f-0b-3c-b9     1     1



          Page 1         <OK>        <First Page>       <Next Page>
                            Return to previous panel.
              Use <TAB> or arrow keys to move. <Enter> to select.
```

Parameter	Description
IP Address	IP addresses for which ARP has resolved the physical address through a broadcast message.
MAC Address	MAC address that maps to the corresponding IP address.
VLAN	The VLAN group to which this host has been assigned.
Port	The port to which this host device is attached.

Note: To scroll through the address table, use the <First Page> and <Next Page> buttons.

4.6.6.3 Routing Table

The Routing Table lists the routes through which all recognized Ethernet networks (and corresponding VLAN) can be reached. This table includes all routes learned through routing protocols or manual configuration.



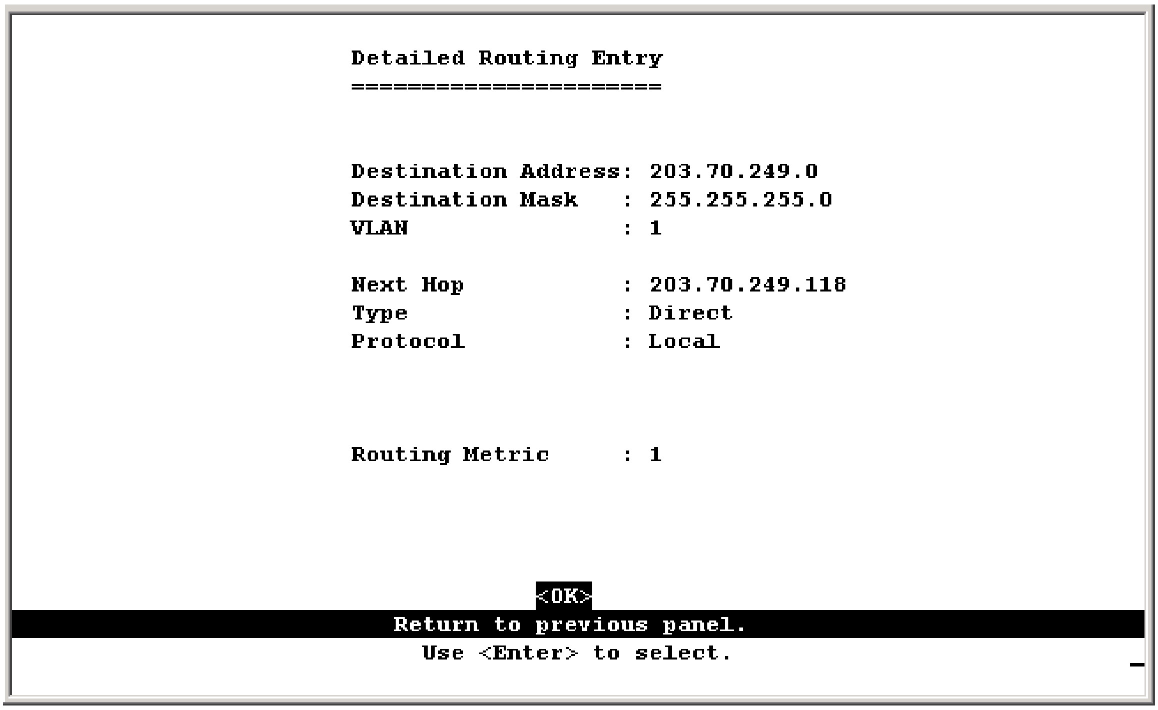
```
                                 Routing Table
                                 =============


Destination Network   Destination Mask VLAN   Next Hop          Type      Protocol
0.0.0.0               0.0.0.0            1   203.70.249.254   Indirect  Mgmt
203.70.249.0          255.255.255.0      1   203.70.249.118   Direct    Local











           Page    1   <Apply>          Total    1        Pages
           <OK>        <Prev Page>      <Next Page>       <Flush RIP>
                                Return to previous panel.
              Use <TAB> or arrow keys to move. <Enter> to select.
```

Parameter	Description
Destination Network	A destination network, subnet or host.
Destination Mask	The subnet mask that specifies the bits to match. A routing entry will be used for a packet if the bits in the address set by the destination mask match the Destination Network.
VLAN	The VLAN within which the gateway or destination address resides.
Next Hop	The IP address of the router at the next hop.
Type	The IP route type for the destination network. This switch supports the following types: Direct - A directly connected subnetwork. Indirect - A remote IP subnetwork or host address. Myself - A switch IP address on a specific IP subnetwork. Bcast - A subnetwork broadcast address. Mcast - An IP multicast address. Invalid - An illegal IP address to be filtered.
Protocol	The route was learned in one of the following ways: Local - Manually configured Mgmt - Set via SNMP ICMP - Obtained via ICMP redirect. RIP - Learned via RIP protocol. Other - Learned by some other method.

Note: Use the <Next Page> and <Prev Page> buttons to scroll through the routing table. To display a specific page, set the page number in the Page field and then press <Apply>. Select <Flush RIP> to clear any routing entries learned through RIP.

4.6.6.3.1 Displaying Detailed Routing Information

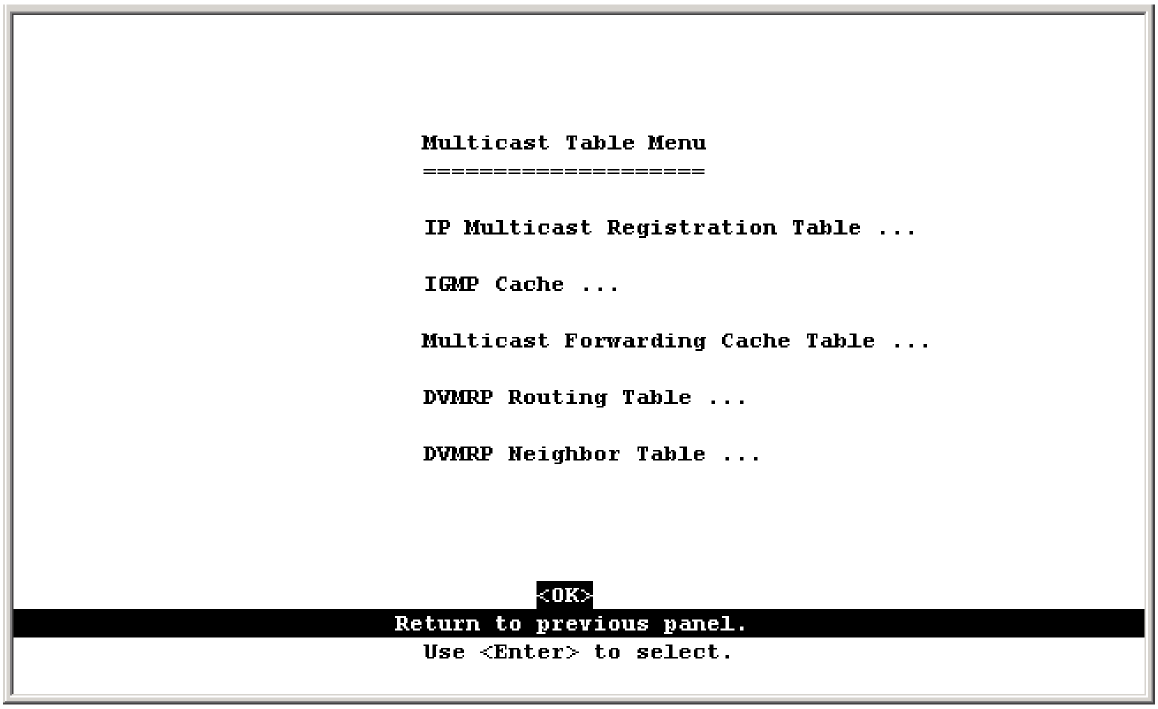
To display detailed routing information, select any entry in the Routing Table with your cursor and press Enter. The following screen will display. All the items displayed on this page are the same as that shown in the Routing Table, except for Routing Metric, which represents a relative measure of the path cost from this switch to the destination network. (Note that this metric depends on the specific routing protocol.)



```
                        Detailed Routing Entry
                        ======================


                        Destination Address: 203.70.249.0
                        Destination Mask   : 255.255.255.0
                        VLAN               : 1

                        Next Hop           : 203.70.249.118
                        Type               : Direct
                        Protocol           : Local



                        Routing Metric     : 1




                                     <OK>
                           Return to previous panel.
                             Use <Enter> to select.
```

4.6.6.4 Multicast Table

You can use this menu to display all the multicast groups currently active on this switch, the IGMP registration table, the multicast forwarding cache, and DVMRP routing information.

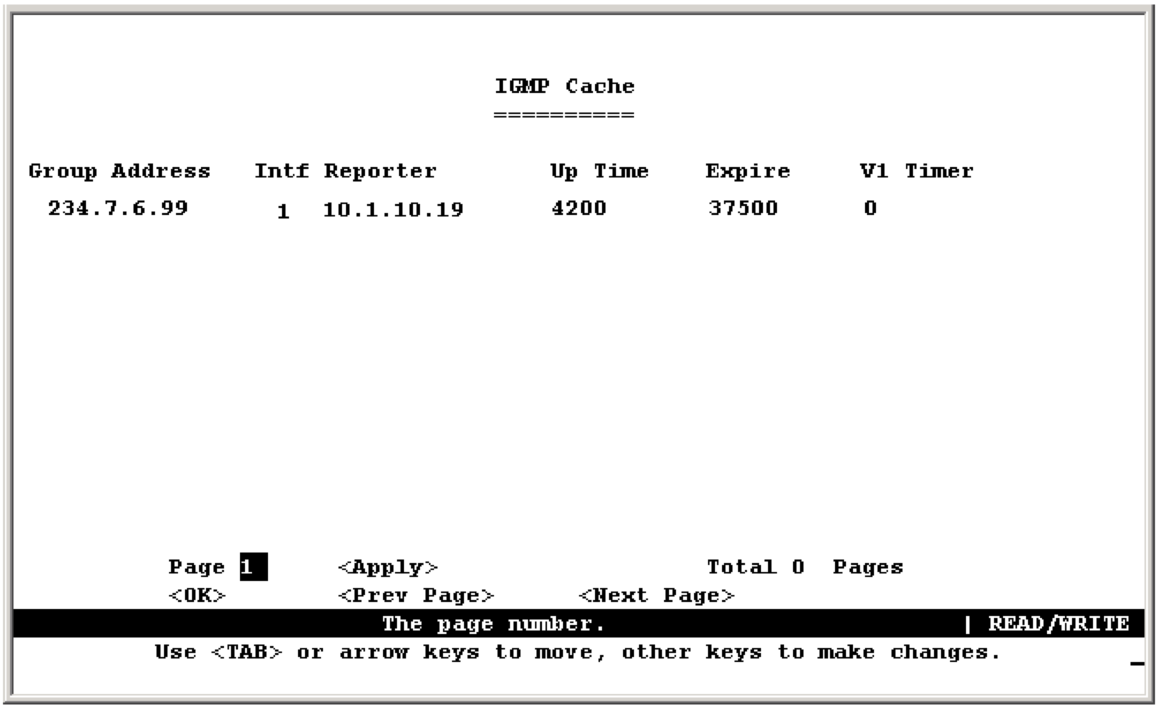


```
Multicast Table Menu
====================

IP Multicast Registration Table ...

IGMP Cache ...

Multicast Forwarding Cache Table ...

DVMRP Routing Table ...

DVMRP Neighbor Table ...



                <OK>
Return to previous panel.
Use <Enter> to select.
```

Parameter	Description
IP Multicast Registration Table	Displays all active multicast groups, including the multicast IP address and the corresponding VLANs. (See 4.6.5 IP Multicast Registration Table.)
IGMP Registration Table	Displays all active multicast groups, including the IP interface each entry appears on, the entry age, and the time left before the entry is aged out.
Multicast Forwarding Cache Table	Displays all active multicast groups, including the multicast source address, the upstream neighbor, the multicast routing protocol, and the entry age.
DVMRP Routing Table	Displays the source address for each known multicast service, the upstream neighbor, the IP interface each entry appears on, the routing metric, and the entry age.
DVMRP Neighbor Table	Displays all the neighbor routers accessible through each IP interface, including the entry age, the time left before the entry is aged out, the protocol version, and the number of routing updates received from each neighboring router.

4.6.6.4.1 Displaying IGMP Registration Table

The switch provides a local registry of active multicast groups for each IP interface, including the age and expiration time for each entry.



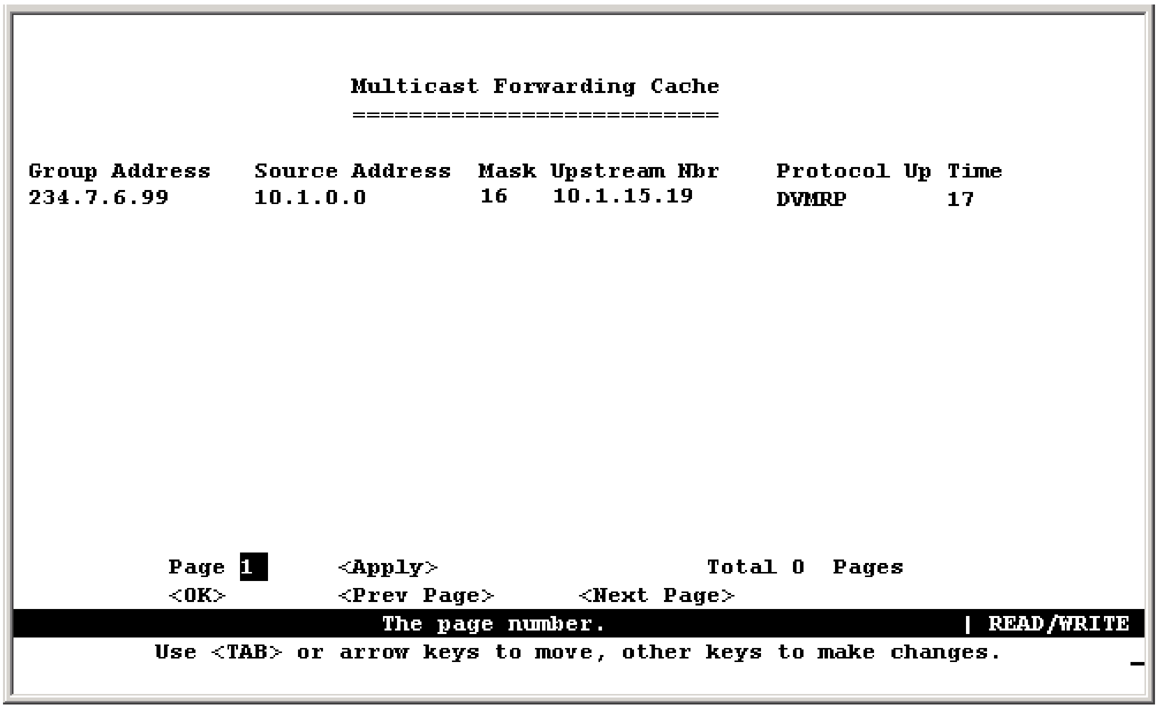
```
                                 IGMP Cache
                                 ==========

Group Address    Intf Reporter        Up Time     Expire      V1 Timer
  234.7.6.99       1   10.1.10.19      4200        37500       0









          Page 1      <Apply>                      Total 0  Pages
          <OK>        <Prev Page>      <Next Page>
                          The page number.                        | READ/WRITE
         Use <TAB> or arrow keys to move, other keys to make changes.
```

Parameter	Description
Group Address	An IP multicast group address with subscribers directly attached or downstream from this switch.
Intf	The IP interface on this switch that has received traffic directed to the IP multicast group address. (See4.6.6.1 Displaying Subnet Information.)
Reporter	IP address of the source of the last membership report received for this multicast group on this interface. If no membership report has been received, this object has the value 0.0.0.0.
Up Time	The time elapsed since this entry was created.
Expire	The time remaining before this entry will be aged out. (The default is 260 seconds.)
V1 Timer	The time remaining until the switch assumes that there are no longer any IGMP Version 1 members on the IP subnet attached to this interface. (The default is 400 seconds.) If the switch receives an IGMP Version 1 Membership Report, it sets a timer to note that there are Version 1 hosts present which are members of the group for which it heard the report. If there are Version 1 hosts present for a particular group, the switch will ignore any Leave Group messages that it receives for that group.

Note: To scroll through the table, use the <Next Page> and <Prev Page> buttons. To display a specific page, set the page number in the Page field and then select <Apply>.

4.6.6.4.2 Displaying the Multicast Forwarding Cache

The switch maintains a cache of multicast routing entries used to calculate the delivery tree in multicast routing protocols. The Multicast Forwarding Cache includes the subnetwork that contains the multicast source and the nearest upstream neighbor for each known multicast group address.



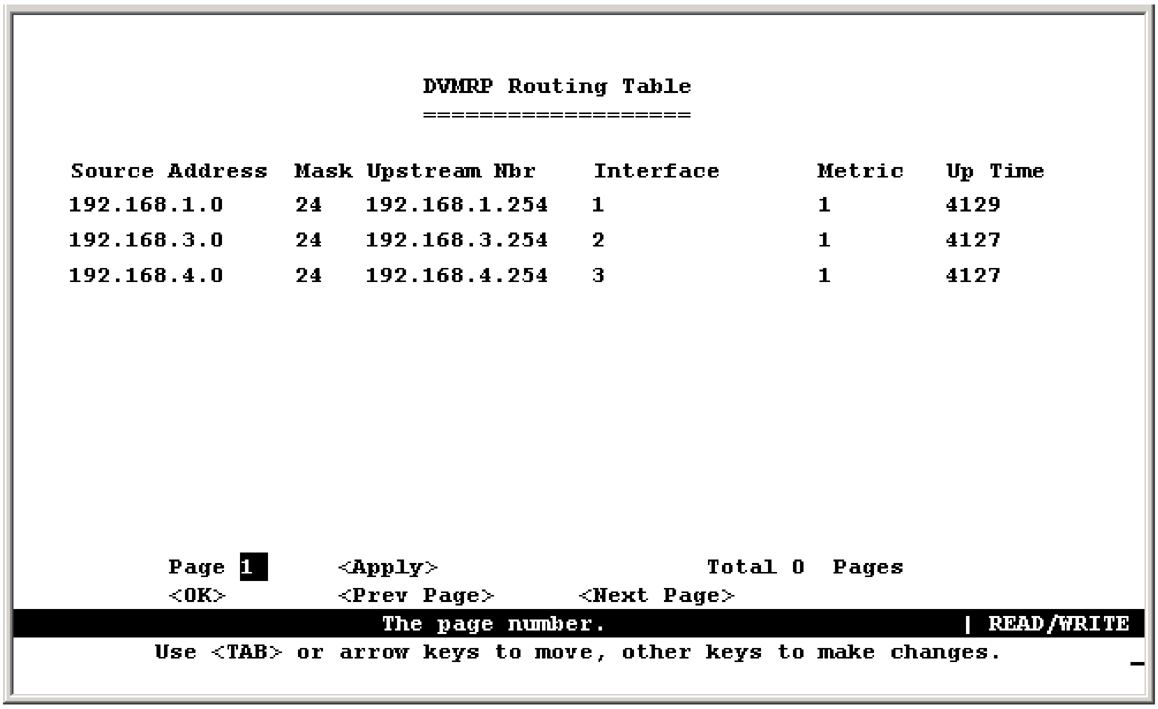
```
                     Multicast Forwarding Cache
                     ==========================

Group Address    Source Address   Mask Upstream Nbr     Protocol Up  Time
234.7.6.99       10.1.0.0         16   10.1.15.19       DVMRP        17









          Page 1       <Apply>                  Total 0  Pages
          <OK>         <Prev Page>      <Next Page>
                          The page number.                      | READ/WRITE
         Use <TAB> or arrow keys to move, other keys to make changes.
```

Parameter	Description
Group Address	An IP multicast group address with subscribers directly attached or downstream from this switch.
Source Address	The IP subnetwork at the root of the multicast delivery tree. This subnetwork contains a known multicast source.
Mask	Subnet mask that is used for the source address. This mask identifies the host address bits used for routing to specific subnets.
Upstream Nbr	The IP address of the network device immediately upstream for this group.
Protocol	The multicast routing protocol associated with this entry.
Up Time	The time elapsed since this entry was created.

Note: To scroll through the table, use the <Next Page> and <Prev Page> buttons. To display a specific page, set the page number in the Page field and then select <Apply>.

4.6.6.4.3 Displaying the DVMRP Routing Table

The DVMRP Routing Table contains all the IP multicast routes learned by the DVMRP protocol. The routes displayed in this table are used by this switch to forward new IP multicast traffic. They do not reflect active multicast flows.



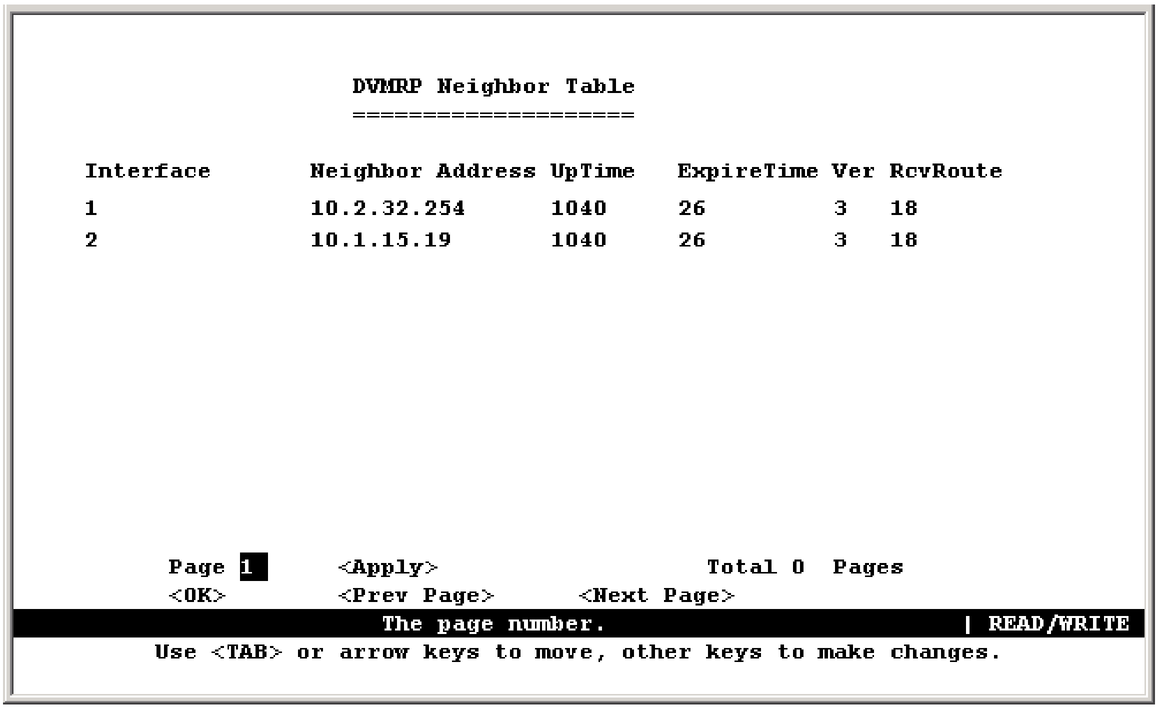
```
                          DVMRP Routing Table
                          ===================

 Source Address  Mask Upstream Nbr    Interface       Metric   Up Time
 192.168.1.0     24   192.168.1.254   1               1        4129
 192.168.3.0     24   192.168.3.254   2               1        4127
 192.168.4.0     24   192.168.4.254   3               1        4127









         Page 1      <Apply>                 Total 0  Pages
         <OK>        <Prev Page>      <Next Page>
                       The page number.                       | READ/WRITE
        Use <TAB> or arrow keys to move, other keys to make changes.
```

Parameter	Description
Source Address	The IP subnetwork at the root of the multicast delivery tree. This subnetwork contains a known multicast source.
Subnet Mask	Subnet mask that is used for the source address. This mask identifies the host address bits used for routing to specific subnets.
Upstream Nbr	The IP address of the network device immediately upstream for this multicast delivery tree.
Intf	The IP interface on this switch that connects to the upstream neighbor. (See 4.6.6.1 Displaying Subnet Information.)
Metric	The metric for this interface used to calculate distance vectors.
Up Time	The time elapsed since this entry was created.

Note: To scroll through the table, use the <Next Page> and <Prev Page> buttons. To display a specific page, set the page number in the Page field and then select <Apply>.

4.6.6.4.4 Displaying the DVMRP Neighbor Table

The DVMRP Neighbor Table contains the switch's DVMRP neighbors, as discovered by receiving DVMRP protocol messages.



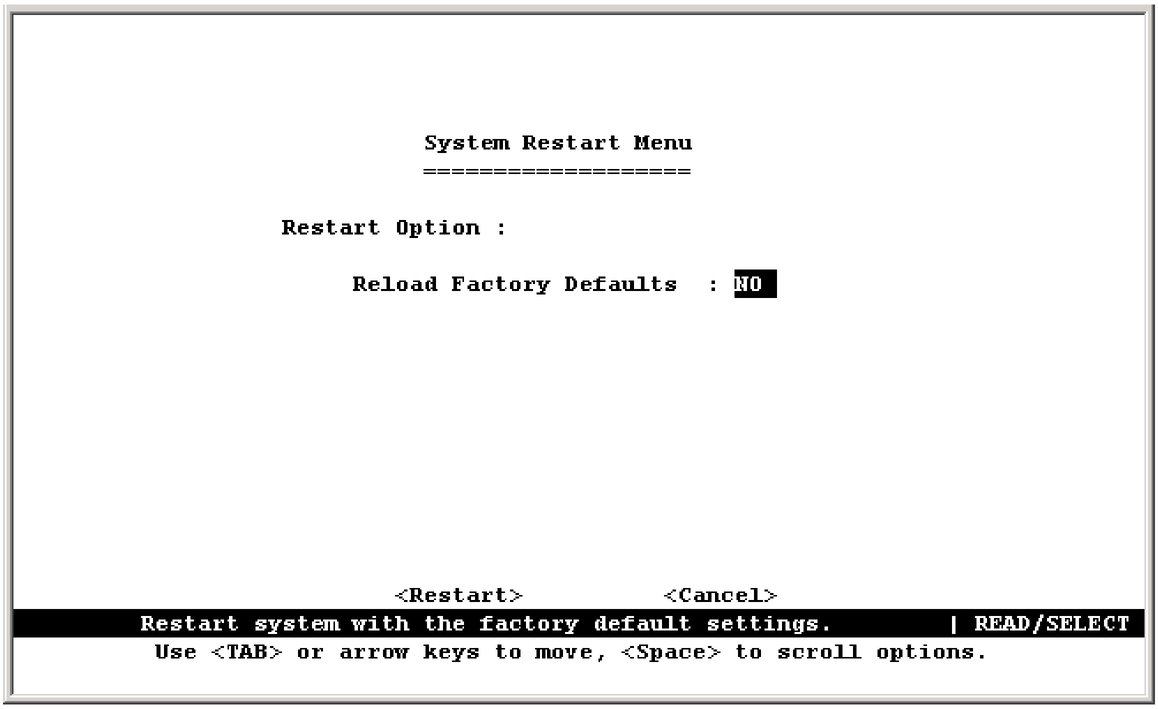
```
                        DVMRP Neighbor Table
                        ====================

     Interface       Neighbor Address UpTime   ExpireTime Ver RcvRoute
     1               10.2.32.254      1040     26         3   18
     2               10.1.15.19       1040     26         3   18











           Page 1      <Apply>                 Total 0  Pages
           <OK>        <Prev Page>      <Next Page>
                          The page number.                  | READ/WRITE
          Use <TAB> or arrow keys to move, other keys to make changes.
```

Parameter	Description
Intf	The IP interface on this switch that connects to the upstream neighbor. (See 4.6.6.1 Displaying Subnet Information.)
Neighbor Address	The IP address of the network device immediately upstream for this multicast delivery tree.
UpTime	The time since this device last became a DVMRP neighbor to this switch.
ExpireTime	The time remaining before this entry will be aged out.
Ver	The neighboring router's DVMRP version number.
RcvRoute	The total number of routes received in valid DVMRP packets from this neighbor. This can be used to diagnose problems such as unicast route injection, as well as giving an indication of the level of DVMRP route exchange activity.

Note: To scroll through the table, use the <Next Page> and <Prev Page> buttons. To display a specific page, set the page number in the Page field and then select <Apply>.

4.7 Resetting the System

Use the Restart command under the Main Menu to reset the management agent. The reset screen is shown below.



```
                    System Restart Menu
                    ===================

          Restart Option :

               Reload Factory Defaults  : NO

                  <Restart>          <Cancel>
         Restart system with the factory default settings.         | READ/SELECT
          Use <TAB> or arrow keys to move, <Space> to scroll options.
```

Parameter	Description
Reload Factory Defaults	Reloads the factory defaults
[Restart]	Restarts the switch.

Note: When restarting the system, it will always run the Power-On Self-Test. It will also retain all system information, unless you select to reload the factory defaults.

4.8 Logging Off the System

Use the Exit command under the Main Menu to exit the configuration program and terminate communications with the switch for the current session.

Chapter 5. Web Interface

5.1 Web-Based Configuration and Monitoring

As well as the menu-driven system configuration program, this switch provides an embedded HTTP Web agent. Using a Web browser you can configure the switch and view statistics to monitor network activity. The Web agent can be accessed by any computer on the network using Internet Explorer 4.0 or above Web browser.

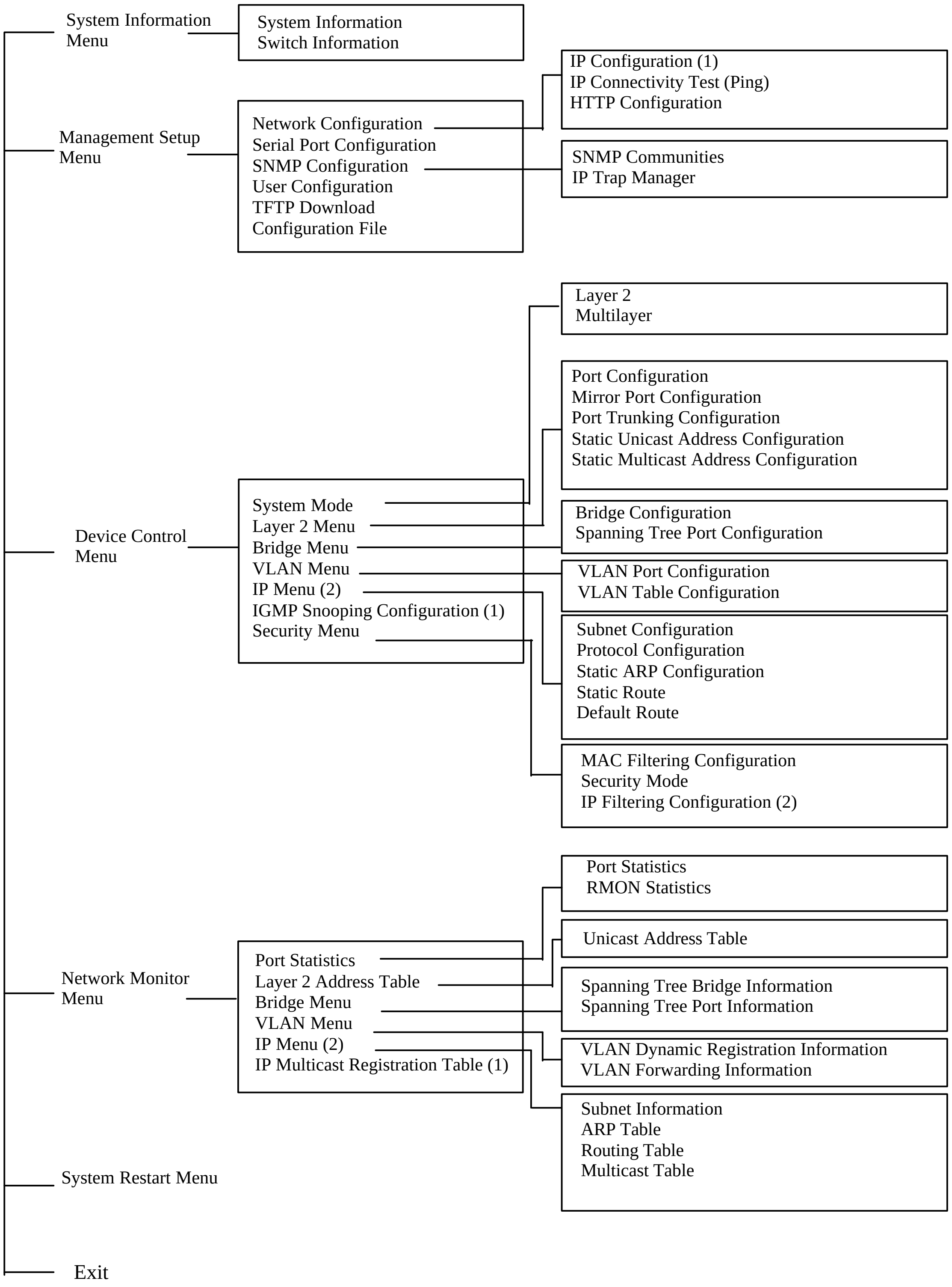
Note: Current firmware version does not support Netscape Navigator.

Prior to accessing the switch from a Web browser, be sure you have first performed the following tasks:

1. Configure it with a valid IP address, subnet mask, and default gateway (for Layer 2 mode) using an out-of-band serial connection or BOOTP protocol. Provide a default gateway for Layer 2 operation(see or a default route for multilayer operation (see 4.5.6.5 Configuring the Default Route).
2. Set a user name and password using an out-of-band serial connection(see 4.4.4 User Login Configuration). Access to the Web agent is controlled by the same user name and password as the on-board configuration program.

Note: If the path between your management station and this switch does not pass through any device that uses the Spanning Tree Algorithm, then you can set the switch port attached to your management station to Fast Forwarding (see 4.5.3.2 Configuring STA for Ports) to improve the switch's response time to management commands issued through the Web interface.

After you enter the user name and password, you will have access to the system configuration program illustrated by the following menu hierarchy:



1.Displayed for layer 2 mode only.
2.Displayed for multilayer mode

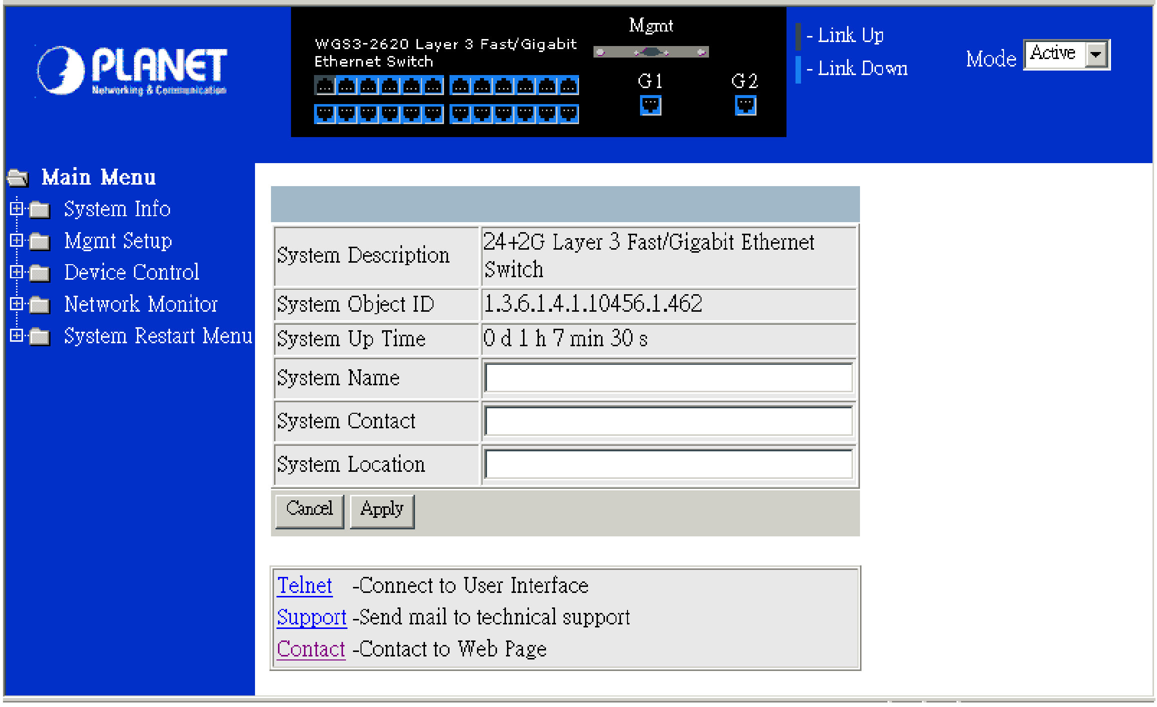
5.2 Navigating the Web Browser Interface

To access the Web-browser interface you must first enter a user name and password. The administrator has Read/Write access to all configuration parameters and statistics. The default user name for the administrator is “admin” with no password.

5.2.1 Home Page

When your Web browser connects with the switch' s Web agent, the home page is displayed as shown below. The home page displays the Main Menu on the left side of the screen and System Information on the right side.

The Main Menu links are used to navigate to other menus and display configuration parameters and statistical data.



System Description	24+2G Layer 3 Fast/Gigabit Ethernet Switch
System Object ID	1.3.6.1.4.1.10456.1.462
System Up Time	0 d 1 h 7 min 30 s
System Name	
System Contact	
System Location	

Telnet -Connect to User Interface
Support -Send mail to technical support
Contact -Contact to Web Page

If this is your first time to access the management agent, you should define a new Administrator name and password, record it and put it in a safe place. Select Mgt Setup / User Cfg. from the Main Menu, and then enter a new name and password for the Administrator. Note that user names and passwords can consist of up to 11 alphanumeric characters and are not case sensitive.

Note: Your are allowed three attempts to enter the correct password; on the third failed attempt the current connection is terminated.

5.2.2 Configuration Options

Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click on the "Apply" button at the bottom of the page to confirm the new setting. The following table summarizes the Web page configuration buttons.

Web Page Configuration Buttons

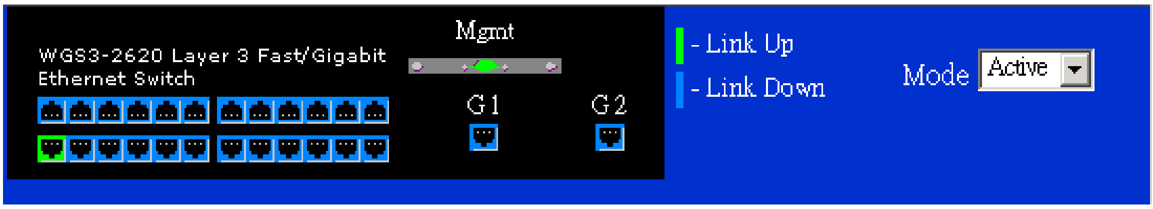
Button	Action
Apply	Sets specified values in the SNMP agent.
Cancel	Cancels specified values prior to pressing the "Apply" button.
Refresh	Immediately updates values from the SNMP agent

Notes:

1. To ensure proper screen refresh, be sure that Internet Explorer 5.0 is configured as follows: Under the menu "Tools / Internet Options / General / Temporary Internet Files / Settings," the setting for item "Check fo r newer versions of stored pages" should be "Every visit to the page."
2. When using Internet Explorer 5.0, you may have to manually refresh the screen after making configuration changes by pressing the browser's refresh button.

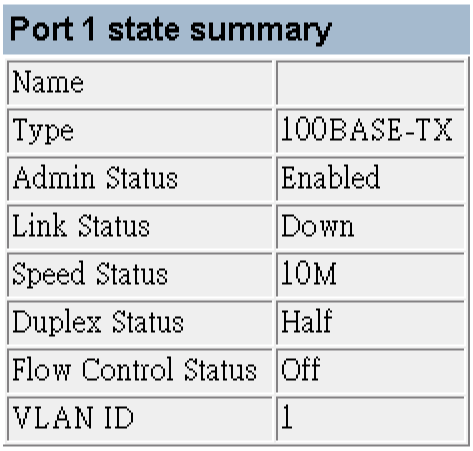
5.3 Panel Display

The Web agent displays an image of the switch' s ports, showing port links and activity. Clicking on the image of a port displays statistics and configuration information for the port. Clicking on the image of the serial port (labeled "Mgmt") displays the Consol e Configuration screen. Clicking on any other part of the front panel displays "Displaying Switch Version Information".



5.3.1 Port State Display

Click on any port to display a summary or port status as shown below, as well as Etherlike statistics.



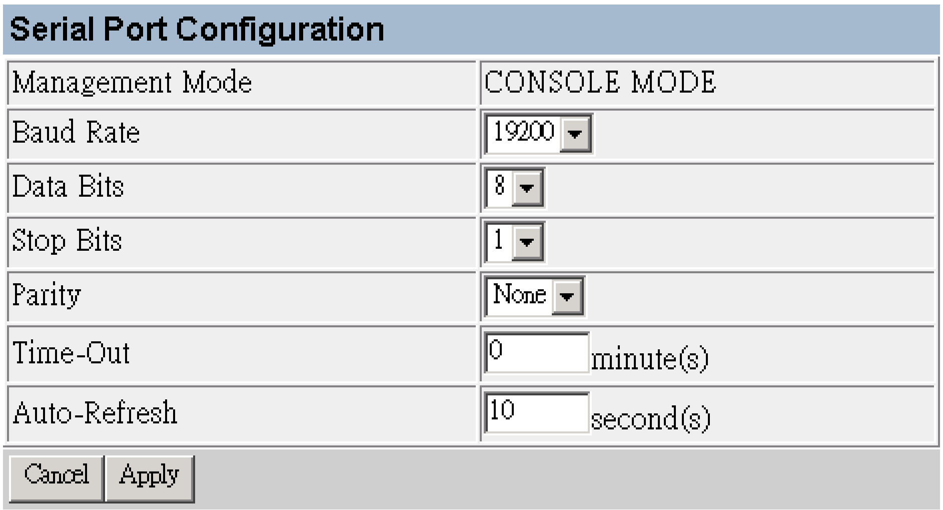
Port 1 state summary

Name	
Type	100BASE-TX
Admin Status	Enabled
Link Status	Down
Speed Status	10M
Duplex Status	Half
Flow Control Status	Off
VLAN ID	1

Parameter	Description
Type	Shows port type as: 100BASE-TX (10BASE-T / 100BASE-TX) 1000BASE-T
Admin Status	Shows if the port is enabled, or has been disabled due to abnormal behavior or for security reasons. See "Configuring Port Parameters".
Link Status	Indicates if the port has a valid connection to an external device.
Speed Status	Indicates the current port speed.
Duplex Status	Indicates the port' s current duplex mode.
Flow Control Status	Shows the flow control type in use. Flow control can eliminate frame loss by "blocking" traffic from end stations connected directly to the switch.
VLAN ID	The VLAN ID assigned to untagged frames received on this port. Use the PVID to assign ports to the same untagged VLAN.

5.3.2 Configuring the Serial Port

If you are having difficulties making an out-of-band console connection to the serial port on the switch, you can display or modify the current settings for the serial port through the Web agent. Click on the serial port icon in the switch image to display or configure these settings, as shown below.



Serial Port Configuration

Management Mode	CONSOLE MODE
Baud Rate	19200
Data Bits	8
Stop Bits	1
Parity	None
Time-Out	0 minute(s)
Auto-Refresh	10 second(s)

Parameter	Default	Description
Management Mode	Console Mode	Indicates that the port settings are for direct console connection.
Baud Rate	19200	The rate at which data is sent between devices. Options : 9600, 19200 and 38400 baud.
Data Bits	8 bits	Sets the data bits of the RS-232 port. Options : 7, 8
Stop Bits	1 bit	Sets the stop bits of the RS-232 port. Options : 1, 2
Parity	none	Sets the parity of the RS-232 port. Options : none/odd/even
Time-Out	0 minutes	If no input is received from the attached device after this interval, the current session is automatically closed. Range : 0 - 100 minutes; where 0 indicates disabled
Auto Refresh	10 second	Sets the interval before a console session will auto refresh the console information, such as Spanning Tree Information, Port Configuration, Port Statistics, and RMON Statistics. Range : 0, or 5-255 seconds; where 0 indicates disabled

5.4 Main Menu

Using the on-board Web agent, you can define system parameters, manage and control the switch, and all its ports, or monitor network conditions. The interface screen includes the menu tree on the left side and a list of commands beneath the image of the switch. The following table briefly describes the selections available from this program.

Menu	Description
System Information Menu	
System Information	Provides basic system description, including contact information.
Switch Information	Shows hardware/firmware version numbers, power status, and expansion modules used in the switch.
Management Setup Menu	
Network Configuration	Includes IP Configuration ^{*1}, Ping facility, and HTTP (Web agent) setup.
Serial Port Configuration	Sets communication parameters for the serial port, including baud rate, console time-out, and screen data refresh interval.
SNMP Configuration	Activates authentication failure traps; and configures community access strings, and trap managers.
User Configuration	Sets the user names and passwords for system access.
TFTP Download	Downloads new version of firmware to update your system (in-band).
Configuration File	Save or restores configuration data based on the specified file.
Device Control Menu	
System Mode	Sets the switch to operate as a Layer 2 switch or as a multilayer routing switch.
Layer 2 Menu	Configures port communication mode, mirror ports, port trunking and static unicast/multicast address.
Bridge Menu	Configures GMRP and GVRP for the bridge, and STA for the global bridge or for specific ports.
VLAN Menu	Configures VLAN settings for specific ports, and defines the port membership for VLAN groups.
IGMP Snooping Configuration ^{*1}	Configures IGMP multicast filtering.
IP Menu ^{*2}	Configures the subnets for each VLAN group, global configuration for unicast and multicast protocols, BOOTP/DHCP relay, static ARP table entries, static routes and the default route.
Security	Restrict access through MAC address or IP address^{*2}
Network Monitor Menu	
Port Statistics	Displays statistics on network traffic passing through the selected port, including information from the Interfaces Group, Ethernet-link MIB, and RMON MIB
Layer 2 Address Table	Contains the unicast address table.
Bridge Menu	Displays Spanning Tree information for the overall bridge and for specified ports.
VLAN Menu	Displays dynamic port registration information for VLANs, as well as all VLAN forwarding information for static and dynamic assignment.

IP Multicast Registration Table *1	Displays all the multicast groups active on this switch, including the multicast IP addresses and corresponding VLANs.
IP Menu *2	Displays all the IP subnets used on this switch, as well as the corresponding VLANs and ports. Also contains the ARP table, routing table and multicast table.
Restart System Menu	Restarts the system with options to reload factory defaults.

*1: Only displays when the switch is set to Layer 2 mode.
*2. Only displays when the switch is set to multilayer mode.

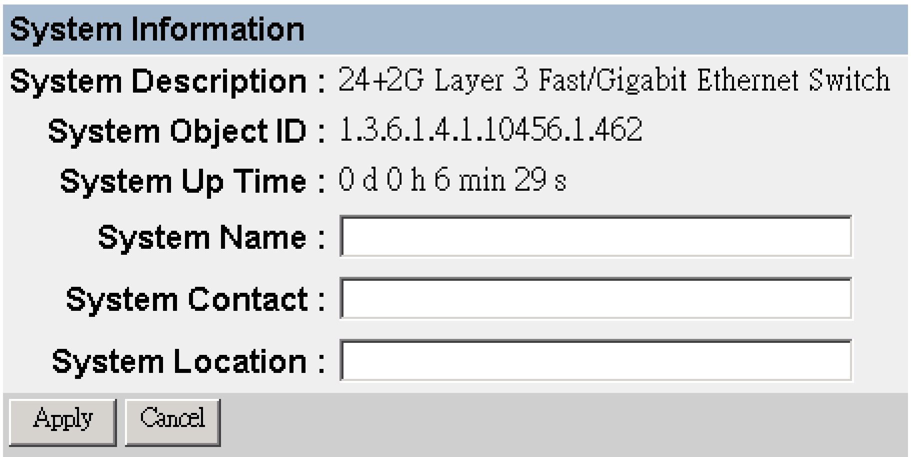
5.5 System Information Menu

Use the System Information Menu to display a basic description of the switch, including contact information, and hardware/firmware versions.

Menu	Description
System Information	Provides basic system description, including contact information.
Switch Information	Shows hardware/firmware version numbers, power status, and expansion modules used in the stack.

5.5.1 Displaying System Information

Use the System Information screen to display descriptive information about the switch, or for quick system identification as shown in the following figure and table.



System Information

System Description : 24+2G Layer 3 Fast/Gigabit Ethernet Switch

System Object ID : 1.3.6.1.4.1.10456.1.462

System Up Time : 0 d 0 h 6 min 29 s

System Name :

System Contact :

System Location :

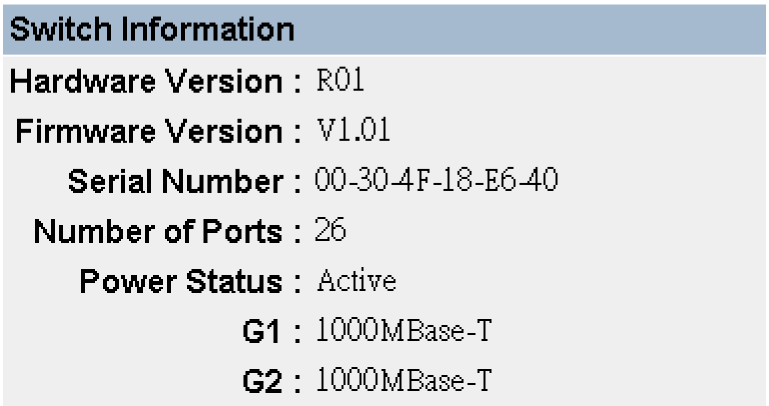
Parameter	Description
System Description	System hardware description.
System Name*.	Name assigned to the switch system
Object ID	MIB II object identifier for switch's network management subsystem.
Location*	Specifies the area or location where the system resides.
Contact*	Contact person for the system.
System Up Time	Length of time the current management agent has been running.

* Maximum string length is 99, but the screen only displays 45 characters. You can use the arrow keys to browse the whole string.

5.5.2 Displaying Switch Version Information

Use the Switch Information screen to display hardware/firmware version numbers for the main board, as well as the power status and modules plugged into the system.

5.5.2.1 Main Board



Switch Information

Hardware Version : R01

Firmware Version : V1.01

Serial Number : 00-30-4F-18-E6-40

Number of Ports : 26

Power Status : Active

G1 : 1000MBase-T

G2 : 1000MBase-T

Parameter	Description
Hardware Version	Hardware version of the main board.
Firmware Version	System firmware version in ROM.
Serial Number	Serial number of the main board.
Number of Ports	Number of ports on this switch
Power Status	Power status for the switch.
Fan Power Status	Shows if power to the fan is active or inactive.
G1, G2	Show Connected type of G1 and G2

5.6 Management Setup Menu

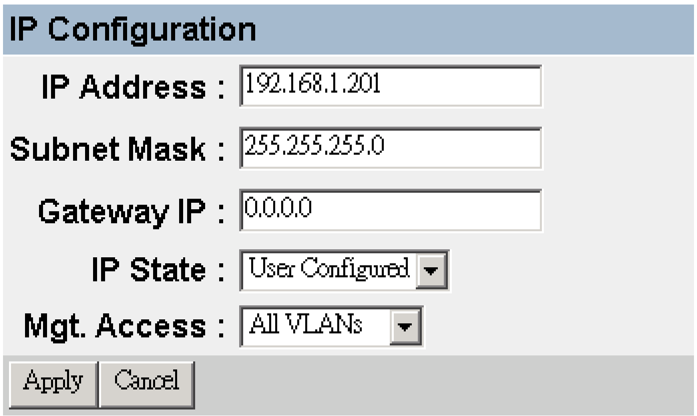
After initially logging onto the system, you can use this menu to configure access rights. You should set user names and passwords (User Configuration). Remember to record them in a safe place. You should also set the community string which controls access to the on-board SNMP agent via in-band management software (SNMP Configuration). The items provided by the Management Setup Menu are described in the following sections.

Menu	Description
Network Configuration	Includes IP setup * and HTTP setup for the on-board Web agent.
Serial Port Configuration	Sets communication parameters for the serial port, including baud rate, console time-out, and screen data refresh interval. (See "Configuring the Serial Port")
SNMP Configuration	Activates authentication failure traps; and configures communities and trap managers.
User Configuration	Sets the user names and passwords for system access.
TFTP Download	Downloads new version of firmware to update your system (in-band).
Configuration File	Saves or restores configuration data based on the specified file.

* Only displays when the switch is set to Layer 2 mode.

5.6.1 Changing the Network Configuration (Layer 2 Mode)

Use the Network Configuration menu to set the bootup option, configure the switch' s Internet Protocol (IP) parameters. The screen shown below is described in the following table.



IP Configuration

IP Address : 192.168.1.201

Subnet Mask : 255.255.255.0

Gateway IP : 0.0.0.0

IP State : User Configured

Mgt. Access : All VLANs

Parameter	Description
Interface Type	Indicates IP over Ethernet.
IP Address	IP address of the switch you are managing. The system supports SNMP over UDP/IP transport protocol. In this environment, all systems on the Internet, such as network interconnection devices and any PC accessing the agent module must have an IP address. Valid IP addresses consist of four numbers, of 0 to 255, and separated by periods. Anything outside of this format will not be accepted by the configuration program.
Subnet Mask	Subnet mask of the switch. This mask identifies the host address bits used for routing to specific subnets.
Gateway IP	Gateway used to pass trap messages from the system' s agent to the management station. Note that the gateway must be defined (when operating at Layer 2) if the management station is located in a different IP segment.
IP State	Specifies whether IP functionality is enabled via manual configuration, or set by Boot Protocol (BOOTP). Options include: USER-CONFIG - IP functionality is enabled based on the default or user specified IP Configuration. (This is the default setting.) BOOTP Get IP - IP is enabled but will not function until a BOOTP reply has been received. BOOTP requests will be periodically broadcasted by the switch in an effort to learn its IP address. (BOOTP values can include the IP address, default gateway, and subnet mask.)
VLAN ID	The VLAN used for management access when "Mgmt VLAN" is selected. See the next item.
Mgt. Access	Specifies which VLAN have access right to its management interface. Options include: All VLANs – All VLANs have access right to its management interface. (This is the default setting.) Mgmt VLAN – Only the specified VLAN have access right to its management interface

Note: When using multilayer mode, refer to "Subnet Configuration" on

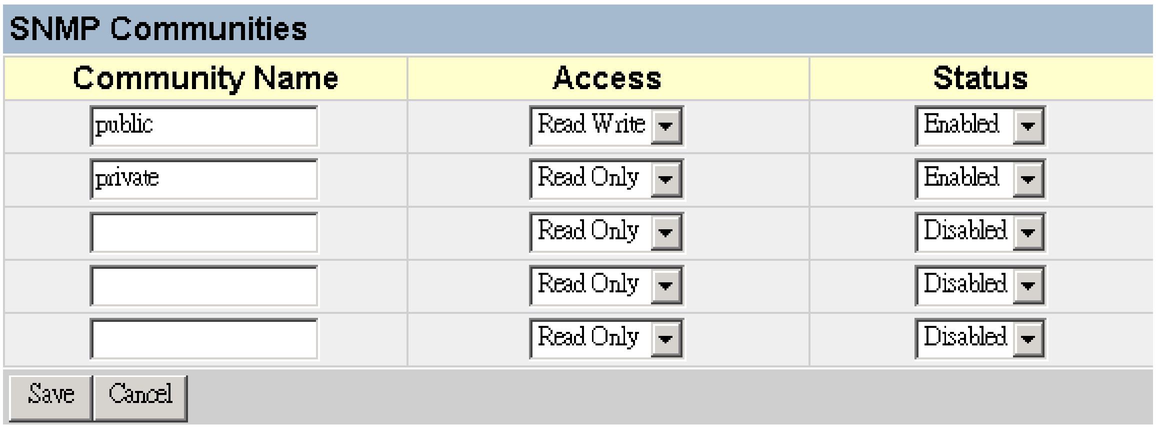
5.7.5.1 Subnet *Configuration*

5.6.2 Assigning SNMP Parameters

Use the SNMP Configuration screen to display and modify parameters for the Simple Network Management Protocol (SNMP). The switch includes an on-board SNMP agent which monitors the status of its hardware, as well as the traffic passing through its ports. A computer attached to the network, called a Network Management Station (NMS), can be used to access this information. Access rights to the agent module are controlled by community strings. To communicate with the switch, the NMS must first submit a valid community string for authentication. The options for configuring community strings and related trap functions are described in the following figures and table.

5.6.2.1 Configuring Community Names

The following figure and table describe how to configure the community strings authorized for management access. Up to 5 community names may be entered.



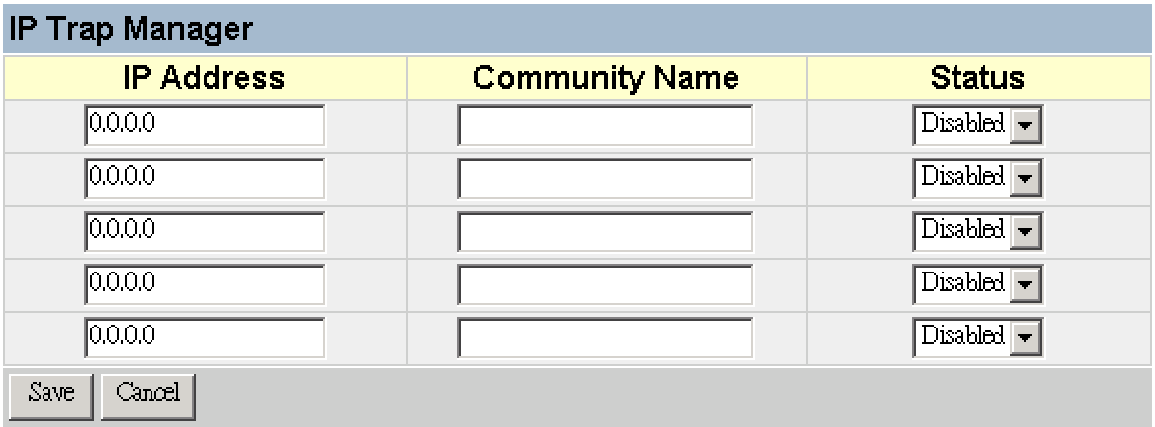
SNMP Communities

Community Name	Access	Status
public	Read Write	Enabled
private	Read Only	Enabled
	Read Only	Disabled
	Read Only	Disabled
	Read Only	Disabled

Parameter	Description
Community Name	A community entry authorized for management access. (The maximum string length is 20 characters.)
Access	Management access is restricted to Read Only or Read/Write.
Status	Displays the administrative status of entry. An entry can only be to enabled or disabled via the console interface.

5.6.2.2 Configuring IP Trap Managers

The following figure and table describe how to specify management stations that will receive authentication failure messages or other trap messages from the switch. Up to 5 trap managers may be entered.



IP Trap Manager

IP Address	Community Name	Status
0.0.0.0		Disabled
0.0.0.0		Disabled
0.0.0.0		Disabled
0.0.0.0		Disabled
0.0.0.0		Disabled

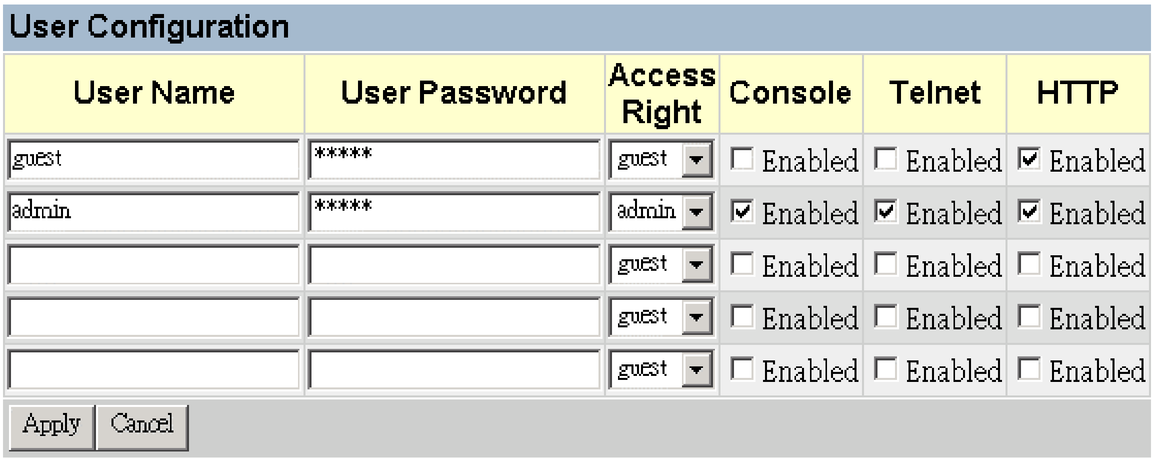
Parameter	Description
IP Address	IP address of the trap manager.
Community Name	A community authorized to receive trap messages.
Status	Displays the administrative status of entry. An entry can only be to enabled or disabled via the console interface.

5.6.3 User Login Configuration

Use the User Configuration screen to restrict management access based on user names and passwords. The default administrator (admin) has write access for parameters governing the on-board agent. You should therefore assign a password to the administrator as soon as possible, and store it in a safe place.

5.6.3.1 Displaying the Current User Configuration

Use this menu to display the names and access rights for people authorized to manage the switch.



User Configuration

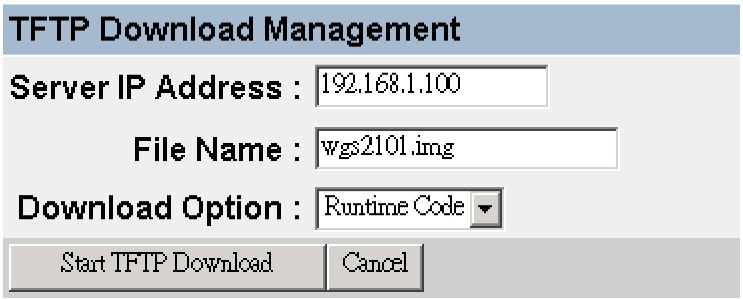
User Name	User Password	Access Right	Console	Telnet	HTTP
guest	*****	guest	□ Enabled	□ Enabled	☑ Enabled
admin	*****	admin	☑ Enabled	☑ Enabled	☑ Enabled
		guest	□ Enabled	□ Enabled	□ Enabled
		guest	□ Enabled	□ Enabled	□ Enabled
		guest	□ Enabled	□ Enabled	□ Enabled

Parameter	Description
User Name*	Specifies a user authorized management access to the switch via the console, Telnet or HTTP. An entry can only be deleted via the console interface.
User Password*	Password associated with this entry.
Access Right	ADMIN: Read/Write for all screens. GUEST: Read Only for all screens.
Console	Authorizes management via the console.
Telnet	Authorizes management via Telnet.
HTTP	Authorizes management via HTTP.

*These entries can consist of up to 15 alphanumeric characters and are not case sensitive.

5.6.4 Downloading System Software

Use the TFTP Download menu to load software updates to permanent flash ROM in the switch. The download file should be a binary file or an image file; otherwise the agent will not accept it. The success of the download operation depends on the accessibility of the TFTP server and the quality of the network connection. After downloading the new software, the agent will automatically restart itself. Parameters shown on this screen are indicated in the following figure and table



TFTP Download Management

Server IP Address : 192.168.1.100

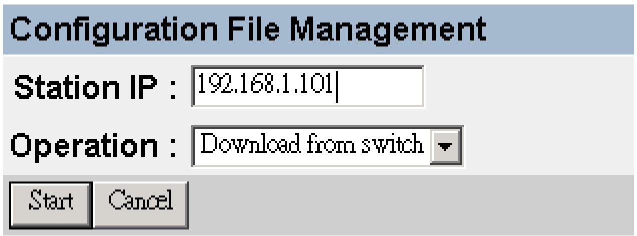
File Name : wgs2101.img

Download Option : Runtime Code

Parameter	Description
Server IP Address	IP address of a TFTP server.
File Name	The binary file or image file to download.
Download Option	Specify the file to be Runtime Code or POST Code
Start TFTP Download	Issues request to TFTP server to download the specified file.

5.6.5 Saving or Restoring the System Configuration

Use the Configuration File menu to save the switch configuration settings to a file on a TFTP client. The file can be later downloaded to the switch to restore the switch's settings. The success of the operation depends on the accessibility of the TFTP client and the quality of the network connection. Parameters shown on this screen are indicated in the following figure and table.



Configuration File Management

Station IP : 192.168.1.101

Operation : Download from switch

Parameter	Description
Station IP	IP address of a PC running TFTP client software.
Operation	Download from switch – Downloads the current switch configuration to a file on the client PC. Upload to switch – Uploads a configuration file to the switch from the client PC.

Note: Saving and restoring switch configuration settings can then be initiated by using any TFTP client utility, such as the command line utility included in Windows NT/2000/XP. For example, using Windows NT, from a DOS window command prompt, enter the TFTP command in the form:

TFTP [-i] host [GET : PUT] source [destination]

To transfer a file –

1. On Switch: Specify the IP address of the TFTP client, and select "Download from switch" or "Upload to Switch." Then select <Start> from the menu to start.
2. On TFTP Client: Set the mode to <binary>, specify the IP address of the target switch and the directory path / name of the file to transfer. Then start transferring the configuration from the TFTP client or the switch and wait until the transfer completes.

For example, type "tftp -i 203.70.249.118 GET source wgs3.txt" on Windows 2000's command prompt to download switch's configuration and type "tftp –i 203.70.249.118 PUT wgs3.txt" to upload the configuration file to switch.

5.7 Device Control Menu

The Device Control menu is used to control a broad range of functions, including port mode, port mirroring, port trunking, Spanning Tree, Virtual LANs, IP subnets, multicast filtering, and routing protocols. Each of the setup screens provided by these configuration menus is described in the following sections.

Menu	Description
Layer 2 Menu	Configures port communication mode, mirror ports, port trunking, and static addresses.
Bridge Menu	Configures the Spanning Tree Protocol for the bridge or for specific ports, GMRP and GVRP for automatic registration of multicast and VLAN groups, traffic class priority threshold, and address aging time.
VLAN Menu	Configures VLAN settings for specific ports, and defines the port membership for VLAN groups.
IGMP Snooping Configuration[1]	Configures IGMP multicast filtering.
IP Menu[2]	Configures the subnets for each VLAN group, global configuration for ARP and Proxy ARP, unicast and multicast protocols, static ARP table entries, static routes and the default route.
Security Menu	Configures MAC and IP[2] Address filtering.

1: Only displayed for Layer 2 mode.
2: Only displayed for multilayer mode.
(Note that this menu includes IGMP Snooping Configuration.)

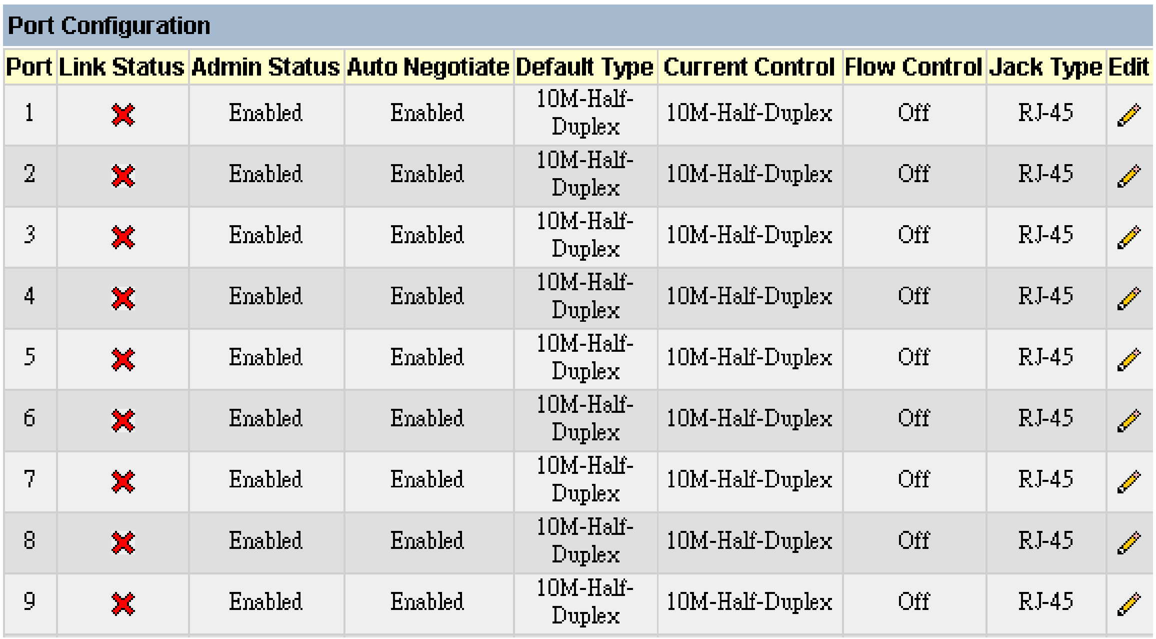
5.7.1 Layer 2 Menu

The Layer 2 menu contains options for port configuration, port mirroring, and port trunking. These menu options are described in the following sections.

Menu	Description
Port Configuration	Enables any port, enables/disables flow control, and sets communication mode to auto-negotiation, full duplex or half duplex.
Mirror Port Configuration	Sets the source and target ports for mirroring.
Port Trunking Configuration	Specifies ports to group into aggregate trunks.
Static Unicast Address Table	Used to manually configure host MAC addresses in the unicast table.
Static Multicast Address Table	Used to manually configure host MAC addresses in the multicast table.

5.7.1.1 Configuring Port Parameters

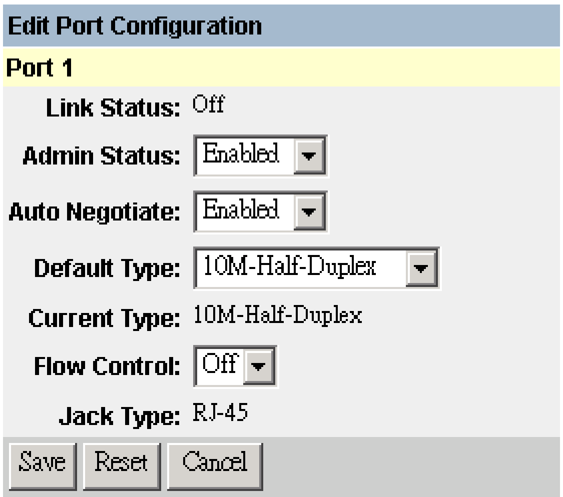
Use the Port Configuration menu to display and Edit icon to set communication parameters for any port on the switch, including administrative status, auto-negotiation, default communication speed and duplex mode, as well as flow control in use.



Port Configuration

Port	Link Status	Admin Status	Auto Negotiate	Default Type	Current Control	Flow Control	Jack Type	Edit
1	✗	Enabled	Enabled	10M-Half-Duplex	10M-Half-Duplex	Off	RJ-45	✏
2	✗	Enabled	Enabled	10M-Half-Duplex	10M-Half-Duplex	Off	RJ-45	✏
3	✗	Enabled	Enabled	10M-Half-Duplex	10M-Half-Duplex	Off	RJ-45	✏
4	✗	Enabled	Enabled	10M-Half-Duplex	10M-Half-Duplex	Off	RJ-45	✏
5	✗	Enabled	Enabled	10M-Half-Duplex	10M-Half-Duplex	Off	RJ-45	✏
6	✗	Enabled	Enabled	10M-Half-Duplex	10M-Half-Duplex	Off	RJ-45	✏
7	✗	Enabled	Enabled	10M-Half-Duplex	10M-Half-Duplex	Off	RJ-45	✏
8	✗	Enabled	Enabled	10M-Half-Duplex	10M-Half-Duplex	Off	RJ-45	✏
9	✗	Enabled	Enabled	10M-Half-Duplex	10M-Half-Duplex	Off	RJ-45	✏

Click ✏, the following table will be show to allow setting each port' s parameter.



Edit Port Configuration

Port 1

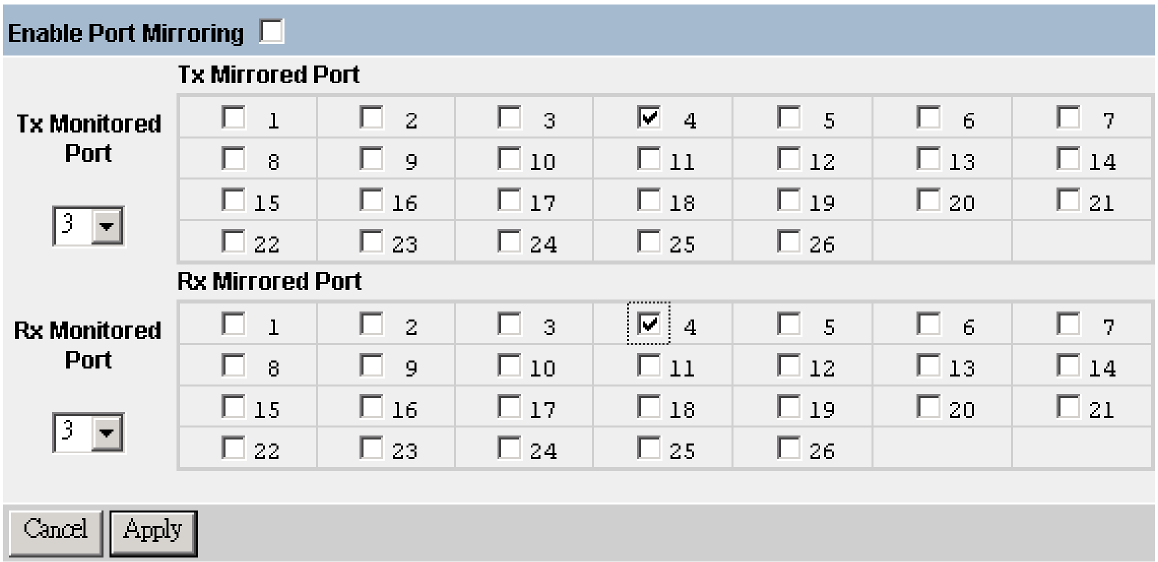
Link Status:	Off
Admin Status:	Enabled
Auto Negotiate:	Enabled
Default Type:	10M-Half-Duplex
Current Type:	10M-Half-Duplex
Flow Control:	Off
Jack Type:	RJ-45

Parameter	Default	Description
Link Status		Indicates if the port has a valid connection to an external device.
Admin Status	Enabled	Allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also disable a port for security reasons.
Auto Negotiate*	Enabled	Enables or disables auto-negotiation for the following features Port Type · Speed · Duplex Mode · Flow Control 10/100BASE-T · auto · auto · auto 1000BASE-T · 1000M · full duplex · auto The 10/100BASE-TX ports can auto-negotiate the speed to 10/100 Mbps, and the transmission mode to half/full duplex. The 1000BASE-T ports are all fixed at the indicated speed and duplex mode. All ports can auto-negotiate flow control.
Default Type	10M-Half-Duplex	If auto-negotiation is disabled, the port will be set to the indicated speed and duplex mode.
Current		Type Indicates the current speed and duplex mode.
Flow Control	Disabled	Used to enable or disable flow control. Flow control can eliminate frame loss by "blocking" traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex and IEEE 802.3x for full-duplex. Note that flow control should not be used if a port is connected to a hub.
Jack Type		Shows the jack type for each port. Ports 1-24: RJ-45 Ports 25-26: RJ-45
Edit		Click ✎ to edit communication parameters.

5.7.1.2 Using a Port Mirror for Analysis

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner. When mirroring port traffic, note that the target port must be included in the same VLAN as the source port. (See “5.7.3.2 VLAN Table Configuration”)

You can use the Mirror Configuration screen to mirror one or more ports to the monitor port as shown below.



Enable Port Mirroring □

Tx Monitored Port: 3

Tx Mirrored Port

□ 1	□ 2	□ 3	☑ 4	□ 5	□ 6	□ 7
□ 8	□ 9	□ 10	□ 11	□ 12	□ 13	□ 14
□ 15	□ 16	□ 17	□ 18	□ 19	□ 20	□ 21
□ 22	□ 23	□ 24	□ 25	□ 26		

Rx Monitored Port: 3

Rx Mirrored Port

□ 1	□ 2	□ 3	☑ 4	□ 5	□ 6	□ 7
□ 8	□ 9	□ 10	□ 11	□ 12	□ 13	□ 14
□ 15	□ 16	□ 17	□ 18	□ 19	□ 20	□ 21
□ 22	□ 23	□ 24	□ 25	□ 26		

Parameter	Description
Enable	Port Mirror Enables or disables the mirror function.
TX Mirrored Port	The port whose transmitted traffic will be mirrored.
TX Monitored Port	The port that will duplicate the transmitted traffic appearing on the mirrored port.
RX Mirrored Port	The port whose received traffic will be mirrored.
RX Monitored Port	The port that will duplicate the received traffic appearing on the mirrored port

Note: You can mirror multiple ports to a single port to view traffic such as that crossing a port trunk. However, note that some packets may be dropped for moderate to heavy loading.

5.7.1.3 Configuring Port Trunks

Ports can be combined into an aggregate link to increase the bandwidth of a network connection or ensure fault recovery. You can configure trunks between any two switches. The RJ-45 ports on this switch can be grouped into a trunk consisting of two, four or eight ports, creating an aggregate bandwidth up to 400, 800 or 1600 Mbps when operating at full duplex. Beyond balancing the load across each port in the trunk, the additional ports provide redundancy by taking over the load if another port in the trunk should fail. However, before making any physical connections between devices, use the Trunk Configuration menu to specify the trunk on the devices at both ends. When using a port trunk, remember that:

¡ EThe ports used in a trunk must all be RJ-45. The ports that can be assigned to the same trunk are listed below:

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

¡ EPorts can only be assigned to one trunk.

¡ EThe ports at both ends of a connection must be configured as trunk ports.

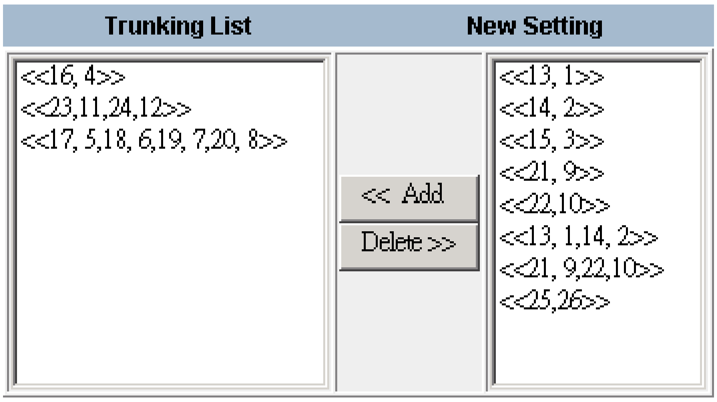
¡ EThe ports at both ends of a trunk must be configured in an identical manner, including communication mode and VLAN assignments.

¡ EAll the ports in a trunk have to be treated as a whole when moved from/to, added to, or deleted from, a VLAN.

¡ EThe Spanning Tree Algorithm will treat all the ports in a trunk as a whole.

¡ EEnable the trunk prior to connecting any cable between the switches to avoid creating a loop.

Use the Trunk Configuration screen to set up port trunks as shown below:



Trunking List

<<16, 4>>
<<23,11,24,12>>
<<17, 5,18, 6,19, 7,20, 8>>

New Setting

<<13, 1>>
<<14, 2>>
<<15, 3>>
<<21, 9>>
<<22,10>>
<<13, 1,14, 2>>
<<21, 9,22,10>>
<<25,26>>

Parameter	Description
Trunk List	The port groups currently configured as trunks.
New Setting	The port groups that can still be configured as trunks.

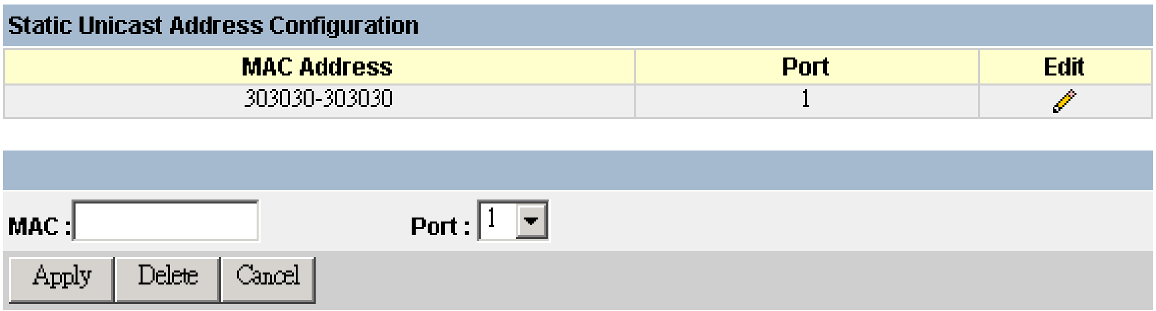
To add a trunk, highlight a port group in the New Setting list and press Add. To delete a trunk, highlight a port group in the Trunk List and press Delete. Before disconnecting a port trunk, take the following steps:

¡ EBefore removing a port trunk via the configuration menu, you must disable all the ports in the trunk or remove all the network cables. Otherwise, a loop may be created.

¡ ETo disable a single link within a port trunk, you should first remove the network cable, and then disable both ends of the link via the configuration menu. This allows the traffic passing across that link to be automatically distributed to the other links in the trunk, without losing any significant amount of traffic.

5.7.1.4 Static Unicast Address Table

The Static Unicast Address Table can be used to assign the MAC address for a host device to a specific port on this switch. Static unicast addresses are never aged out, and cannot be learned by another port. If any packets with a source address specified in this table enter another port, they will be dropped. The Static Unicast Address Table is described in the following figure and table.



Static Unicast Address Configuration

MAC Address	Port	Edit
303030-303030	1	✎

MAC :

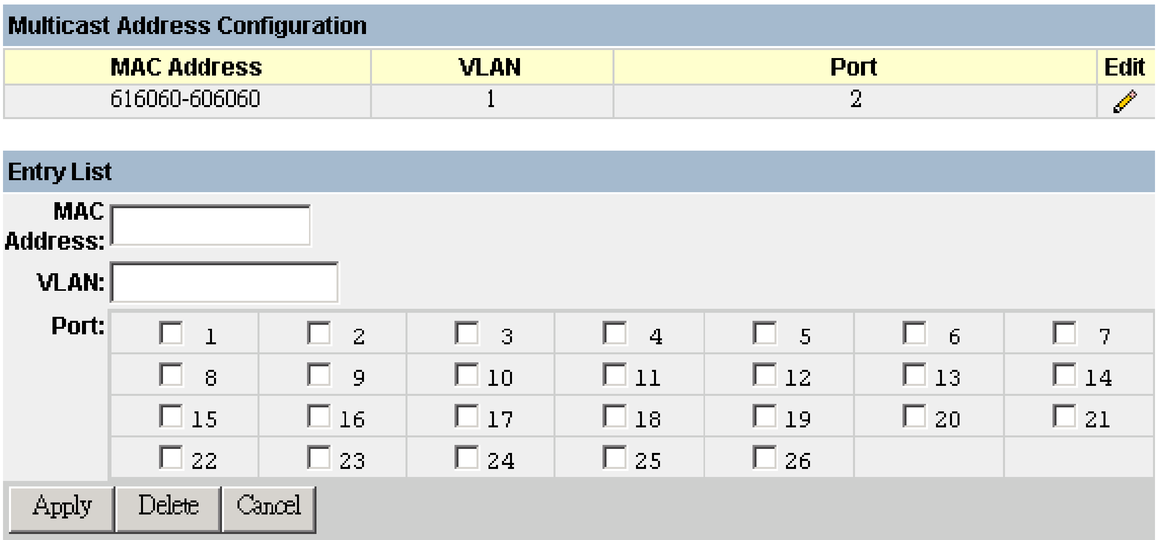
Port : 1

Parameter	Description
MAC Address	The MAC address of a host device attached to this switch.
Port	The port to which the host device is attached.

Note: To assign an address to a specific port, enter it in the MAC Address field, select the corresponding port, and press Save. To delete an address, click ✎ and press Delete for the required entry.

5.7.1.5 Configuring the Static Multicast Address Table

The Static Multicast Address Table can be used to assign a destination MAC address (and the corresponding ports) to the VLAN group used for a specific multicast service. Static multicast addresses are never aged out, and traffic with these addresses can be forwarded only to ports specified in this table.



Multicast Address Configuration

MAC Address	VLAN	Port	Edit
616060-606060	1	2	✎

Entry List

MAC Address:

VLAN:

Port:

□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7
□ 8	□ 9	□ 10	□ 11	□ 12	□ 13	□ 14
□ 15	□ 16	□ 17	□ 18	□ 19	□ 20	□ 21
□ 22	□ 23	□ 24	□ 25	□ 26		

Parameter	Description
MAC Address	The destination MAC address for a multicast service.
VLAN	The VLAN corresponding to this multicast service.
Port.	The ports to which this multicast traffic can be forwarded

Note: To assign a destination MAC address to one or more ports, enter its address and the corresponding VLAN, select the required ports, and then press Apply. To delete an address, click ✎ and press Delete for the required entry. To modify an address, press ✎ for the required entry to copy the configuration to the edit fields, make any necessary changes, then press Apply.

5.7.2 Using the Bridge Menu

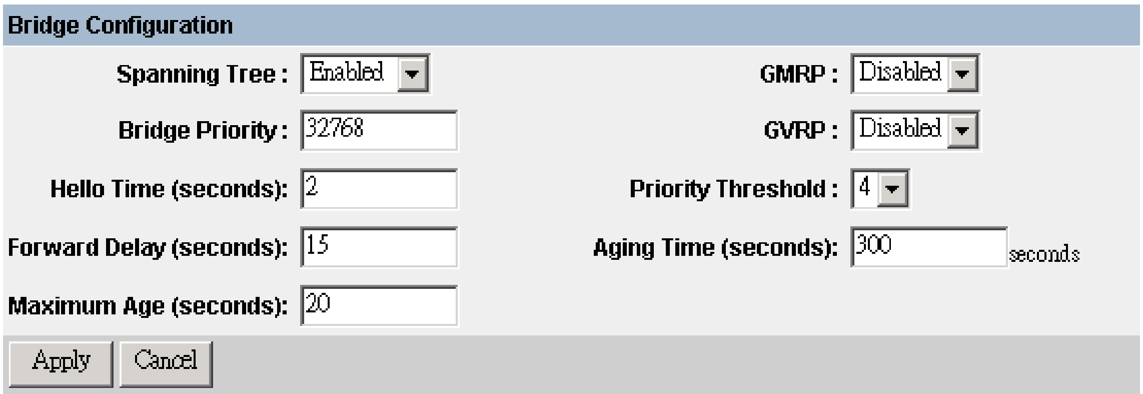
The Bridge menu is used to configure settings for the Spanning Tree Algorithm, as well as the global bridge settings for GMRP (GARP Multicast Registration Protocol) and GVRP (GARP VLAN Registration Protocol), traffic classes priority threshold, and address aging time.

The Spanning Tree Algorithm can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links that automatically take over when a primary link goes down. For a more detailed description of how to use this algorithm, refer to "6.1.3 Spanning Tree Algorithm".

Menu	Description
Bridge Configuration	Contains global bridge settings for STA (including bridge priority, hello time, forward delay, maximum message age), GMRP, GVRP, traffic class priority threshold, and address aging time.
STA Port Configuration	Contains STA settings for individual ports, including port priority, path cost, and fast forwarding

5.7.2.1 Configuring Global Bridge Settings

The following figure and table describe bridge configuration for STA, GMRP, GVRP, priority threshold, and address aging time.



Bridge Configuration

Spanning Tree : Enabled

Bridge Priority : 32768

Hello Time (seconds): 2

Forward Delay (seconds): 15

Maximum Age (seconds): 20

GMRP : Disabled

GVRP : Disabled

Priority Threshold : 4

Aging Time (seconds): 300 seconds

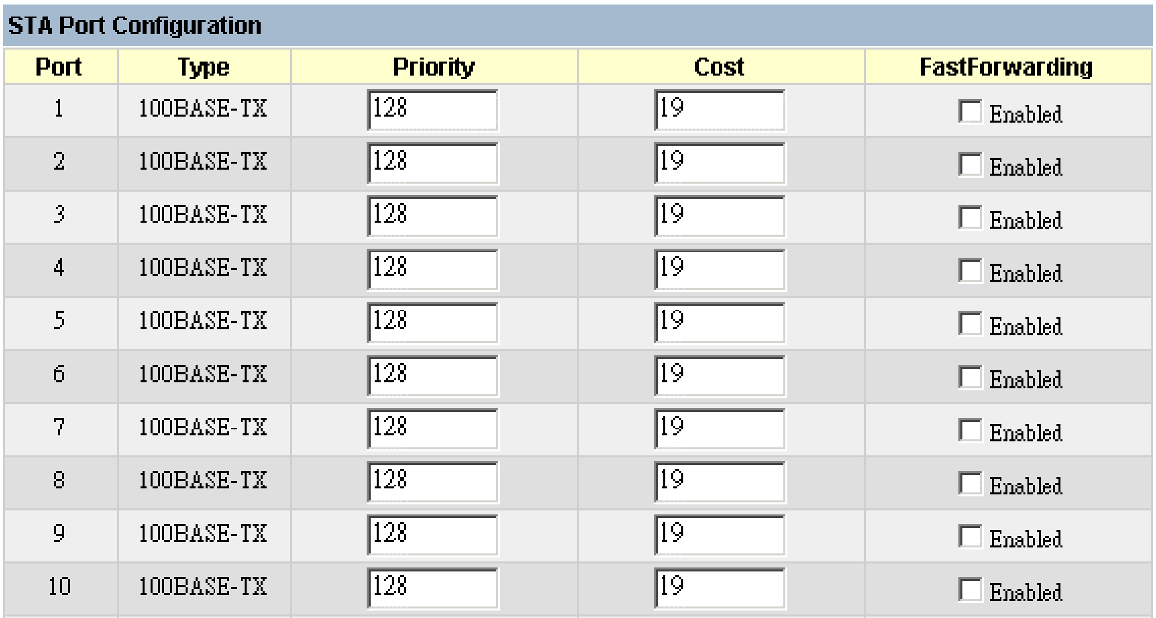
Parameter	Default	Description
Spanning Tree	Enabled	Enable this parameter to participate in a STA compliant network.
Bridge Priority	32,768	Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. Enter a value from 0 - 65535. Remember that the lower the numeric value, the higher the priority.
Hello Time	2	Time interval (in seconds) at which the root device transmits a configuration message.

		The minimum value is 1. The maximum value is the lower of 10 or [(Max. Message Age / 2) -1].
Forward Delay	15	The maximum time (in seconds) the root device will wait before changing states (that is, listening to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The maximum value is 30. The minimum value is the higher of 4 or [(Max. Message Age / 2) + 1].
Maximum (Message) Age	20	The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. The minimum value is the higher of 6 or [2 x (Hello Time + 1)]. The maximum value is the lower of 40 or [2 x (Forward Delay - 1)].
GMRP	Disabled	GARP Multicast Registration Protocol (GMRP) allows network devices to register endstations with multicast groups. If GMRP is globally enabled for the switch, then you can individually enable or disable GMRP for a specific port. See "5.7.3.1 VLAN Port Configuration". IGMP and IGMP Snooping also provide multicast filtering. For multilayer mode, the full IGMP protocol set is automatically enabled/disabled along with DVMRP. (See " 6.4.2 IGMP Protocol", "Configuring DVMRP", and " 5.7.4 Configuring IGMP Snooping".)
GVRP	Disabled	GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. This function should be enabled to permit automatic VLAN registration and to support VLANs which extend beyond the local switch. If GVRP is globally enabled for the switch, then you can individually enable or disable GVRP for a specific port. See "5.7.3.1 VLAN Port Configuration".
Priority Threshold*	4	This switch supports Quality of Service (QoS) by using two priority queues, with Weighted Fair Queuing for each port. Up to 8 separate traffic classes are defined in IEEE 802.1p. Therefore, any packets with a priority equal to or higher than this threshold are placed in the high priority queue.
(Address) Aging Time	300	Timeout period in seconds for aging out dynamically learned forwarding information. Range: 10 – 1000000 seconds

* You can use "5.7.3.1 VLAN Port Configuration" to configure the default priority for each port.

5.7.2.2 Configuring STA for Ports

The following figure and table describe port STA configuration.



STA Port Configuration

Port	Type	Priority	Cost	FastForwarding
1	100BASE-TX	128	19	□ Enabled
2	100BASE-TX	128	19	□ Enabled
3	100BASE-TX	128	19	□ Enabled
4	100BASE-TX	128	19	□ Enabled
5	100BASE-TX	128	19	□ Enabled
6	100BASE-TX	128	19	□ Enabled
7	100BASE-TX	128	19	□ Enabled
8	100BASE-TX	128	19	□ Enabled
9	100BASE-TX	128	19	□ Enabled
10	100BASE-TX	128	19	□ Enabled

Parameter	Default	Description
Type		Shows port type as: 100BASE-TX : 10BASE-T / 100BASE-TX 1000BASE-T : 1000BASE-T
Priority	128	Defines the priority for the use of a port in the STA algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. The range is 0 - 255.
(Path) Cost	100/19/4	This parameter is used by the STA algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) The default and recommended range is: Ethernet: 100 (50~600) Fast Ethernet: 19 (10~60) Gigabit Ethernet: 4 (3~10) The full range is 0 – 65535.
Fast Forwarding*	Enabled	This parameter is used to enable/disabled the Fast Spanning Tree mode for the selected port. In this mode, ports skip the Blocked, Listening and Learning states and proceed straight to Forwarding.

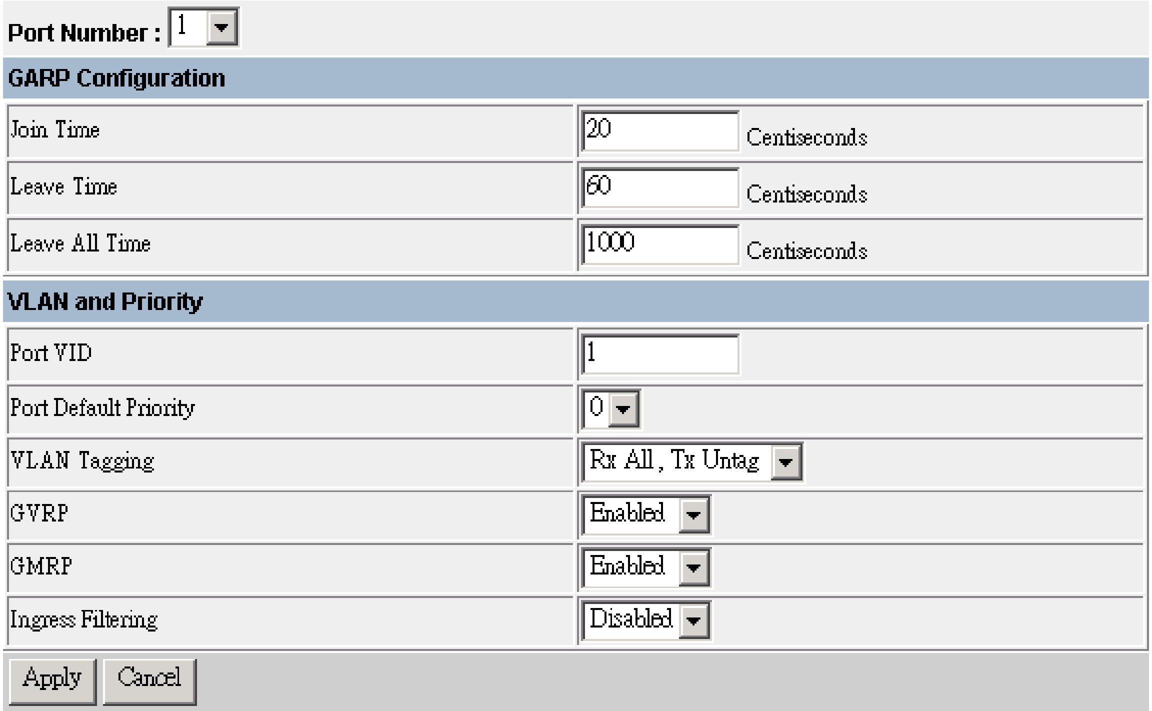
* Since end-nodes cannot cause forwarding loops, they can pass through the Spanning Tree state changes more quickly than allowed by standard convergence time. Fast Forwarding can achieve quicker convergence for end-node workstations and servers, and also overcome other STA related timeout problems. (Remember that Fast Forwarding should only be enabled for ports connected to an end-node device.)

5.7.3 Configuring Virtual LANs

You can use the VLAN configuration menu to assign any port on the switch to any of up to 256 LAN groups. In conventional networks with routers, broadcast traffic is split up into separate domains. Switches do not inherently support broadcast domains. This can lead to broadcast storms in large networks that handle traffic such as IPX or NetBEUI. By using IEEE 802.1Q compliant VLANs, you can organize any group of network nodes into separate broadcast domains, thus confining broadcast traffic to the originating group. This also provides a more secure and cleaner network environment. For more information on how to use VLANs, see “6.3 Virtual LANs”. The VLAN configuration screens are described in the following sections.

5.7.3.1 VLAN Port Configuration

You can use the VLAN Port Configuration screen to configure GARP, the default VLAN identifier, default port priority, VLAN tagging on outgoing frames, GVRP and GMRP status, and filtering for incoming frames for VLAN groups this port does not belong to.



Port Number : 1

GARP Configuration

Join Time	20 Centiseconds
Leave Time	60 Centiseconds
Leave All Time	1000 Centiseconds

VLAN and Priority

Port VID	1
Port Default Priority	0
VLAN Tagging	Rx All, Tx Untag
GVRP	Enabled
GMRP	Enabled
Ingress Filtering	Disabled

Parameter	Default	Description
GARP Configuration[1]		Group Address Registration Protocol is used by GVRP and GMRP to register or deregister client attributes for client services within a bridged LAN.
Join Time	20	The interval (centiseconds) between transmitting requests/queries to participate in a group.
Leave Time	60	The interval (centiseconds) a port waits before leaving a group. This time should be set to more than twice the join time. This ensures that after a Leave or LeaveAll message has been issued, the applicants can rejoin before the port actually leaves the group.

Leave All Time	1000	The interval (centiseconds) between sending out a LeaveAll query message for group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group.

1:The default values for the GARP timers are independent of the media access method or data rate. These values should not changed unless you are experiencing some difficulties with GMRP or GVRP registration/deregistration.

Parameter	Default	Description
VLAN and Priority		These fields set the default values for VLANs, port priority, GVRP and GMRP.
Port VID	1	The VLAN ID assigned to untagged frames received on this port.
Port Default Priority[2]	0	Set the default ingress priority to any value beneath the priority threshold to specify the low priority queue, or to any value equal to or above this threshold to specify the high priority queue.
VLAN Tagging3	Layer 2 - Rx All, Tx All Multilayer – Rx All, Tx Untag	Indicates whether or not VLAN tags will be included on frames transmitted out of this port. The options include: Rx All: Accepts all frames, tagged or untagged. Rx Untag: Only accepts untagged frames. Tx All: If PVID and frame tag are same, sends tagged frame, otherwise send untagged. Tx Untag: Sends only untagged frames.
Port GVRP	Enabled	Enables or disables GVRP for this port. When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports. Note that GVRP must be enabled globally for the switch before this setting can take effect. (See " 5.7.2.1 Configuring Global Bridge *Settings*".)
Port GMRP	Enabled	Enables or disables GMRP for this port. When enabled, this port will allow endstations to register with multicast groups using GMRP. Note that GMRP must be enabled for the switch before this setting can take effect. IGMP and IGMP Snooping also provide multicast filtering. For multilayer mode, the full IGMP protocol set is automatically enabled/disabled along with DVMRP. (See " 6.4.2 IGMP Protocol", " Configuring DVMRP" and " 5.7.4 Configuring IGMP Snooping".)
Ingress Filtering[4]	Disabled	If enabled, incoming frames for VLANs which do not include this ingress port in their member set will be discarded at the ingress port.

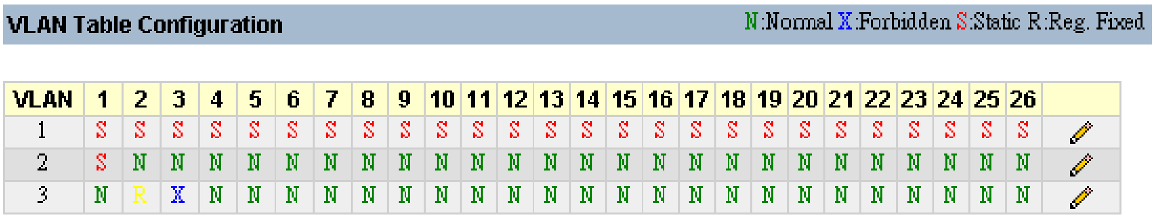
2:This switch supports Quality of Service (QoS) by using two priority queues, with Weighted Fair Queuing for each port. Inbound frames that do not have VLAN tags are tagged with the input port's default ingress user priorit y, and then placed in the appropriate priority queue at the output port. The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in the low priority queue of the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.)

3:If you want to create a small port-based VLAN for just one or two switches, you can assign ports to the same untagged VLAN (and use a separate connection where a VLAN crosses the switches). However, to participate in a VLAN group that extends beyond this switch, we recommend using the VLAN ID for that group (using VLAN tagging for Layer 2 mode, or a common PVID for multilayer mode). When operating the switch in Layer 2 mode, ports assigned to a large VLAN group that crosses several switches must use VLAN tagging. But when operating in multilayer mode, this switch does not currently support tagging, so you should set the PVID to the same value at both ends of the link (if the device you are attaching to is VLAN-aware), and configure an IP interface for this VLAN if you need to connect it to other groups. (This limitation will be removed for future firmware versions.)

4:This control does not affect VLAN independent BPDU frames, such as GVRP or STP. However, they do affect VLAN dependent BPDU frames, such as GMRP.

5.7.3.2 VLAN Table Configuration

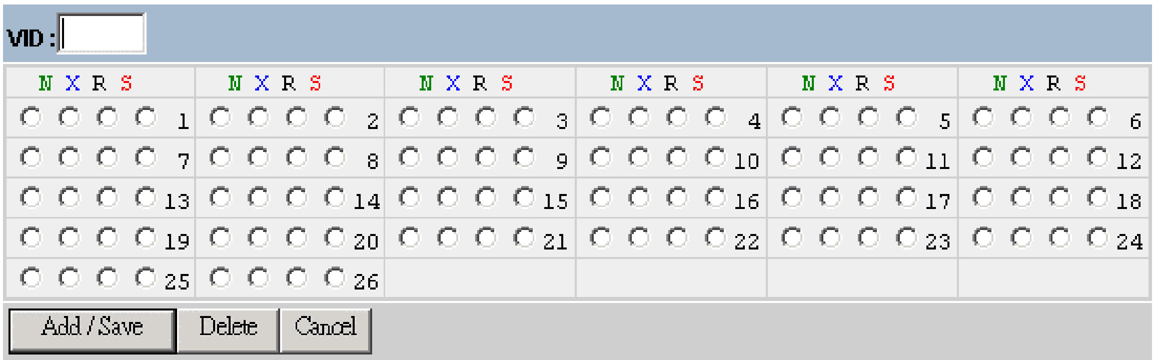
Use this screen to create a new VLAN or modify the settings for an existing VLAN.



VLAN Table Configuration

N:Normal X:Forbidden S:Static R:Reg. Fixed

VLAN	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	
1	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	✎
2	S	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	✎
3	N	R	X	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	✎



VID :

N X R S	N X R S	N X R S	N X R S	N X R S	N X R S
○ ○ ○ ○ 1	○ ○ ○ ○ 2	○ ○ ○ ○ 3	○ ○ ○ ○ 4	○ ○ ○ ○ 5	○ ○ ○ ○ 6
○ ○ ○ ○ 7	○ ○ ○ ○ 8	○ ○ ○ ○ 9	○ ○ ○ ○ 10	○ ○ ○ ○ 11	○ ○ ○ ○ 12
○ ○ ○ ○ 13	○ ○ ○ ○ 14	○ ○ ○ ○ 15	○ ○ ○ ○ 16	○ ○ ○ ○ 17	○ ○ ○ ○ 18
○ ○ ○ ○ 19	○ ○ ○ ○ 20	○ ○ ○ ○ 21	○ ○ ○ ○ 22	○ ○ ○ ○ 23	○ ○ ○ ○ 24
○ ○ ○ ○ 25	○ ○ ○ ○ 26				

Parameter	Description
VLAN	The ID for the VLAN currently displayed. Range: 1-4094
(Port)	Port entries may be marked as: N : (Normal) Uses GVRP to determine port membership. S : (Static) Adds port as a static entry. GVRP protocol is disabled. R : (Registration Fixed) Adds port as a static entry. GVRP protocol messages are still forwarded through this port. X : (Forbidden) Disables GVRP for this VLAN on the specified port. If a removed port is no longer assigned to any other group as an untagged port, it will automatically be assigned to VLAN group 1 as untagged.

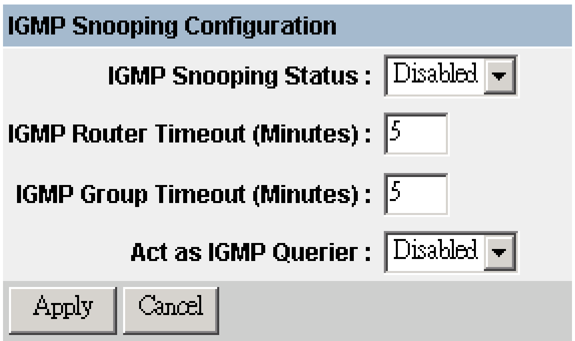
Note: To add a new VLAN, enter a new VLAN number in the VID field, select the port members, and press Add/Save. To modify a VLAN, click on the edit icon (✎) for the required entry, modify the port settings, and press Add/Save. To delete a VLAN, click on the edit icon (✎) for the required entry then press Delete.

5.7.4 Configuring IGMP Snooping

Multicasting is used to support real-time applications such as video conferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts which want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully filtered at every multicast switch/router it passes through to ensure that traffic is passed on only to the hosts which subscribed to this service.

This switch uses IGMP (Internet Group Management Protocol) Snooping to monitor for any attached hosts who want to receive a specific multicast service. It looks up the IP Multicast Group used for this service, and adds any port which received a similar request to that group.

You can use the IGMP Snooping Configuration screen to configure multicast filtering as shown below.



IGMP Snooping Configuration

IGMP Snooping Status : Disabled

IGMP Router Timeout (Minutes) : 5

IGMP Group Timeout (Minutes) : 5

Act as IGMP Querier : Disabled

Parameter	Default	Description
IGMP Snooping Status[1]	Disabled	If enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. This is also referred to as IGMP Snooping.
IGMP Router Timeout	5	A switch port that stops receiving multicast protocol packets for this interval will be removed from the IGMP forwarding list. Range: 3 - 5 minutes
IGMP Group Timeout	5	The time between spotting an IGMP Report message for an IP multicast address on a specific port before the switch removes that entry from its list. Range: 3 - 5 minutes
Act as IGMP Querier[2]	Disabled	If enabled, the switch can serve as the “querier,” which is responsible for asking hosts if they want to receive multicast traffic.

1:This item is only displayed for Layer 2 mode. For multilayer mode, the full IGMP protocol set is automatically enabled/disabled along with DVMRP. (See IGMP and DVMRP on 6.4 Multicast Filtering.)

2:This item is only displayed for Layer 2 mode. When IGMP is enabled for multilayer mode, the switch will always serve as the querier if elected.

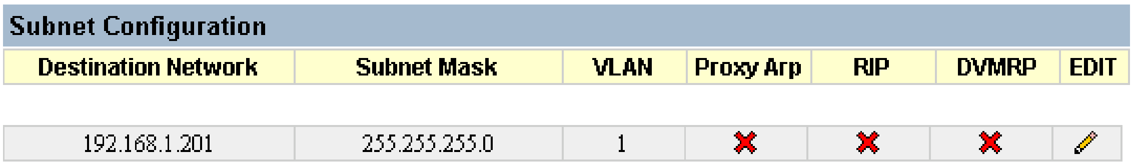
5.7.5 Configuring IP Settings

If this switch is set to multilayer mode, the IP Menu will be displayed.
Use this menu to configure the IP subnets for each VLAN on your switch, the unicast and multicast routing protocols, static ARP entries, static IP routes, and the default IP route.

Parameter	Description
Subnet Configuration	IP Subnet Configuration – Specifies the IP interface for VLANs configured on this switch, including the subnet address and routing protocols. Port Group Configuration – See “5.7.3.2 VLAN Table Configuration”.
Protocol Configuration	Configures ARP timeout, enables Proxy ARP, sets the preferred servers for BOOTP/DHCP Relay, as well as enabling/configuring unicast and multicast protocols globally for this switch.
Static ARP Configuration	Used to map an IP address to a specific physical MAC address.
Static Route	Used to configure static routes to other IP networks, subnetworks, or hosts.
Default Route	Defines the router to which this switch will forward all traffic for unknown networks.

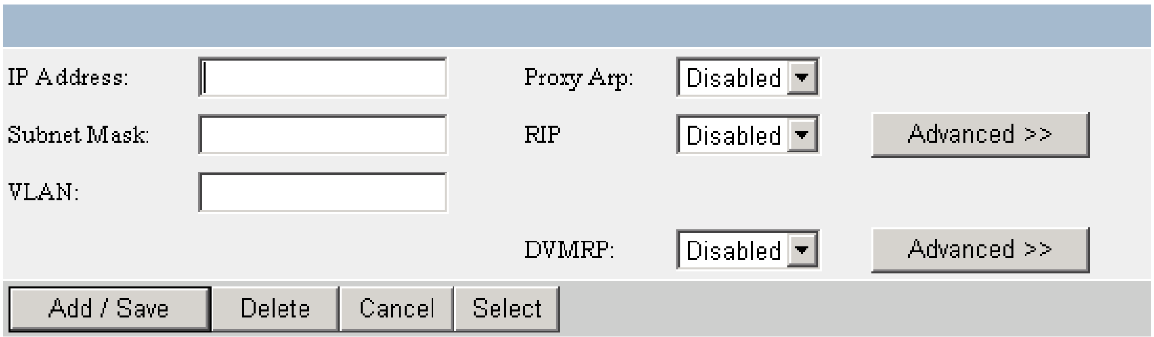
5.7.5.1 Subnet Configuration

Use this menu to specify an IP interface for any VLAN configured on this switch that needs to communicate with a device outside of its own group (that is, another network segment). You also need to define a VLAN for each IP subnet connected directly to this switch. Note that you must first create a VLAN as described under “5.7.3 Configuring Virtual LANs” before configuring the corresponding subnet.



Subnet Configuration

Destination Network	Subnet Mask	VLAN	Proxy Arp	RIP	DVMRP	EDIT
192.168.1.201	255.255.255.0	1	✗	✗	✗	✎



IP Address:

Subnet Mask:

VLAN:

Proxy Arp: Disabled

RIP: Disabled

DVMRP: Disabled

Parameter	Description
IP Address	The IP address associated with the specified VLAN interface. By convention, the last three digits should be set to “254” to readily distinguish this device as a router port.
Subnet Mask	A template that identifies the address bits in the host address used for routing to specific subnets. Each bit that corresponds to a “1” is part of the network / subnet number and each bit that corresponds to “0” is part of the host number.
VLAN	The VLAN associated with this IP interface.
Proxy ARP	Enables or disables Proxy ARP for the interface. This feature allows the switch forward an ARP request from a node in the attached subnetwork (that does not have routing or a default gateway configured) to a remote subnetwork. (See “6.2.5 Proxy ARP”) Note that Proxy ARP must be enabled globally for the switch before this setting can take effect. (See “5.7.5.2 Protocol Configuration”.)
RIP	Routing Information Protocol for unicast routing.
DVMRP	Distance-Vector Multicast Routing Protocol.

Note: To add an IP interface, specify the interface settings in the dialog box at the bottom of the screen, and press Add. To modify an interface, click on the edit icon (✎) for the required entry, update the interface settings in the dialog box at the bottom of the screen, and press Save. To delete an interface, click on the edit icon (✎) for the required entry and press Delete.

Adding an IP Interface

To add an IP interface, specify the interface settings in the dialog box at the bottom of the screen. Configure the IP address, assign an existing VLAN group to this interface, enable the required routing protocols, and then press Add. To configure the unicast and multicast routing protocols, you must edit an existing entry (as described in the following section) and press the Advanced button for RIP or DVMRP.

Modifying an IP Interface

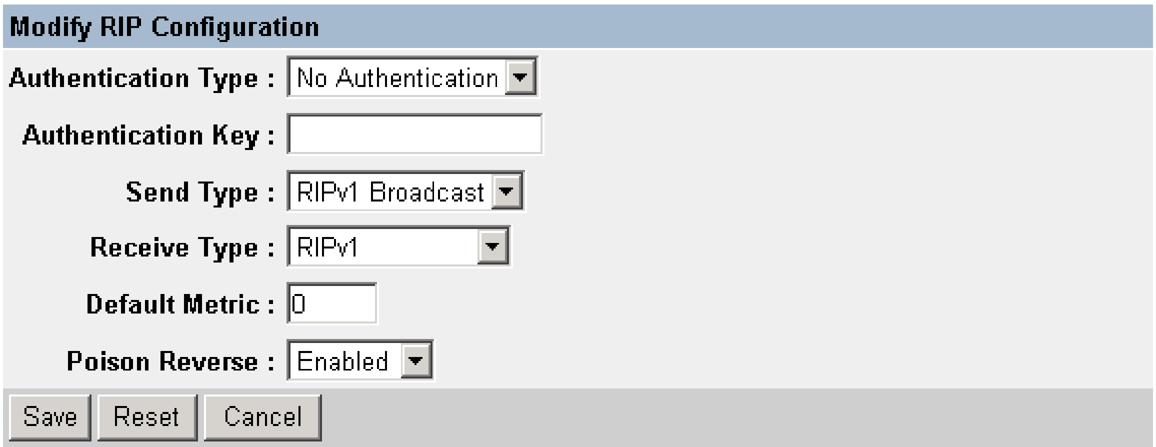
To modify an IP interface, click on the edit icon (✎) for the required entry, update the interface settings in the dialog box at the bottom of the screen, use the Advanced button to configure the unicast and multicast routing protocols (as described in the following sections), and then press Save.

Configuring RIP

The Routing Information Protocol is used to specify how routers exchange routing table information. (See “6.2.6.1 RIP and RIP-2 Dynamic Routing Protocols”.)

When RIP is enabled on this routing switch, it broadcasts RIP messages to all devices in the network every 30 seconds, and updates its own routing table when RIP messages are received from other routers. RIP messages contain both the IP address and a metric for each destination network it knows about, and the metric indicates the number of hops from this device to the destination network.

You can use the following menu to specify authentication, the protocol used for sending or receiving routing messages on this port, the default metric used in calculating the best path, and enable or disable Poison Reverse.



Modify RIP Configuration

Authentication Type : No Authentication

Authentication Key :

Send Type : RIPv1 Broadcast

Receive Type : RIPv1

Default Metric : 0

Poison Reverse : Enabled

Parameter	Description
Authentication Type	Authentication can be used to ensure that routing information comes from a valid source.
Authentication Key	A simple password must be provided if authentication is enabled. (An authentication string is case sensitive, and can be up to 16 characters.)
Send Type	The protocol used for traffic sent out this port: RIP1 Broadcast: Route information is broadcast to other routers on the network using RIPv1. RIP2 Broadcast: Route information is broadcast to other routers on the network using RIPv2. RIP2 Multicast: Route information is multicast to other routers on the network using RIPv2. Do Not Send: The switch will passively monitor route information advertised by other routers attached to the network.
Receive Type	The routing protocol messages accepted on this port includes RIP1, RIP2, RIP1/RIP2, or Do Not Receive.
Default Metric	A "metric" indicates the number of hops between the switch and the destination network. The "default metric" is used for the defau lt route in RIP updates originated on this interface. A value of zero indicates that no default route should be originated; in this case, a default route via another router may be propagated. Range: 0-15
Poison Reverse*	Directs routes back to an interface port from which they have been acquired, but sets the distance vector metrics to infinity.

* This is a method of preventing routing information from looping back to the source. Note that Split Horizon is also enabled on this switch for this purpose. (See "6.2.6.1 RIP and RIP-2 Dynamic Routing Protocols".)

Configuring DVMRP

Distance Vector Multicast Routing Protocol is used to route multicast traffic to nodes which have requested a specific multicast service via IGMP. (See "6.4.4 DVMRP Routing Protocol".) To configure DVMRP, you must specify the routing metric, probe interval, and neighbor router timeout.

Parameter	Default	Description
Metrics	1 hop	This value is used to select the best reverse path to networks that are connected directly to an interface on this switch. Range: 1-31 hops
Probe Interval	10 seconds	The interval between sending neighbor probe messages to the multicast group address for all DVMRP routers. Range: 5-30 seconds
Neighbor Timeout	35 seconds	The interval to wait without hearing from a DVMRP neighbor before declaring it dead. This is used for timing out routes, and for setting the children and leaf flags. Range: 10-8000 seconds

Note: IGMP is automatically enabled/disabled along with DVMRP. (See "6.4.2 IGMP Protocol".)

5.7.5.2 Protocol Configuration

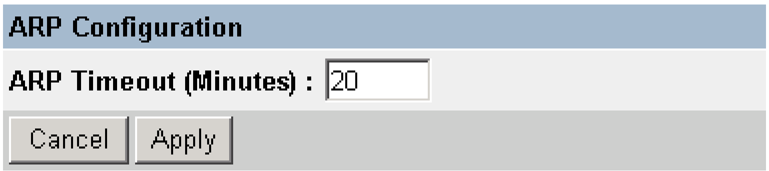
Use the Protocol Configuration screen to globally enable or disable unicast or multicast routing protocols for the switch.

Parameter	Description
ARP	Sets the aging time for dynamic ARP entries.
RIP	Sets the interval at which the switch advertises known routes, enables or disables advertising the switch as the default router, and enables or disables advertising static routes.
Boot Relay	Defines the preferred servers or the outbound subnetworks for broadcasting a BOOTP/DHCP request.
IGMP Snooping	Enables or disables IGMP Snooping. The Advanced menu sets the timeout for inactive multicast ports or for specific multicast flows when there are no longer any clients. See 5.7.4 Configuring IGMP Snooping.

Note: Once RIP and DVMRP have been enabled globally, you can enable or disable them for any specific subnet via the Subnet Configuration menu (5.7.5.1 Subnet Configuration).

Setting the ARP Timeout

You can use the following configuration screen to modify the aging time for dynamically learned entries in the ARP cache.



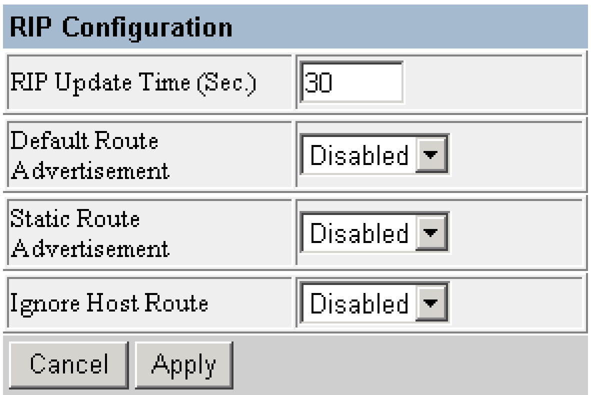
ARP Configuration

ARP Timeout (Minutes) : 20

Parameter	Default	Description
ARP Timeout	20 minutes	The time that dynamically learned entries are retained in the ARP cache. Range: 0-999 minutes, where 0 disables aging

Setting the RIP Advertisement Policy

You can use the following configuration screen to set the timing interval and policies RIP uses to advertise route information.



RIP Configuration

RIP Update Time (Sec.)	30
Default Route Advertisement	Disabled
Static Route Advertisement	Disabled
Ignore Host Route	Disabled

Parameter	Default	Description
RIP Update Time	30 seconds	The interval at which RIP advertises known route information. Range: 0-999 seconds, where 0 disables route advertisements
Default Route Advertisement	Disabled	Enables or disables advertising this switch as a default router.
Static Route Advertisement	Disabled	Enables or disables advertisement of static routes.

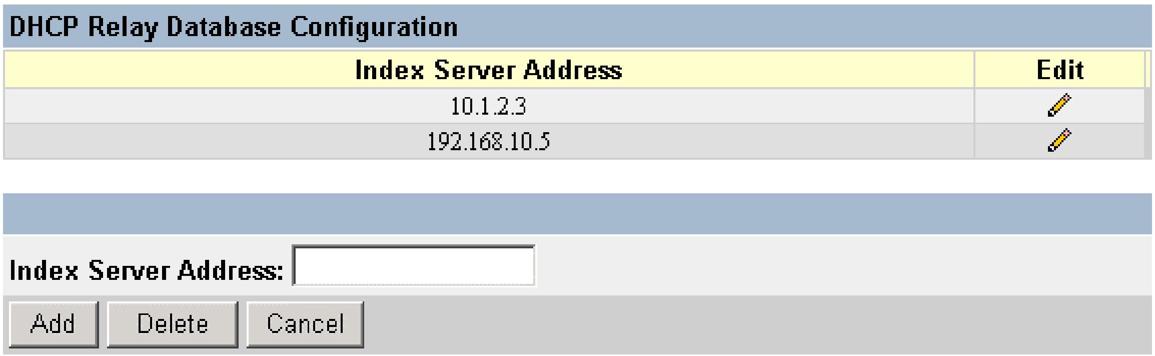
Configuring BOOTP/DHCP Relay

If a DHCP/BOOTP server is not located in the same subnet with a host, you can configure this switch to forward any host configuration queries to a server located on another subnet or on another network. Depending on the configuration setup, the switch either:

• Forwards the packet to a preferred server as defined in the switch configuration using unicast routing, or

• Broadcasts the DHCP Request again to another directly attached IP subnet specified in the switch configuration.

Specify the address for any DHCP server, or specify the subnet address for an outbound IP interface already configured on this switch (5.7.5.1 Subnet Configuration) as described in the following screens.



DHCP Relay Database Configuration

Index Server Address	Edit
10.1.2.3	✎
192.168.10.5	✎

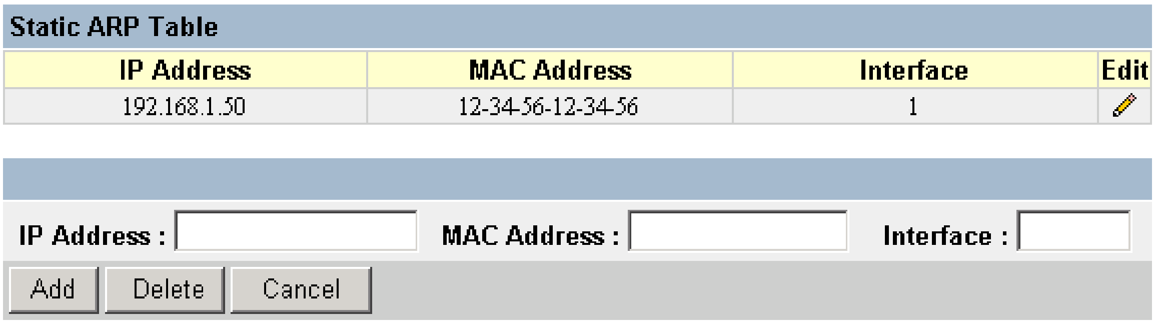
Index Server Address:

Parameter	Description
Index Server Address	Used to define any preferred DHCP servers or the outbound subnetwork for relaying a DHCP request broadcast. (Up to five entries are permitted.)

Note: To add a Relay Server, specify the IP address in the dialog box at the bottom of the screen, and press Add. To delete a Relay Server, click on the edit icon (✎) for the required entry and press Delete.

5.7.5.3 Static ARP Configuration

Use the following screen to display or edit entries in the Static ARP Table. Entries added to this table are retained until the associated IP interface is deleted or the switch is reset to the factory defaults.



Static ARP Table

IP Address	MAC Address	Interface	Edit
192.168.1.50	12-34-56-12-34-56	1	✎

IP Address : MAC Address : Interface :

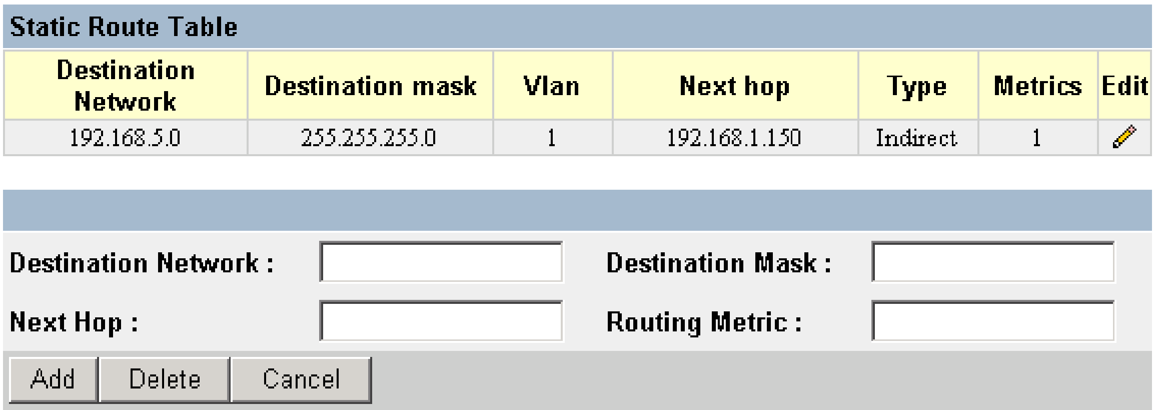
Parameter	Description
IP Address	IP address statically mapped to a physical MAC address.
MAC Address	MAC address statically mapped to the corresponding IP address.
Interface	The index number of the IP interface that will use this static ARP entry. See 5.7.5.1 Subnet Configuration or 5.8.6 IP Menu.

Note: To add a static address, specify it in the dialog box at the bottom of the screen, and press Add. To delete a static address, click on the edit icon (✎) for the required entry and press Delete.

5.7.5.4 Static Route Configuration

This switch can be configured to dynamically learn the routes to other IP networks, subnets or hosts using unicast or multicast routing protocols. If the route to a specific destination cannot be learned via these protocols, or you wish to restrict the path used for transmitting traffic to a destination, it can be statically configured using the Static Route Table.

Before defining a static route, remember that you must first configure at least one IP interface on this switch (See 5.7.5.1 Subnet Configuration). Static routes take precedence over dynamically learned routes and remain in the table until you remove them or the corresponding IP interface from this switch.



Static Route Table

Destination Network	Destination mask	Vlan	Next hop	Type	Metrics	Edit
192.168.5.0	255.255.255.0	1	192.168.1.150	Indirect	1	✎

Destination Network :

Destination Mask :

Next Hop :

Routing Metric :

Parameter	Description
Destination Network	A destination network, subnet or host.
Destination Mask	The subnet mask that specifies the bits to match. A routing entry will be used for a packet if the bits in the address set by the destination mask match the Destination Network
VLAN	The VLAN within which the gateway or destination address resides.
Next Hop	The IP address of the router at the next hop. Note that the network portion of the next hop must match that used for one of the subnet IP interfaces configured on this switch. (See “ 5.7.5.1 Subnet Configuration¨.)
Type	The IP route type for the destination network. This switch supports the following types: Direct - A directly connected subnetwork. Indirect - A remote IP subnetwork or host address.
Routing Metric*	A relative measure of the path cost from this switch to the destination network.

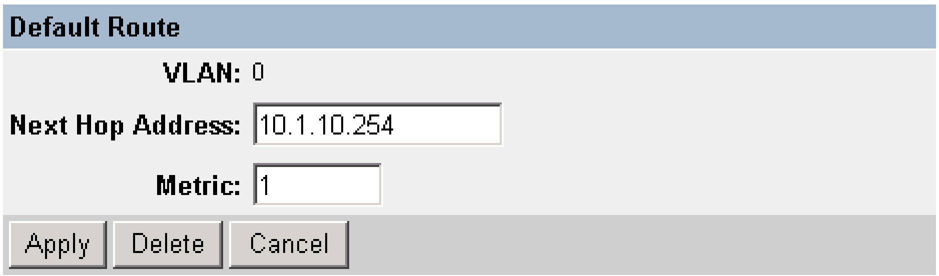
* This value depends on the specific routing protocol.

Note: To add a static route, specify it in the dialog boxes at the bottom of the screen, and press Add. To delete a static route, click on the edit icon (✎) for the required entry and press Delete.

5.7.5.5 Configuring the Default Route

Defines the router to which this switch will forward all traffic for unknown networks.

The default route can be learned from RIP protocol or manually configured. If the switch does not contain a default route, any packet that does not match an entry in the routing table will be dropped. To manually configure a default route, enter the next hop in the following table.



Default Route

VLAN: 0

Next Hop Address: 10.1.10.254

Metric: 1

Parameter	Description
VLAN	The VLAN which has the IP interface to the default router.
Next Hop Address	The IP address of the default router.
Metric	The number of hops required to reach the default router.

5.7.6 Configuring Security Filters

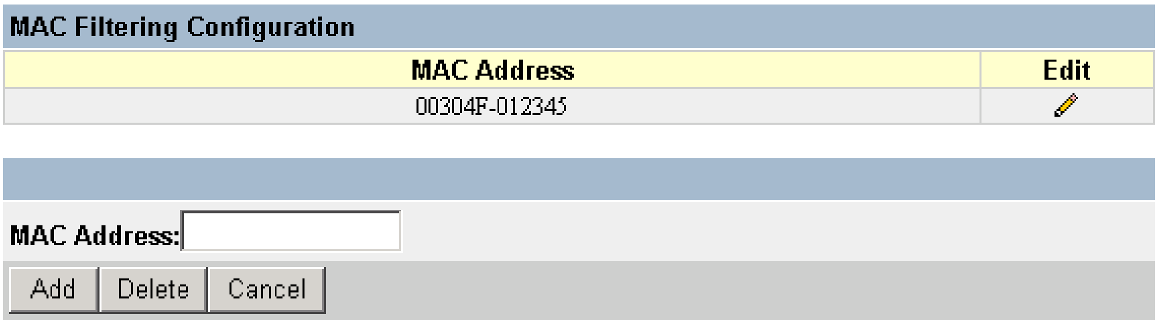
You can use the Security menu to filter MAC and IP addresses.

Parameter	Description
MAC Filtering Configuration	Specifies the source or destination MAC address for any traffic to be filtered from the switch.
IP Filtering Configuration*	Specifies the source or destination IP address for any traffic to be filtered from the switch.

* This menu item is only displayed for multilayer mode.

5.7.6.1 Configuring MAC Address Filters

Any node that presents a security risk or is functioning improperly can be filtered from this switch. You can drop all the traffic from a host device based on a specified MAC address. Traffic with either a source or destination address listed in the Security Filtering Configuration table will be filtered.



MAC Filtering Configuration

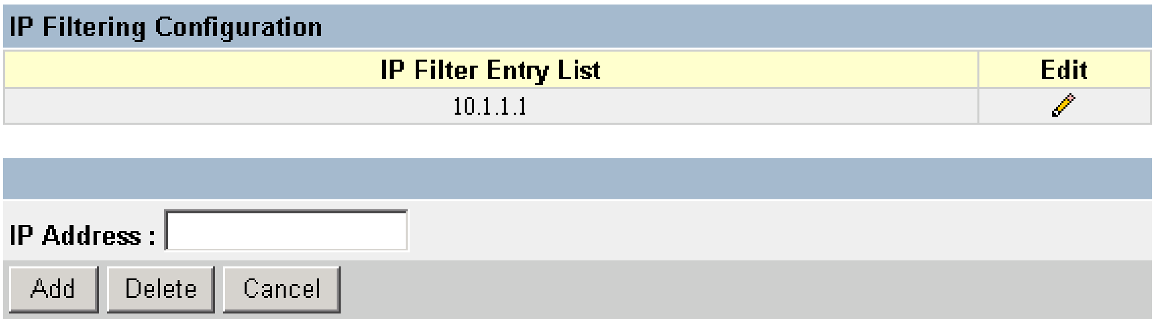
MAC Address	Edit
00304F-012345	✎

MAC Address:

Note: To add a MAC address to the security filter, press Add. To delete an address, click on the edit icon (✎) for the required entry and press Delete.

5.7.6.2 Configuring IP Address Filters

If any node presents a security risk, you can filter all traffic for this node by entering its address into the IP Security Filter. Any packet passing through the switch that has a source or destination IP address matching an entry in this table will be filtered.



IP Filtering Configuration

IP Filter Entry List	Edit
10.1.1.1	✎

IP Address :

Note: To add an IP address to the security filter, press Add. To delete an address, click on the edit icon (✎) for the required entry and press Delete.

5.8 Monitoring the Switch

The Network Monitor Menu provides access to port statistics, address tables, STA information, VLANs registration and forwarding information, multicast groups, and subnet addresses. Each of the screens provided by these menus is described in the following sections.

Menu	Description
Port Statistics	Displays statistics on port traffic, including information from the Interfaces Group, Ethernet-like MIB, and RMON MIB.
Layer 2 Address Table	Contains the unicast address table.
Bridge Menu	Displays Spanning Tree settings for the overall switch and for specific ports.
VLAN Menu	Displays ports dynamically learned through GMRP or GVRP, and ports that are currently forwarding VLAN traffic.
IP Multicast Registration Table[1]	Displays all the multicast groups active on this switch, including the multicast IP address and the corresponding VLANs.
IP Menu[2]	Displays all the IP subnets used on this switch, as well as the corresponding VLANs and ports. Also contains the ARP table, routing table, and multicast menu.

1: This menu is displayed only if the switch is set to Layer 2 mode.
2: This menu is displayed only if the switch is set to multilayer mode.
.

5.8.1 Displaying Port Statistics

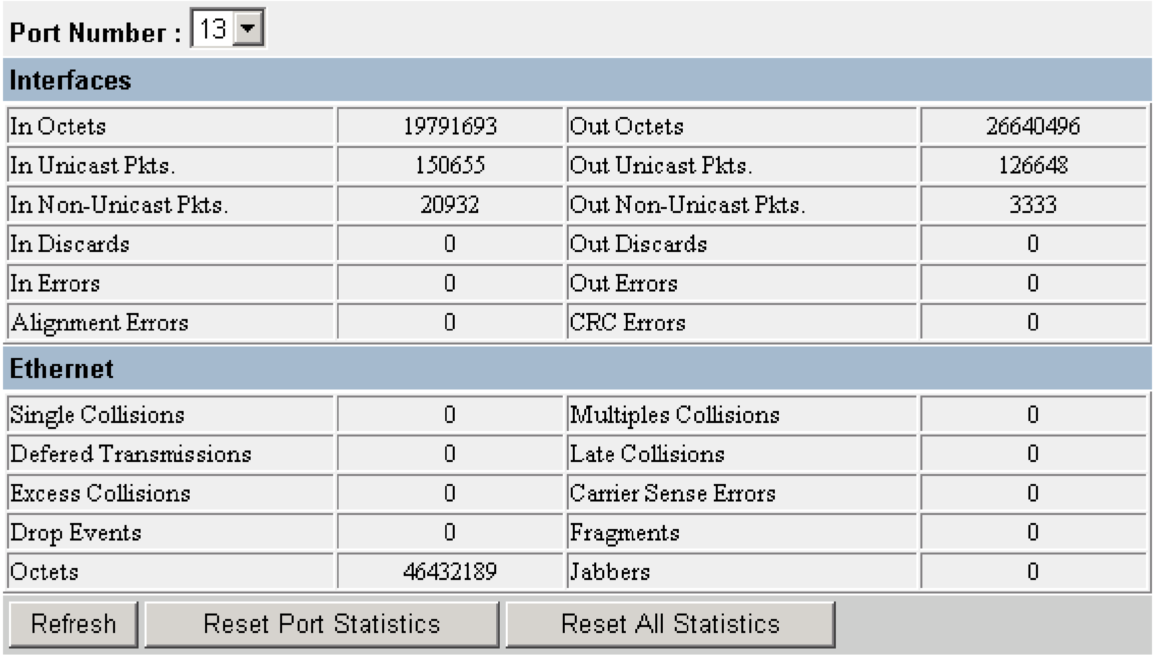
Port Statistics display standard statistics on network traffic from the Interfaces Group and Ethernet-like MIBs, as well as a detailed breakdown of traffic based on the RMOM MIB.

Parameter	Description
Port Statistics	Displays standard statistics on network traffic passing through the selected port.
RMON Statistics	Displays detailed statistics for the selected port, such as packet type and frame size counters.

5.8.1.1 Displaying Ethernet Port Statistics

Port Statistics display key statistics from the Interfaces Group and Ethernet-like MIBs for each port. Error statistics on the traffic passing through each port are displayed. This information can be used to identify potential problems with the switch, such as a faulty port or unusually heavy loading. The values displayed have accumulated since the last system reboot.

Select the required port. The statistics displayed are indicated in the following figure and table.



Port Number : 13

Interfaces			
In Octets	19791693	Out Octets	26640496
In Unicast Pkts.	150655	Out Unicast Pkts.	126648
In Non-Unicast Pkts.	20932	Out Non-Unicast Pkts.	3333
In Discards	0	Out Discards	0
In Errors	0	Out Errors	0
Alignment Errors	0	CRC Errors	0

Ethernet			
Single Collisions	0	Multiples Collisions	0
Defered Transmissions	0	Late Collisions	0
Excess Collisions	0	Carrier Sense Errors	0
Drop Events	0	Fragments	0
Octets	46432189	Jabbers	0

Parameter	Description
Interfaces Group	
In Octets	The total number of octets received on the interface, including framing characters.
In Unicast Pkts.	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
In Non-Unicast Pkts.	The number of non-unicast (that is, subnetwork- broadcast or subnetwork-multicast) packets delivered to a higher-layer protocol.

In Discards	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
In Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Alignment Errors	The number of alignment errors (mis-synchronized data packets).
Out Octets	The total number of octets transmitted out of the interface, including framing characters.
Out Unicast Pkts.	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Out Non-Unicast Pkts.	The total number of packets that higher-level protocols requested be transmitted to a non- unicast (that is, a subnetwork-broadcast or subnetwork-multicast) address, including those that were discarded or not sent.
Out Discards	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Out Errors	The number of outbound packets that could not be transmitted because of errors.
CRC Errors	Number of Ethernet Cyclic Redundancy Check errors detected by this device.
Ethernet-Like	
Single Collisions	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Excessive Collisions	The number of frames for which transmission failed due to excessive collisions.
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Octets	Number of octets passing through this port.
Multiple Collisions	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
Carrier Sense Errors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and contained either an FCS or alignment error.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and contained either an FCS or alignment error.

Note: Statistics are refreshed every 10 seconds by default (See 5.3.2 Configuring the Serial Port).

5.8.1.2 Displaying RMON Statistics

Use the RMON Statistics screen to display key statistics for each port from RMON group 1. (RMON groups 2, 3 and 9 can only be accessed using SNMP management software.) The following screen displays the overall statistics on traffic passing through each port. RMON statistics provide access to a broad range of statistics, including a total count of different frame types and sizes passing through each port.

Values displayed have been accumulated since the last system reboot.

Parameter	Description
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Received Bytes	Total number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Received Frames	The total number of frames (bad, broadcast and multicast) received.
Broadcast Frames	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Frames	The total number of good frames received that were directed to this multicast address.
CRC/Alignment Errors	The number of CRC/alignment errors (FCS or alignment errors).
Undersize Frames	The total number of frames received that were less than 64 octets long(excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Frames	The total number of frames received that were longer than 1518 octets(excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of frames received that were less than 64 octets in length(excluding framing bits, but including FCS octets) and contained either an FCS or alignment error.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and contained either an FCS or alignment error.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
64 Byte Frames	The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65-127 Byte Frames 128-255 Byte Frames 256-511 Byte Frames 512-1023 Byte Frames 1024-1518 Byte Frames 1519-1536 Byte Frames	The total number of frames (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).

Note: Statistics are refreshed every 10 seconds by default (See 5.3.2 Configuring the Serial Port).

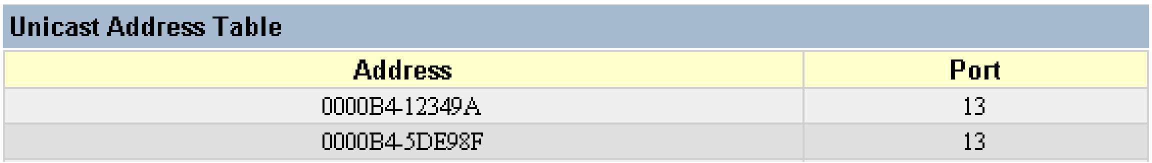
5.8.2 Layer 2 Address Tables

This menu includes the unicast address table.

Menu	Description
Unicast Address Table	Provides a full listing for unicast addresses.

5.8.2.1 Displaying the Unicast Address Table

The Unicast Address Table contains the MAC addresses associated with each port (that is, the source port associated with the address). The information displayed in the Address Table is indicated in the following figure and table.



Unicast Address Table

Address	Port
0000B4-12349A	13
0000B4-5DE98F	13

Parameter	Description
Address	The MAC address of a node seen on this switch.
Port	The port whose address table includes this MAC address.

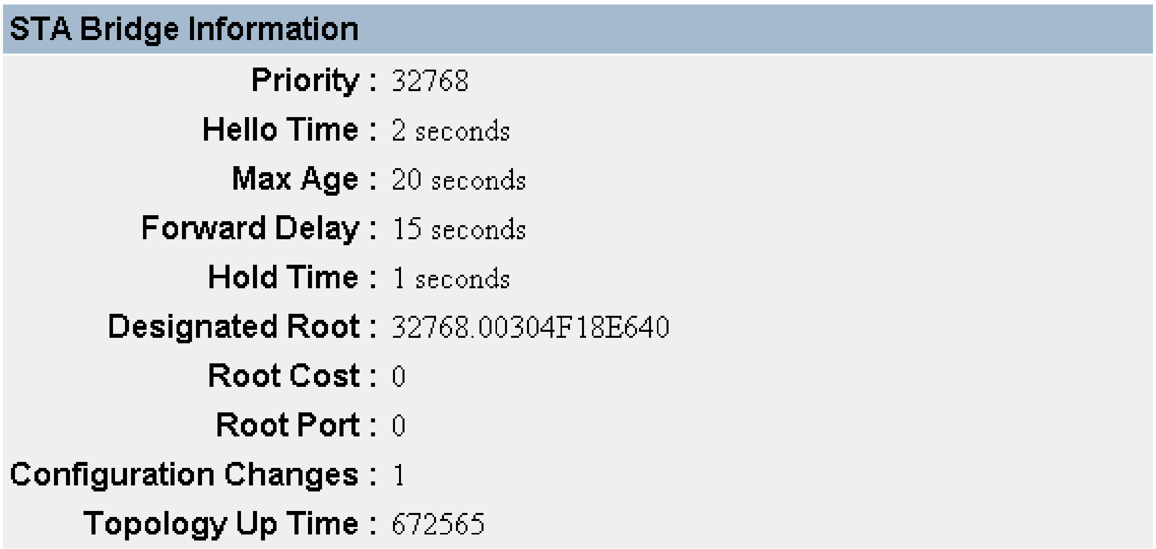
5.8.3 Displaying Bridge Information

The Bridge menu is used to display settings for the Spanning Tree Algorithm. For a more detailed description of how to use this algorithm, refer to “6.1.3 Spanning Tree Algorithm”.

Menu	Description
Spanning Tree Bridge Information	Displays a full list of STA values used for the bridge.
Spanning Tree Port Information	Displays a list of STA values used for each port, including status, designated cost, designated bridge, and designated port.

5.8.3.1 Viewing the Current Spanning Tree Information

The STA Bridge Information screen displays a summary of STA information for the overall bridge. To make any changes to these parameters, use the Bridge STA Configuration menu as described on 5.7.2 Using the Bridge Menu. The parameters shown in the following figure and table describe the current Bridge STA settings.



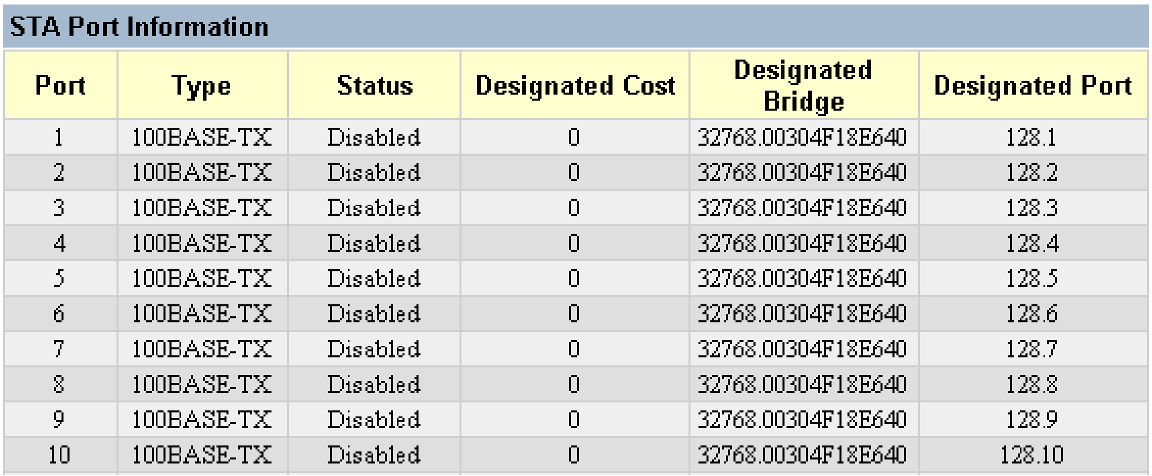
STA Bridge Information

Priority :	32768
Hello Time :	2 seconds
Max Age :	20 seconds
Forward Delay :	15 seconds
Hold Time :	1 seconds
Designated Root :	32768.00304F18E640
Root Cost :	0
Root Port :	0
Configuration Changes :	1
Topology Up Time :	672565

Parameter	Description
Priority	Device priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.
Hello Time	The time interval (in seconds) at which the root device transmits a configuration message.
Max Age	The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure.
Forward Delay	The maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding).
Hold Time	The minimum interval between the transmission of consecutive Configuration BPDUs.
Designated Root	The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.
Root Cost	The path cost from the root port on this switch to the root device.
Root Port	The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.
Configuration Changes	The number of times the Spanning Tree has been reconfigured.
Topology Up Time	The time since the Spanning Tree was last reconfigured.

5.8.3.2 Displaying the Current STA for Ports

The parameters shown in the following figure and table are for port STA Information.



STA Port Information

Port	Type	Status	Designated Cost	Designated Bridge	Designated Port
1	100BASE-TX	Disabled	0	32768.00304F18E640	128.1
2	100BASE-TX	Disabled	0	32768.00304F18E640	128.2
3	100BASE-TX	Disabled	0	32768.00304F18E640	128.3
4	100BASE-TX	Disabled	0	32768.00304F18E640	128.4
5	100BASE-TX	Disabled	0	32768.00304F18E640	128.5
6	100BASE-TX	Disabled	0	32768.00304F18E640	128.6
7	100BASE-TX	Disabled	0	32768.00304F18E640	128.7
8	100BASE-TX	Disabled	0	32768.00304F18E640	128.8
9	100BASE-TX	Disabled	0	32768.00304F18E640	128.9
10	100BASE-TX	Disabled	0	32768.00304F18E640	128.10

Parameter	Description
Type	Shows port type as: 100BASE-TX : 10BASE-T / 100BASE-TX 1000BASE-T : 1000BASE-T
Status	Displays current state of this port within the Spanning Tree: Disabled No link has been established on this port. Otherwise, the port has been disabled by the user or has failed diagnostics. Blocking Port receives STA configuration messages, but does not forward packets. Listening Port will leave blocking state due to a topology change, start transmitting configuration messages, but does not yet forward packets. Learning Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses. Forwarding The port forwards packets, and continues learning addresses. The rules defining port status are: • A port on a network segment with no other STA -compliant bridging device is always forwarding. • If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is blocked. • All ports are blocked when the switch is booted, then some of them change state to listening, to learning, and then to forwarding.
Designated Cost	The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.
Designated Bridge(ID)	The priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.
Designated Port (ID)	The priority and number of the port on the designated bridging device through which this switch must communicate with the root of the Spanning Tree.

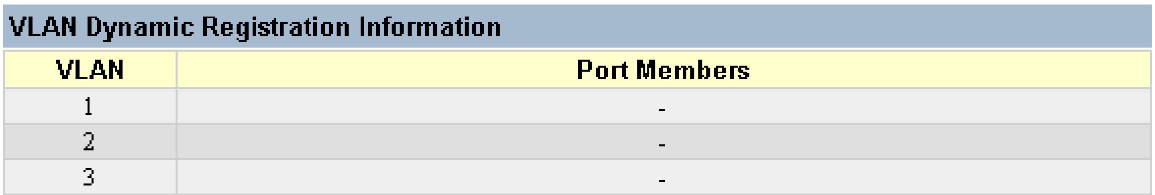
5.8.4 Displaying VLAN Information

These menus display information on the ports that have been automatically learned via GVRP and all those ports that have been configured by dynamic or static means to forward VLAN traffic.

Menu	Description
VLAN Dynamic Registration Information	Shows the ports that have been automatically learned via GVRP.
VLAN Forwarding Information	Shows all those ports that have been configured by either dynamic or static means to forward VLAN traffic.

5.8.4.1 VLAN Dynamic Registration Information

This table shows the ports that have been automatically learned via GVRP.

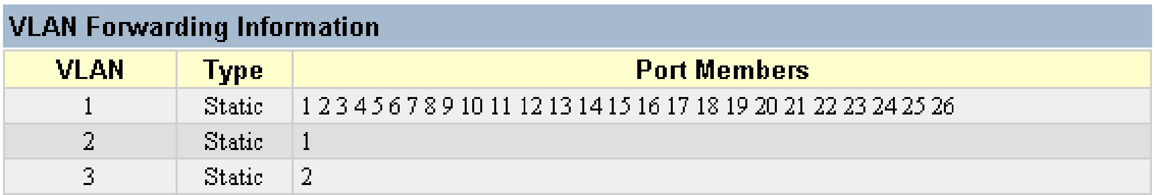


VLAN Dynamic Registration Information

VLAN	Port Members
1	-
2	-
3	-

5.8.4.2 VLAN Forwarding Information

Shows all those ports that have been configured by either dynamic or static means to forward VLAN traffic.

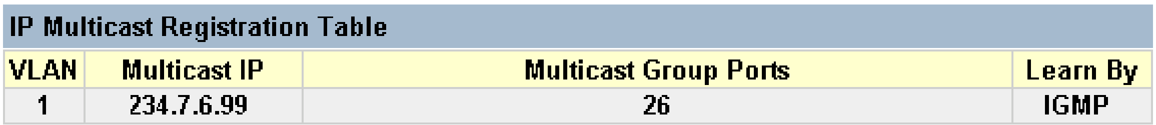


VLAN Forwarding Information

VLAN	Type	Port Members
1	Static	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
2	Static	1
3	Static	2

5.8.5 IP Multicast Registration Table

This table displays all the multicast groups active on the switch, including the multicast IP address and the corresponding VLANs.



IP Multicast Registration Table

VLAN	Multicast IP	Multicast Group Ports	Learn By
1	234.7.6.99	26	IGMP

Parameter	Description
VLAN	A VLAN with host members that have asked to receive the indicated multicast service.
Multicast IP	A source IP address that represents a specific multicast service.
Multicast Group Ports	The ports that belong to the indicated VLAN group.
Learned By	Shows if this entry was learned dynamically or via IGMP Snooping. An entry is learned dynamically if a multicast packet was seen crossing the port, or via IGMP Snooping if an IGMP registration packet was seen crossing the port.

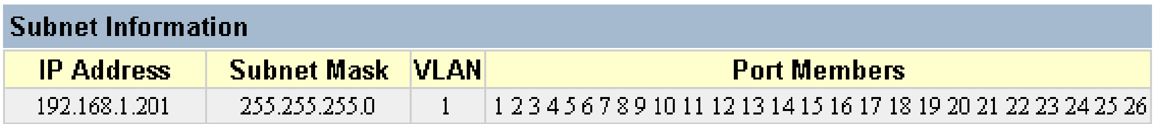
5.8.6 IP Menu

This menu contains IP subnets information, the ARP cache, routing table, as well as multicast groups and multicast routing information.

Menu	Description
Subnet Information	Displays all the IP subnets configured on this switch, as well as the corresponding VLANs and ports.
ARP Table	Shows the IP-to-MAC addresses discovered by ARP.
Routing Table	Shows the routes through which all recognized Ethernet networks (and the corresponding VLAN) can be reached.
Multicast Table	Displays all the multicast groups active on this switch, including the multicast IP address and the corresponding VLANs. Also includes the IGMP registration table, the multicast forwarding cache, and DVMRP routing information.

5.8.6.1 Displaying Subnet Information

You can display a list of all the IP interfaces configured on this switch. This table includes the gateway address, corresponding VLAN, and member ports that use this address.



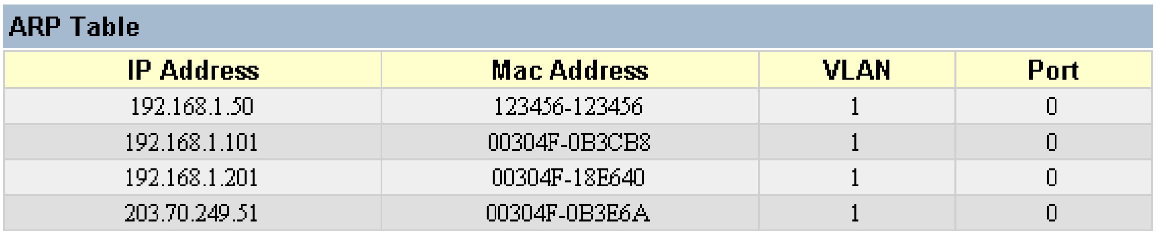
Subnet Information

IP Address	Subnet Mask	VLAN	Port Members
192.168.1.201	255.255.255.0	1	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

Parameter	Description
IP Address	The address for an IP interface on this switch.
Subnet Mask	A template that identifies the address bits in the host address used for routing to specific subnets. Each bit that corresponds to a “1” is part of the network / subnet number; each bit that corresponds to “0” is part of the host number.
VLAN	The VLAN group associated with this IP interface.
Port Members	The ports that can be reached through this IP interface.

5.8.6.2 ARP Table

Address Resolution Protocol (ARP) defines a method for extracting a host’s Ethernet address from its Internet address. This table shows the IP-to-MAC address cache discovered via ARP.



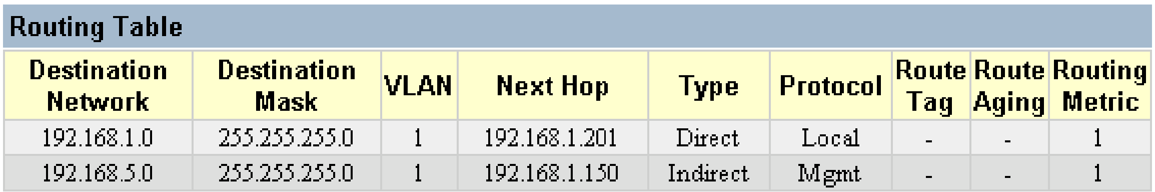
ARP Table

IP Address	Mac Address	VLAN	Port
192.168.1.50	123456-123456	1	0
192.168.1.101	00304F-0B3CB8	1	0
192.168.1.201	00304F-18E640	1	0
203.70.249.51	00304F-0B3E6A	1	0

Parameter	Description
IP Address	IP addresses for which ARP has resolved the physical address through a broadcast message.
MAC Address	MAC address that maps to the corresponding IP address.
VLAN	The VLAN group to which this host has been assigned.
Port	The port this to which host device is attached. (Port “0” refers to an interface defined on this switch.)

5.8.6.3 Routing Table

The Routing Table lists the routes through which all recognized Ethernet networks (and corresponding VLANs) can be reached. This table includes all routes learned through routing protocols or manual configuration.



Routing Table

Destination Network	Destination Mask	VLAN	Next Hop	Type	Protocol	Route Tag	Route Aging	Routing Metric
192.168.1.0	255.255.255.0	1	192.168.1.201	Direct	Local	-	-	1
192.168.5.0	255.255.255.0	1	192.168.1.150	Indirect	Mgmt	-	-	1

Parameter	Description
Destination Network	A destination network, subnet or host.
Destination Mask	The subnet mask that specifies the bits to match. A routing entry will be used for a packet if the bits in the address set by the destination mask match the Destination Network.
VLAN	The VLAN within which the gateway or destination address resides.
Next Hop	The IP address of the router at the next hop.
Type	The IP route type for the destination network. This switch supports the following types: Direct - A directly connected subnetwork. Indirect - A remote IP subnetwork or host address. Myself - A switch IP address on a specific IP subnetwork. Bcast - A subnetwork broadcast address. Mcast - An IP multicast address. Invalid - A illegal IP address to be filtered.
Protocol	The route was learned in one of the following ways: Local - Manually configured Mgmt. - Set via SNMP ICMP - Obtained via ICMP redirect. RIP - Learned via RIP protocol. Other - Learned by some other method.
Route Tag	The route tag represents the device that originated this routing entry.
Route Aging	The number of seconds elapsed since this route was last updated or otherwise determined to be correct. (This entry only applies to RIP.)
Routing Metric	A relative measure of the path cost from this switch to the destination network. (This value depends on the specific routing protocol.)

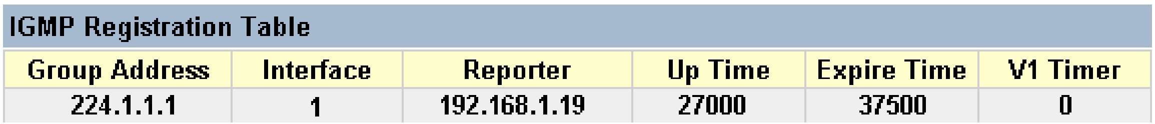
5.8.6.4 Multicast Table

You can use this menu to display all the multicast groups currently active on this switch, the IGMP cache, the multicast forwarding cache, and DVMRP routing information.

Parameter	Description
IP Multicast Registration Table	Displays all active multicast groups, including the multicast IP address and the corresponding VLANs. (See 5.8.5 IP Multicast Registration Table.)
IGMP Cache	Displays all active multicast groups, including the IP interface each entry appears on, the entry age, and the time left before the entry is aged out.
Multicast Forwarding Table	Displays all active multicast groups, including the multicast source address, the upstream neighbor, the multicast routing protocol, and the entry age.
DVMRP Routing Table	Displays the source address for each known multicast service, the upstream neighbor, the IP interface each entry appears on, the routing metric, and the entry age.
DVMRP Neighbor Table	Displays all the neighbor routers accessible through each IP interface, including the entry age, the time left before the entry is aged out, the protocol version, and the number of routing updates received from each neighboring router.

Displaying IGMP Registration Table

The switch provides a local registry of active multicast groups for each IP interface, including the age and expiration time for each entry.



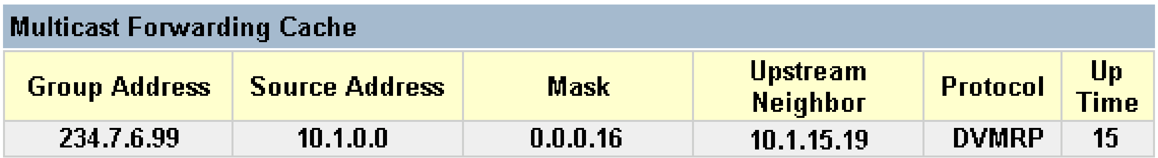
IGMP Registration Table

Group Address	Interface	Reporter	Up Time	Expire Time	V1 Timer
224.1.1.1	1	192.168.1.19	27000	37500	0

Parameter	Description
Group Address	An IP multicast group address with subscribers directly attached or downstream from this switch.
Interface	The IP interface on this switch that has received traffic directed to the IP multicast group address. (See 5.8.6.1 Displaying Subnet Information.)
Reporter	The IP address of the source of the last membership report received for this IP Multicast group address on this interface. If no membership report has been received, this object has the value 0.0.0.0.
Up Time	The time elapsed since this entry was created.
Expire Time	The time remaining before this entry will be aged out. (The default is 260 seconds.)
V1 Timer	The time remaining until the switch assumes that there are no longer any IGMP Version 1 members on the IP subnet attached to this interface. (The default is 400 seconds.) If the switch receives an IGMP Version 1 Membership Report, it sets a timer to note that there are Version 1 hosts present which are members of the group for which it heard the report. If there are Version 1 hosts present for a particular group, the switch will ignore any Leave Group messages that it receives for that group.

Displaying the Multicast Forwarding Cache

The switch maintains a cache of multicast routing entries used to calculate the delivery tree in multicast routing protocols. The Multicast Forwarding Cache includes the subnetwork that contains the multicast source and the nearest upstream neighbor for each known multicast group address.



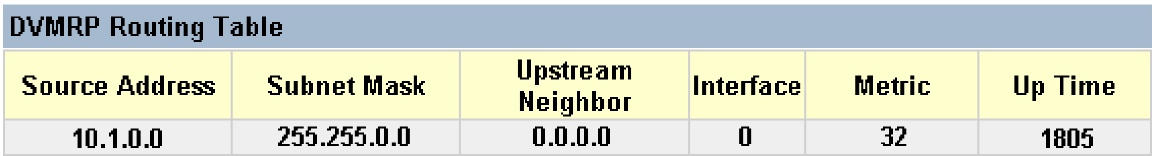
Multicast Forwarding Cache

Group Address	Source Address	Mask	Upstream Neighbor	Protocol	Up Time
234.7.6.99	10.1.0.0	0.0.0.16	10.1.15.19	DVMRP	15

Parameter	Description
Group Address	An IP multicast group address with subscribers directly attached or downstream from this switch.
Source Address	The IP subnetwork at the root of the multicast delivery tree. This subnetwork contains a known multicast source.
Mask	Subnet mask that is used for the source address. This mask identifies the host address bits used for routing to specific subnets.
Upstream Neighbor	The IP address of the network device immediately upstream for this group.
Protocol	The multicast routing protocol associated with this entry.
Up Time	The time elapsed since this entry was created.

Displaying the DVMRP Routing Table

The DVMRP Routing Table contains all the IP multicast routes learned by the DVMRP protocol. The routes displayed in this table are used by this switch to forward new IP multicast traffic. They do not reflect active multicast flows.



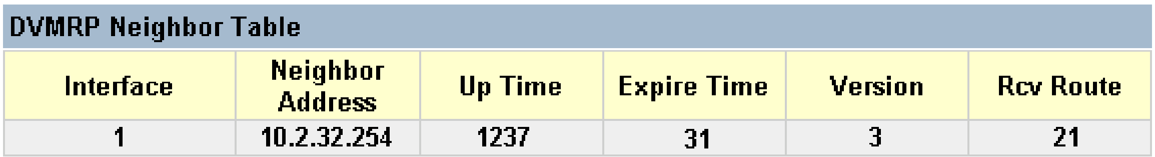
DVMRP Routing Table

Source Address	Subnet Mask	Upstream Neighbor	Interface	Metric	Up Time
10.1.0.0	255.255.0.0	0.0.0.0	0	32	1805

Parameter	Description
Source Address	The IP subnetwork at the root of the multicast delivery tree. This subnetwork contains a known multicast source.
Subnet Mask	Subnet mask that is used for the source address. This mask identifies the host address bits used for routing to specific subnets.
Upstream Neighbor	The IP address of the network device immediately upstream for this multicast delivery tree.
Interface	The IP interface on this switch that connects to the upstream neighbor.
Metric	The metric for this interface used to calculate distance vectors.
Up Time	The time elapsed since this entry was created.

Displaying the DVMRP Neighbor Table

The DVMRP Neighbor Table contains the switch's DVMRP neighbors, as discovered by receiving DVMRP protocol messages.



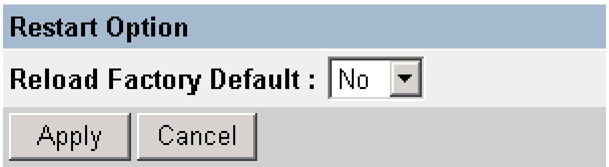
DVMRP Neighbor Table

Interface	Neighbor Address	Up Time	Expire Time	Version	Rcv Route
1	10.2.32.254	1237	31	3	21

Parameter	Description
Interface	The IP interface on this switch that connects to the upstream neighbor. (See 5.8.6.1 Displaying Subnet Information.)
Neighbor Address	The IP address of the network device immediately upstream for this multicast delivery tree.
UpTime	The time since this device last became a DVMRP neighbor to this switch.
ExpireTime	The time remaining before this entry will be aged out.
Version	The neighboring router's DVMRP version number .
Rcv Route	The total number of routes received in valid DVMRP packets from this neighbor. This can be used to diagnose problems such as unicast route injection, as well as giving an indication of the level of DVMRP route exchange activity.

5.9 Resetting the System

Use the Restart command under the Main Menu to reset the management agent. The reset screen is shown below.



Restart Option

Reload Factory Default : No

Parameter	Description
Reload Factory Defaults	Reloads the factory defaults
[Apply]	Restarts the switch.

Note: When restarting the system, it will always run the Power-On Self-Test. It will also retain all system information, unless you elect to reload the factory defaults.

Chapter 6. Advanced Topics

This Layer 3 switch supports both Layer 2 which is based on physical device addresses and Layer 3 switching which is based on IP network addresses. These functions, along with other advanced features are described in this chapter.

6.1 Layer 2 Switching

When a frame enters a port, its destination MAC address is checked in the address database to see which port leads to this destination. If the destination address belongs to the incoming port, the frame is dropped or "filtered." If the destination port is found on another port, the frame is forwarded to that port and queued for output. But, if the destination address is **not** found in the address database, the frame is sent to one or more output ports based on the rules for handling tagged or untagged VLAN frames.

If the source MAC address of the frame was not found in the address database, it is recorded along with the incoming port number where it entered the switch. This information is then used to make later decisions for frame forwarding.

During switching, the switch performs multiple steps, including:

- VLAN Classification
- Learning
- Filtering
- Forwarding
- Aging

The following sections provide additional information about the tasks the switch performs during unicast and multicast switching.

6.1.1 Unicast Switching

This section describes VLAN classification, learning, filtering, and forwarding for unicast switching.

• VLAN Classificatio n— When the switch receives a frame, it classifies the frame in one of two ways:
- If the frame is untagged, the switch classifies the frame into the default VLAN for the incoming port.
- If the frame is tagged, the switch uses the tagged VLAN ID to identify the broadcast domain of the frame.

• Learnin g — After VLAN classification, the switch checks the <source MAC address, VLAN> pair in the address table to see whether this pair is known.
- If unknown, the switch adds this pair to the address table.
- If known, the switch checks the pair for an incorrect Port ID. If the PID associated with the pair in the address table is different from the receiving port, the switch modifies the PID in the address table.

• Filterin g— After learning the address, the switch checks:
- If the source or destination port is not in the forwarding state. (For example, if it is in blocking state or has been disabled.)
- If the source or destination MAC address is to be filtered.
- If the source PID is the same as the destination PID.
If any of these conditions are met, the switch drops the received frame. Otherwise, it continues with the forwarding process as described below.

• Forwardin g— During the forwarding process, the switch checks whether the <destination MAC address, VLAN> pair is unknown.
- If unknown, the switch floods the received frame to all ports in the VLAN, excluding the source port.
- If known, the switch forwards the received frame to the port associated with the pair. At the same time, the switch decides whether a VLAN tag needs to be added to or stripped from the frame, depending on the VLAN tagged/untagged configuration and VLAN ID for the output port.

• Aging —the switch performs the aging process for the <MAC addresses, VLAN> pair in the MAC address table. Once a pair is aged out, the address table is modified.

6.1.2 Multicast Switching

For multicast switching, the switch checks whether the received frame is a Bridge Protocol Data Unit (BPDU). If a BPDU is received, the switch forwards the frame for processing by the Spanning Tree Protocol. Otherwise, the switch performs the following processes:

- VLAN classification —same as for unicast switching.
- Learning —same as for unicast switching.
- Filter ing —after learning, the switch checks the same filtering criteria used for unicast switching, except that there is no destination MAC address to check.
- Forwarding —the switch floods the received multicast frame to all ports within the VLAN, excluding the source port. At the same time, the switch decides whether a VLAN tag needs to be added to or stripped from the frame, depending on the VLAN tagged/untagged configuration and VLAN ID for the output port.
- Aging —same as for unicast switching.

6.1.3 Spanning Tree Algorithm

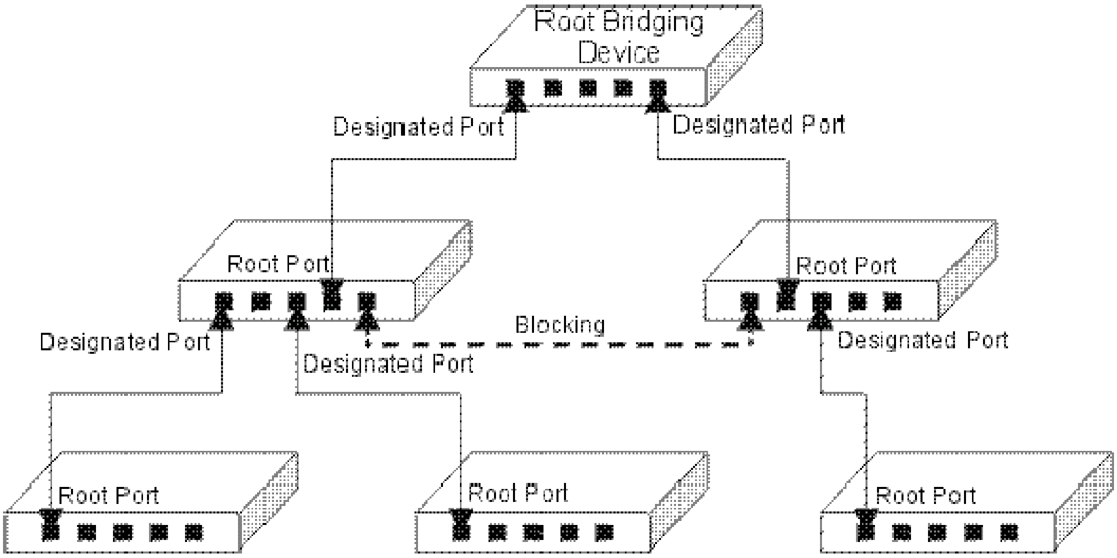
The Spanning Tree Algorithm (that is, the STA-configuration algorithm as outlined in IEEE 802.1D) can be used to detect and disable network loops, and to provide link backup. This allows the switch to interact with other bridging devices (including STA- compliant switches, bridges or routers) in your network to ensure that only one route exists between any two stations on the network. If redundant paths or loops are detected, one or more ports are put into a blocking state (stopped from forwarding packets) to eliminate the extra paths. Moreover, if one or more of the paths in a stable spanning tree topology fail, this algorithm will automatically change ports from blocking state to forwarding state to reestablish contact with all network stations.

STA uses a distributed algorithm to select a bridging device (STA-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports.

After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

The following figure gives an illustration of how the Spanning Tree Algorithm assigns bridging device ports.

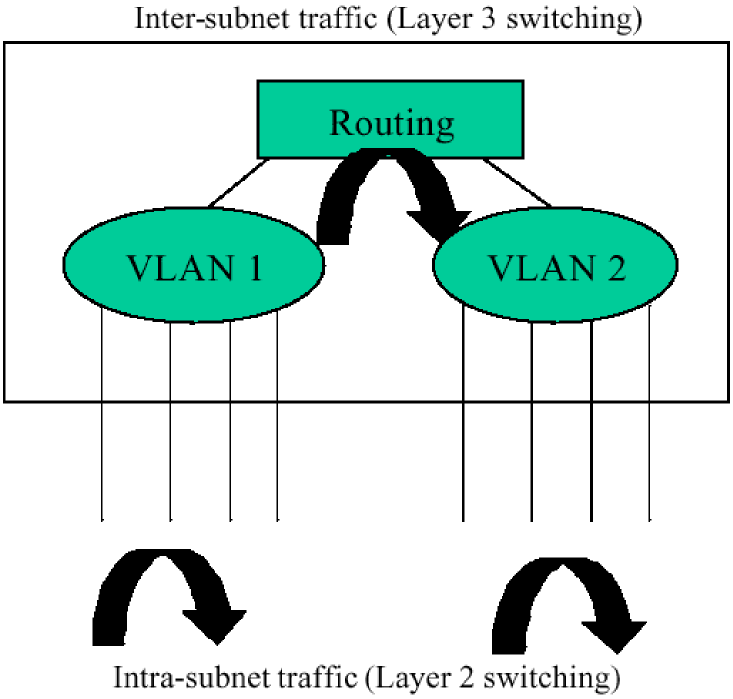


6.2 Layer 3 Switching

The two major functions provided by a Layer 3 switch include IP Switching and Routing Path Management. When the switch is set to multilayer mode, it acts as a routing switch, with support for standard IP routing and the ability to pass traffic between VLANs as required. However, when the switch is first set to multilayer mode, no default routing is defined. As with all traditional routers, the routing function must first be configured to work. (RIP).

6.2.1 Initial Configuration

In the default configuration, all ports belong to the same virtual LAN and the switch provides only Layer 2 functionality. So you should first group all the ports that belong to the same subnet into virtual LANs. By separating the switch into different VLANs, the network is partitioned into subnetworks that are disconnected at Layer 2. Network traffic within the same subnet is still switched using Layer 2 switching. And the VLANs can now be interconnected (only as required) with Layer 3 switching. Each VLAN represents a virtual interface to Layer 3. You just need to provide the network addresses for each virtual interface, and the traffic between different subnetworks will be routed by Layer 3 switching.


Inter-subnet traffic (Layer 3 switching)
Routing
VLAN 1
VLAN 2
Intra-subnet traffic (Layer 2 switching)

VLAN Configuration for Layer 3

Note: When operating the switch in multilayer mode, all ports should be defined as untagged, and no VLANs can overlap. You should also assign the same default PVID to the ports at both ends of a link if the VLAN must cross the switches. (See “VLAN Tagging” configuration.) These limitations will be removed for future firmware versions.

6.2.2 IP Switching

IP Switching (or packet forwarding) encompasses tasks required to forward packets for both Layer 2 and Layer 3, as well as traditional routing.

These functions include:

• Layer 2 forwarding (switching) based on the Layer 2 destination MAC address

• Layer 3 forwarding (routing):

- Based on the Layer 3 destination address
- Replacing destination/source MAC addresses for each hop
- Incrementing the hop count
- Decrementing the time-to-live
- Verifying and recalculating the Layer 3 checksum

If the destination node is on the same subnetwork as the source network, then the packet can be transmitted directly without the help of a router.

However, if the MAC address is not yet known to the switch, an Address Resolution Protocol (ARP) packet with the destination IP address is broadcast to get the destination MAC address from the destination node. The IP packet can then be sent directly with the destination MAC address.

If the destination belongs to a different subnet on this switch, the packet can be routed directly to the destination node. However, if the packet belongs to a subnet not included on this switch, then the packet should be sent to a router (with the MAC address of the router used as the destination MAC address, and the destination IP address of the destination node). The router will then forward the packet to the destination node via the correct path. The router can also use the ARP protocol to find out the MAC address of the destination node of the next router when necessary.

Note: In order to perform IP switching, the switch should be recognized by other network nodes as an IP router, either by setting it as the default gateway, or by redirection from another router via the ICMP process.

When the switch receives an IP packet addressed to its own MAC address, the packet follows the Layer 3 routing process. The destination IP address is checked against the Layer 3 address table. If the address is not already there, the switch broadcasts an ARP packet to all the ports on the destination VLAN to find out the destination MAC address. After the MAC address is discovered, the packet is reformatted and sent out to the destination. The reformat process includes decreasing the Time-To-Live (TTL) field of the IP header, recalculating the IP header checksum, and replacing the destination MAC address with either the MAC address of the destination node or that of the next hop router.

When another packet destined to the same node arrives, the destination MAC can be retrieved directly from the Layer 3 address table; the packet is then reformatted and sent out the destination port. IP switching can be done at wire-speed when the destination address entry is already in the Layer 3 address table.

If the switch determines that a frame must be routed, the route is calculated only during setup. Once the route has been determined, all packets in the current flow are simply switched or forwarded across the chosen path. This takes advantage of the high throughput and low latency of switching by enabling the traffic to bypass the routing engine once path calculation has been performed.

6.2.3 Routing Path Management

Routing Path Management involves the determination and updating of all the routing information required for packet forwarding, including:

- Handling routing protocols
- Updating the routing table
- Updating the Layer 3 switching database

6.2.4 ICMP Router Discovery

Before a host can send IP datagrams beyond its directly attached subnet, it must discover the address of at least one operational router on that subnet.

Typically, this can be accomplished by reading a list of one or more router addresses from a configuration file at start-up time. On multicast links, some hosts also discover router addresses by listening to routing protocol traffic.

The ICMP Router Discovery message is an alternative router discovery method that uses a pair of ICMP messages on multicast links. It eliminates the need to manually configure router addresses and is independent of any specific routing protocol.

ICMP Router Discovery messages are called “Router Advertisements” and “Router Solicitations.” Each router periodically multicasts a R outer Advertisement from each of its multicast interfaces, announcing the IP address(es) of that interface. Hosts discover the addresses of their neighboring routers simply by listening for advertisements. When a host attached to a multicast link starts up, it may multicast a Router Solicitation to ask for immediate advertisements, rather than waiting for the subsequent, periodic ones to arrive.

Router Discovery messages do not constitute a routing protocol: they enable hosts to discover the existence of neighboring routers, but not which router provides a route to a particular destination. If a host chooses a poor first-hop router for a particular destination, it should receive an ICMP Redirect from that router, identifying a better one.

6.2.5 Proxy ARP

When a node in the attached subnetwork does not have routing or a default gateway configured, ARP Proxy can be used to forward an ARP request to a remote subnetwork. When the switch receives an ARP request for a remote network and ARP Proxy is enabled, it determines if it has the best route to the remote network, and then answers the ARP request by sending its own MAC address to the requesting node. That node then sends traffic to the switch, which in turn uses its own routing table to forward the traffic to the remote destination. End stations that require Proxy ARP must view the entire network as a single network. These nodes must therefore use a smaller subnet mask than that used by the switch or other relevant network devices.

Note that extensive use of Proxy ARP can adversely affect the performance of the switch because it may lead to increased ARP traffic and increased search time for larger ARP address tables.

6.2.6 Routing Protocols

The switch supports both static and dynamic routing.

- Static routing requires routing information to be stored in the switch, either manually or when a connection is set up by an application outside the switch.
- Dynamic routing uses a routing protocol to exchange routing information, calculate routing tables, and respond to changes in the status or loading of the network.

Dynamic routing involves the determination and updating of all the routing information required for packet forwarding.

- Handling routing protocols
- Updating the routing table
- Updating the Layer 3 switc hing database

The switch supports RIP and RIP-2 dynamic routing protocols.

6.2.6.1 RIP and RIP-2 Dynamic Routing Protocols

The RIP protocol is the most widely used routing protocol. The RIP protocol uses a distance vector-based approach to routing. Routes are determined on the basis of minimizing the distance vector, or hop count, which serves as a rough estimate of transmission cost. Each router broadcasts its advertisement every 30 seconds, together with any updates to its routing table. This allows all routers on the network to learn consistent tables of next hop links which lead to relevant subnets. Just as Layer 2 switches use the Spanning Tree Algorithm to prevent loops, routers also use methods for preventing loops that would cause endless retransmission of data traffic. RIP utilizes the following three methods to prevent loops from occurring:

- Split horizon —never propagate routes back to an interface port from which they have been acquired.
- Poison reverse —propagate routes back to an interface port from which they have been acquired, but set the distance vector metrics to infinity. (This provides faster convergence.)
- Triggered updates — whenever a route gets changed, broadcast an update message after waiting for a short random delay, but without waiting for the periodic cycle.

RIP-2 is a compatible upgrade to RIP. RIP-2 adds useful capabilities for plain text authentication, multiple independent RIP domains, variable length subnet masks, and multicast transmissions for route advertising

(RFC 1388).

There are several serious problems with RIP that you should consider before deciding which routing protocol to use for your network. First of all, RIP (version 1) has no knowledge of subnets, both RIP versions can take a long time to converge on a new route after the failure of a link or router during which time routing loops may occur, and its small hop count limitation of 15 restricts its use to smaller networks. Moreover, RIP (version 1) wastes valuable network bandwidth by propagating routing information via broadcasts, nor does it consider enough network variables to make the best routing decision.

6.2.7 Non-IP Protocol Routing

The switch supports IP routing only. Non-IP protocols such as IPX and AppleTalk can not be routed by this switch, and will be confined within their local VLAN group unless bridged by an external router.

To coexist with a network built on other multilayer switches, the subnetworks for non-IP protocols must follow the same logical boundary as that of the IP subnetworks. A separate multi-protocol router can then be used to link the subnetworks by connecting to one port from each available VLAN on the network.

6.3 Virtual LANs

Switches do not inherently support broadcast domains, which can lead to broadcast storms in large networks that handle a lot of traffic such as NetBUEI or IPX. In conventional networks with routers, broadcast traffic is split up into separate domains to confine this traffic to the originating group and provide a much cleaner network environment. Instead of using physically separate subnets which are linked by traditionally slow routers, this switch creates segregated broadcast domains based on easily configurable VLANs, and then links these VLANs as required with wire-speed routing.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as video conferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

This switch supports the following VLAN features:

- Up to 256 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging and GVRP protocol
- Port overlapping, allowing a port to participate in multiple VLANs (Not supported for multilayer mode.)
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Priority tagging

6.3.1 Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) it will participate in. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port (that is, a port attached to a VLAN-aware device) if you want it to carry traffic for one or more VLANs and the device at the other end of the link also supports VLANs. Then assign the port at the other end of the link to the same VLAN(s). However, if you want a port on this switch to participate in one or more VLANs, but the device at the other end of the link does not support VLANs, then you must add this port as an untagged port (that is, a port attached to a VLAN-unaware device).

6.3.1.1 VLAN Classification

When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the PVID of the receiving port). But if the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

6.3.1.2 Port Overlapping

Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. (Not supported for multilayer mode) Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them by setting this switch to multilayer mode, and assigning an IP interface address to the different VLANs. (See “Connecting VLAN Groups”)

6.3.1.3 Port-based VLANs

Port-based (or static) VLANs are manually tied to specific ports. The switch’ s forwarding decision is based on the destination MAC address and its associated port. Therefore, to make valid forwarding or flooding decisions, the switch must learn the relationship of the MAC address to its related port —and thus to the VLAN —at run-time. However, when GVRP is enabled, this process can be fully automated.

6.3.1.4 Automatic VLAN Registration (GVRP)

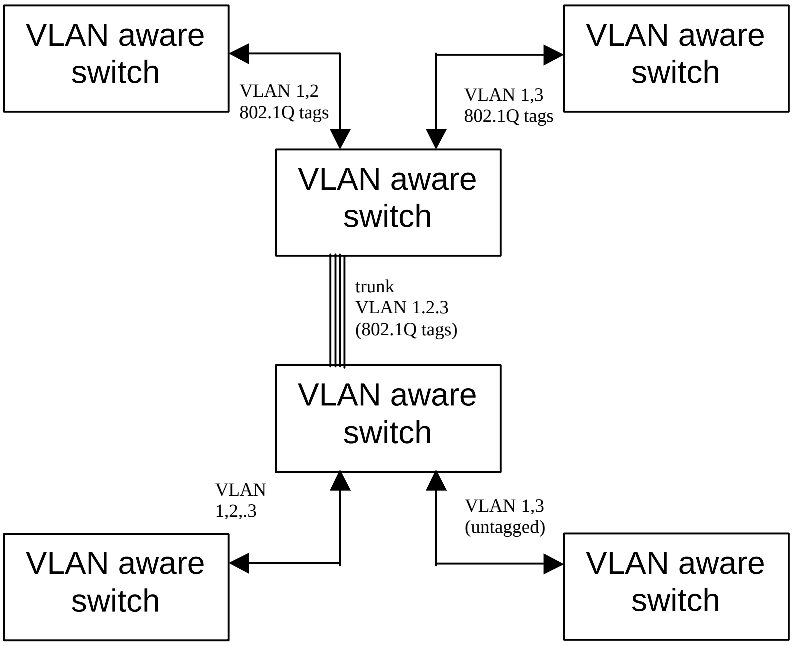
GVRP defines a system whereby the switch can automatically learn the VLANs each endstation should be assigned to. If an endstation (or its network adapter) supports the IEEE 802.1Q VLAN protocol, it can be configured to broadcast a message to your network indicating the VLAN groups it wants to join. When this switch receives these messages, it will automatically place the receiving port in the specified VLANs, and then forward the message to all other ports. When the message arrives at another switch that supports GVRP, it will also place the receiving port in the specified VLANs, and pass the message on to all other ports. VLAN requirements are propagated in this way throughout the network. This allows GVRP-compliant devices to be automatically configured for VLAN groups based solely on endstation requests.

6.3.2 Forwarding Tagged/Untagged Frames

Ports can be assigned to multiple tagged or untagged VLANs. Each port on the switch is therefore capable of passing tagged or untagged frames.

To forward a frame from a VLAN-aware device to a VLAN-unaware device, the switch first decides where to forward the frame, and then strips off the VLAN tag. However, to forward a frame from a VLAN-unaware device to a VLAN-aware device, the switch first decides where to forward the frame, and then inserts a VLAN tag reflecting this port' s default VID.

The default PVID is VLAN 1 for all ports, but this can be changed.



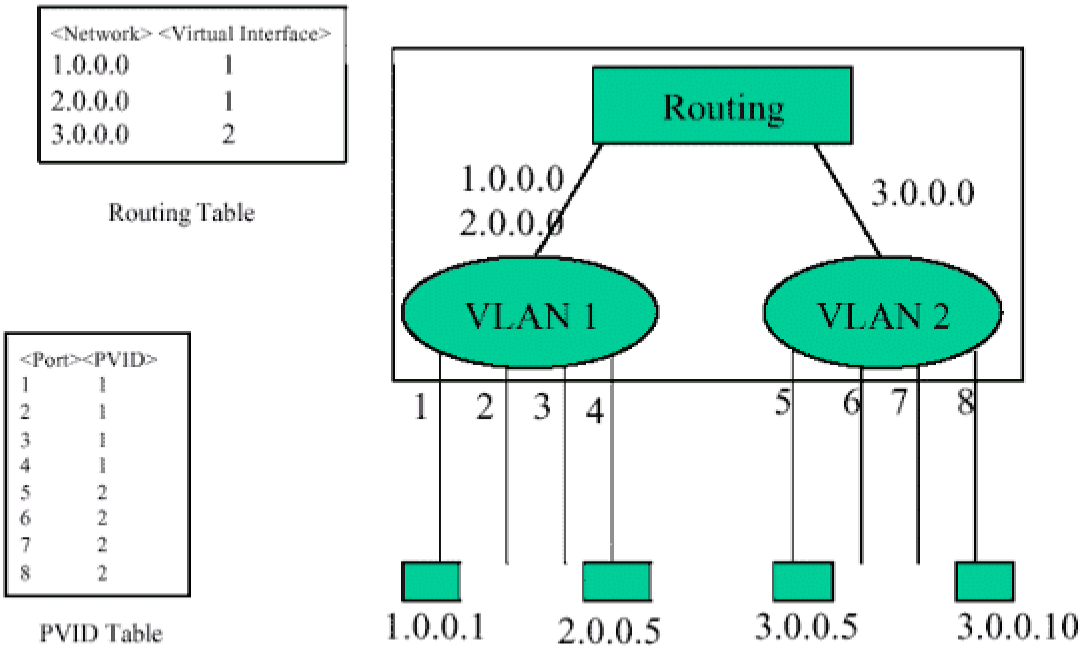
6.3.3 Connecting VLAN Groups

The switch supports communication within a common VLAN using store-and-forward switching. However, if you have devices in separate VLANs that must communicate, and it is not practical to include these devices in a common VLAN, then the VLANs can be connected via Layer 3 routing provided by this switch.

Traditional routers use only physical port numbers in their routing tables, which provides no support for VLANs. By contrast, this device supports Layer 3 routing by using both logical and physical port numbers to support VLANs and Layer 3 switching simultaneously.

By using the abstraction of a logical port number to represent a collection of physical switch ports in the same VLAN, Layer 3 switching can occur from one VLAN to another transparently without changing the routing protocol and IP routing software, while Layer 2 switching is still used for intra-VLAN traffic.

The switch uses standard routing tables that are constructed via static configuration or dynamic routing protocols such as RIP. Each routing entry consists of a network address (that is, an IP address with a subnet mask), and a virtual interface number. Each virtual interface corresponds to a virtual LAN, identified by the VLAN ID. Also note that multiple routing entries can be provided for the same virtual interface by adding the required routing table entries for the same virtual interface. A simple VLAN configuration that supports routing is shown below.



<Network>	<Virtual Interface>
1.0.0.0	1
2.0.0.0	1
3.0.0.0	2

Routing Table

<Port>	<PVID>
1	1
2	1
3	1
4	1
5	2
6	2
7	2
8	2

PVID Table

VLANs Connected via IP Routing

6.4 Multicast Filtering

Multicasting sends data to a group of nodes instead of a single destination. The simplest way to implement multicasting is to broadcast data to all nodes on the network. However, such an approach wastes a lot of bandwidth if the target group is small compared to the overall broadcast domain.

Since applications such as video conferencing and data sharing are widely used today, efficient multicasting has become vital. A common approach is to use a group registration protocol that lets nodes join or leave multicast groups. A switch or router can then easily determine which ports contain group members and send data out to those ports only. This procedure is called multicast filtering.

The purpose of IP multicast filtering is to optimize a switched network's performance, so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast routers/switches, instead of flooding traffic to all ports in the subnet (VLAN).

The switch routing switch supports IP multicast filtering not only by passively monitoring IGMP Query and Report messages and DVMRP Probe messages to register end-stations as multicast group members (Layer 2), but also by actively sending GMRP Query messages to learn the location of multicast routers/switches and member hosts in multicast groups within each VLAN (Layer 3). This switch also supports the DVMRP multicast routing protocol required to forward multicast traffic to other subnets.

6.4.1 IGMP Snooping

A Layer 2 switch can passively snoop on IGMP Query and Report packets transferred between IP multicast routers/switches and IP multicast host groups to learn the IP multicast group members. It simply monitors the IGMP packets passing through it, picks out the group registration information, and configures multicast filters accordingly. IGMP Snooping generates no additional network traffic, allowing you to significantly reduce the multicast traffic passing through your switch.

6.4.2 IGMP Protocol

The Internet Group Management Protocol (IGMP) runs between hosts and their immediately neighboring multicast router/switch. IGMP is as a multicast host registration protocol that allows any host to inform its local router that it wants to receive transmissions addressed to a specific multicast group.

A router, or multicast-enabled switch, can periodically ask their hosts is they want to receive multicast traffic. If there is more than one router/ switch on the LAN performing IP multicasting, one of these devices is elected “querier” and assume s the responsibility of querying the LAN for group members. It then propagates the service requests on to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

Based on the group membership information learned from IGMP, a router/switch can determine which (if any) multicast traffic needs to be forwarded to each of its ports. At Layer 3, multicast routers use this information, along with a multicast routing protocol such as DVMRP, to support IP multicasting across the Internet.

Note that IGMP neither alters nor routes any IP multicast packets. A multicast routing protocol must be used to deliver IP multicast packets across different subnetworks. Therefore, when DVMRP routing is enabled for a subnet on this switch, the switch will automatically enable IGMP.

6.4.3 GMRP Protocol

GARP Multicast Registration Protocol (GMRP) allows network devices to register end-stations with multicast groups. GMRP requires that any participating network devices or end-stations comply with the IEEE 802.1p standard. Compliant end-stations can request to receive traffic from a multicast group simply by issuing a *join* packet that includes a known multicast address. When the join packet reaches a port on the switch, it configures this port to receive multicast traffic for the requested group, and then issues a similar join packet to all other ports on the switch, informing them that incoming multicast traffic for the stated group is to be forwarded to the requesting port.

6.4.4 DVMRP Routing Protocol

The Distance-Vector Multicast Routing Protocol (DVMRP) behaves somewhat similar to RIP. A router supporting DVMRP periodically floods its attached networks to pass information about supported multicast services along to new routers and hosts. Routers that receive a DVMRP packet send a copy out to all paths (except the path back to the origin). These routers then send a prune message back to the source to stop a data stream if the router is attached to a LAN that does not want to receive traffic from a particular multicast group. However, if a host attached to this routing switch issues an IGMP message indicating that it wants to subscribe to the concerned multicast service, this switch will use DVMRP to build up a source-rooted multicast delivery tree that allows it to prevent looping and determine the shortest path to the source of this multicast traffic.

When this switch receives the multicast message, it checks its unicast routing table to locate the port that provides the shortest path back to the source. If that path passes through the same port the multicast message was received on, then this switch records path information for the concerned multicast group in its routing table and forwards the multicast message on to adjacent routers, except for the port through which the message arrived on. This process eliminates any potential loops from the tree and ensures that the shortest path (in terms of hop count) is always used.

6.5 Class-of-Service (CoS) Support

The switch provides two transmit queues on each port, with a weighted fair queuing scheme. This function can be used to provide independent priorities for various types of data such as real-time video or voice, and best-effort data.

Priority assignment to a packet in this switch can be accomplished in any of the following ways:

- Priority can be explicitly assigned by end stations which have applications that require a higher priority than best-effort. This switch utilizes the IEEE 802.1p and 802.1Q tag structure to decide priority assignments for the received packets.
- A port may be manually configured as high priority. In this case, when any other port receives traffic from a high-priority port, that traffic is automatically placed in the high-priority output queue.

6.6 BOOTP/DHCP Relay

Dynamic Host Configuration Protocol (DHCP), described in RFC 1541, is an extension of the Bootstrap Protocol (BOOTP). DHCP allows hosts on a TCP/IP network to dynamically obtain basic configuration information. When a DHCP client starts, it broadcasts a DHCP Request packet, looking for DHCP servers. DHCP servers respond to this packet with a DHCP Response packet. The client then chooses a server to obtain TCP/IP configuration information, such as its own IP address.

Since DHCP uses a broadcast mechanism, a DHCP server and its client must physically reside on the same subnet. However, it is not practical to have one DHCP server on every subnet; in fact in many cases, DHCP/BOOTP clients and their associated DHCP/BOOTP server(s) do not reside on the same IP network or subnet. In such cases, a third-party agent is required to transfer BOOTP messages between clients and servers.

BOOTP/DHCP Relay, described in RFC 1542, enables a host to use a BOOTP or DHCP server to obtain basic TCP/IP configuration information, even if the servers do not reside on the local subnet. When an Switch BOOTP/DHCP Relay Agent receives a DHCP Request packet destined for a BOOTP/DHCP server, it inserts its own IP address into the DHCP Request packet so the server knows the subnet where the client is located. Then, depending on the configuration setup, the switch either:

- Forwards the packet to a specific server as defined in the switch's configuration using unicast routing, or
- Broadcasts the DHCP Request again to another directly attached IP subnet specified in the switch configuration for the receiving IP subnet.

When the DHCP server receives the DHCP request, it allocates a free IP address for the DHCP client from its scope in the DHCP client's subnet, and sends a DHCP Response back to the DHCP Relay Agent. The DHCP Relay Agent then broadcasts this DHCP Response packet received from the DHCP server to the appropriate client.

6.7 Security Features

The switch provides security features that allow you to control management access and network access as described in the following sections.

6.7.1 SNMP Community Strings

Access to the switch using network management tools (HP OpenView) is controlled by SNMP community strings. This switch supports up to five community strings. A character string indicating the access rights of the management community must be provided whenever you send an SNMP message to the switch. Each community has either read-only or read/write access rights. A community that has read-only access can only use GET and GETNEXT commands to view the current configuration settings and status of the switch. While a community with read/write access can GET and GETNEXT commands, as well as the SET command to configure the switch.

6.7.2 User Name and Passwords

This switch can also be accessed via a direct connection to the console port, or through a network connection using Telnet or a Web browser. When managing the switch by any of these means, a user name and password is required to enter the system. There are two sets of user names and passwords. One set has administrator rights, which allows you to view or modify system parameters. The other set has read-only access, which allows you to view the status of the system, but not to modify it.

6.7.3 MAC Address Filters

If you discover that some nodes are sending abnormal or malicious data that could adversely affect the network or cause security problems, you can set their MAC addresses to be filtered by the switch. Any packets with a source or destination address listed in the MAC address filter will then be dropped by the switch upon entry.

6.7.4 IP Address Filters

IP addresses can also set to be filtered by the switch. IP packets with a source or destination address listed in the IP address filter will be dropped by the switch upon entry.

6.8 SNMP Management Software

SNMP (Simple Network Management Protocol) is a communication protocol designed specifically for managing devices or other elements on a network. Network equipment commonly managed with SNMP includes hubs, switches, bridges, routers and host computers. SNMP is typically used to configure these devices for proper operation in a network environment, as well as monitor them to evaluate performance and detect potential problems.

6.9 Remote Monitoring (RMON)

Remote Monitoring provides a cost-effective way to monitor large networks by placing embedded or external probes on distributed network equipment (hubs, switches or routers). Network management software can access the embedded probes in network products to perform traffic analysis, troubleshoot network problems, evaluate historical trends, or implement proactive management policies. RMON has already become a valuable tool for network managers faced with a quickly changing network landscape that contains dozens or hundreds of separate segments. RMON is the only way to retain control of the network and analyze applications running at multi-megabit speeds. It provides the tools you need to implement either reactive or proactive policies that can keep your network running based on real-time access to key statistical information.

This switch provides support for mini-RMON which contains the four key groups required for basic remote monitoring. These groups include:

Statistics: Includes all the tools needed to monitor your network for common errors and overall traffic rates. Information is provided on bandwidth utilization, peak utilization, packet types, errors and collisions, as well as the distribution of packet sizes.

History: Can be used to create a record of network utilization, packet types, errors and collisions. You need a historical record of activity to be able to track down intermittent problems. Historical data can also be used to establish normal baseline activity, which may reveal problems associated with high traffic levels, broadcast storms, or other unusual events.

Historical information can also be used to predict network growth and plan for expansion before your network becomes too overloaded.

Alarms: Can be set to test data over any specified time interval, and can monitor absolute or changing values (such as a statistical counter reaching a specific value, or a statistic changing by a certain amount over the set interval). Alarms can be set to respond to either rising or falling thresholds.

Events: Defines the action to take when an alarm is triggered. The response to an alarm can include recording the alarm in the Log Table or sending a message to a trap manager. Note that the Alarm and Event Groups are used together to record important events or immediately respond to critical network problems.

Appendix A Troubleshooting

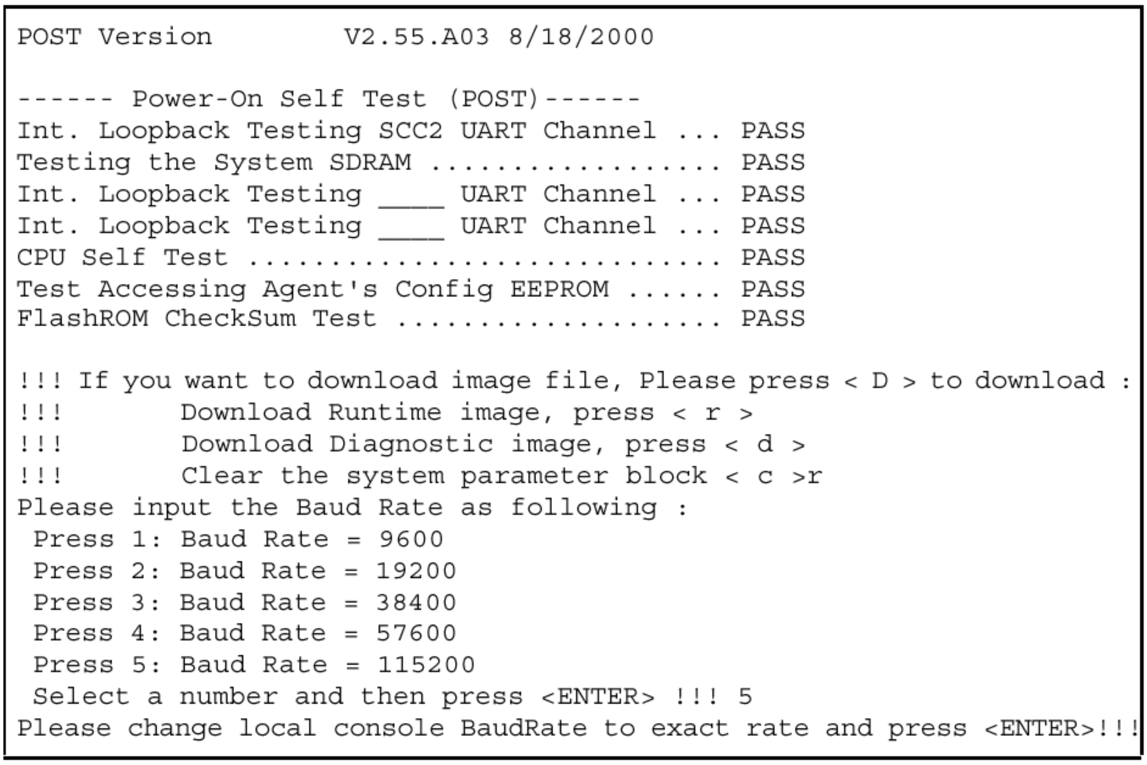
A.1 Troubleshooting Chart

Troubleshooting Chart	
Symptom	**Action**
Cannot connect using Telnet, Web browser, or SNMP software	• Be sure you have configured the agent with a valid IP address, subnet mask and default gateway (Layer 2). • Check that you have a valid network connection to the switch and that the port you are using has not been disabled. • Check network cabling between the management station and the switch. • If you cannot con nect using Telnet, there may already be four active sessions. Try connecting again at a later time.
Can' t access the on-board configuration program via a serial port connection	• Be sure you have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity, and 19200 bps. • Check that the null -modem serial cable conforms to the pin-out connections provided in Appendix B.
Forgot or lost the password	• Reinstall the switch firmware as described on the next page. Otherwise, contact Technical Support for help.

A.2 Upgrading Firmware via the Serial Port

You can upgrade system firmware by connecting your computer to the serial port on the switch, and using a console interface package that supports the XModem protocol. (See “3.2 Required Connections”)

1. Restart the system by using the Restart System command; or by pulling out the power cord to reset the power, waiting five seconds, and plugging it back in.



```
POST Version        V2.55.A03 8/18/2000

------ Power-On Self Test (POST)------
Int. Loopback Testing SCC2 UART Channel ... PASS
Testing the System SDRAM ................. PASS
Int. Loopback Testing ____ UART Channel ... PASS
Int. Loopback Testing ____ UART Channel ... PASS
CPU Self Test ............................ PASS
Test Accessing Agent's Config EEPROM ...... PASS
FlashROM CheckSum Test ................... PASS

!!! If you want to download image file, Please press < D > to download :
!!!       Download Runtime image, press < r >
!!!       Download Diagnostic image, press < d >
!!!       Clear the system parameter block < c >r
Please input the Baud Rate as following :
 Press 1: Baud Rate = 9600
 Press 2: Baud Rate = 19200
 Press 3: Baud Rate = 38400
 Press 4: Baud Rate = 57600
 Press 5: Baud Rate = 115200
 Select a number and then press <ENTER> !!! 5
Please change local console BaudRate to exact rate and press <ENTER>!!!
```

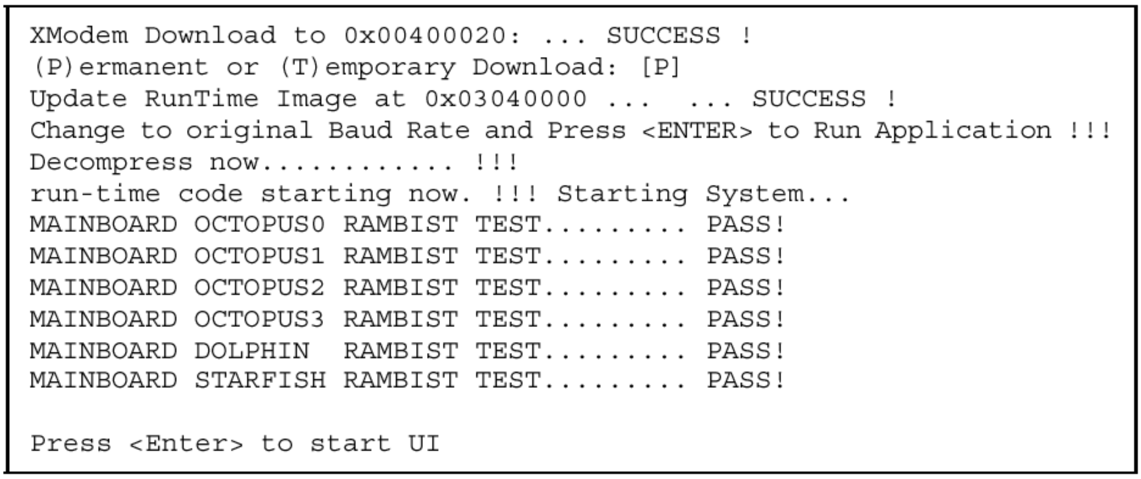
2. When the system initialization screen appears as shown above, press “D” to download system firmware, and then indicate the code type (<r> Runtime image or <d> Diagnostic image).
3. Change your baud rate to the selected value, and press Enter to enable download. From the terminal emulation program, select the file you want to download, set the protocol to XModem, and then initialize downloading.

Notes:

1. If you use Windows HyperTerminal, disconnect☎ , set the baud rate, and reconnect☎ .

2. The download file should be a binary file or an image file; otherwise the agent will not accept it.

4. After the file has been downloaded, the console screen will display information similar to that shown below. Press Enter to download to permanent memory, change the baudrate back to 19200, press Enter to start decompressing the new firmware, and then press Enter to open the Logon screen.



```
XModem Download to 0x00400020: ... SUCCESS !
(P)ermanent or (T)emporary Download: [P]
Update RunTime Image at 0x03040000 ...  ... SUCCESS !
Change to original Baud Rate and Press <ENTER> to Run Application !!!
Decompress now........... !!!
run-time code starting now. !!! Starting System...
MAINBOARD OCTOPUS0 RAMBIST TEST......... PASS!
MAINBOARD OCTOPUS1 RAMBIST TEST......... PASS!
MAINBOARD OCTOPUS2 RAMBIST TEST......... PASS!
MAINBOARD OCTOPUS3 RAMBIST TEST......... PASS!
MAINBOARD DOLPHIN  RAMBIST TEST......... PASS!
MAINBOARD STARFISH RAMBIST TEST......... PASS!

Press <Enter> to start UI
```

For details on managing the switch, refer to Chapter "Chapter 4. Console Interface" for information on the out-of-band console interface, or Chapter "Chapter 5. Web Interface" for information on the Web interface.

Appendix B Pin Assignments

B.1 Console Port Pin Assignments

The DB-9 serial port on the switch' s rear panel is used t o connect to the switch for out-of-band console configuration. The on-board menu-driven configuration program can be accessed from a terminal, a PC running a terminal emulation program, or from a remote location via a modem connection. The pin assignments used to connect to the serial port are provided in the following tables.

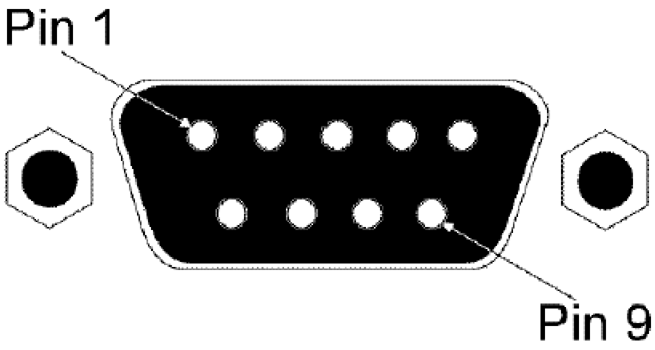


Figure B-1. DB-9 Console Port Pin Numbers

B.2 DB-9 Port Pin Assignments

EIA Circuit	CCITT Signal	Description	Switch's DB9 DTE Pin #	PC DB9 DTE Pin #	Modem DB25 DCE Pin #	Signal Direction DTE-DCE
CF	109	DCD (Data Carrier Detected)	1	1	8	<------
BB	104	RxD (Received Data)	3	2	3	<------
BA	1033	TxD (Transmitted Data)	2	3	2	------>
CD	108	DTR (Data Terminal Ready)	6	4	20	------>
AB	102	SG (Signal Ground)	5	5	7	-------
CC	107	DSR (Data Set Ready)	4	6	6	<------
CA	105	RTS (Request-to-Send)	8	7	4	------>
CB	106	CTS (Clear-to-Send)	7	8	5	<------
CE	125	RI (Ring Indicator)	9	9	22	<------

B.3 Console Port to 9-Pin COM Port on PC

Switch's 9 -Pin Serial Port	CCITT Signal	PC's 9 -Pin COM Port
1 DCD	----------- DCD ------------	1
2 TXD	----------- RXD ---------->	2
3 RXD	<--------- TXD ------------	3
4 DSR	----------- DTR ------------	4
5 SGND	----------- SGND ----------	5
6 DTR	----------- DSR ---------->	6
7 CTS -	<--------- RTS ------------	7
8 RTS	----------- CTS ----------->	8
9 RI	----------- RI ---------------	9

B.4 Console Port to 25-Pin DCE Port on Modem

Switch' s 9 -Pin Serial Port	CCITT Signal	Modem's 25 -Pin DCE Port
1	<--------- DCD ------------	8
3	<--------- RXD ------------	3
2	----------- TXD ---------->	2
6	----------- DTR ---------->	20
5	----------- SGND ----------	7
4	<--------- DSR ------------	6
8	----------- RTS ----------->	4
7	<--------- CTS -------------	5
9	<--------- RI ---------------	22

GLOSSARY

Bandwidth Utilization
The percentage of packets received over time as compared to overall bandwidth.

BOOTP
Boot protocol used to load the operating system for devices connected to the network.

Distance Vector Multicast Routing Protocol (DVMRP)
A distance-vector-style routing protocol used for routing multicast datagrams through the Internet. DVMRP combines many of the features of RIP with Reverse Path Broadcasting (RPB).

GARP VLAN Registration Protocol (GVRP)
Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

Generic Attribute Registration Protocol (GARP)
GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment such that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. Formerly called Group Address Registration Protocol.

Group Attribute Registration Protocol
See Generic Attribute Registration Protocol.

Generic Multicast Registration Protocol (GMRP)
GMRP allows network devices to register end-stations with multicast groups. GMRP requires that any participating network devices or end-stations comply with the IEEE 802.1p standard.

ICMP Router Discovery
ICMP Router Discovery message is an alternative router discovery method that uses a pair of ICMP messages on multicast links. It eliminates the need to manually configure router addresses and is independent of any specific routing protocol.

Internet Control Message Protocol (ICMP)
Commonly used to send echo messages (i.e., Ping) for monitoring purposes.

IEEE 802.1D
Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

IEEE 802.1Q
VLAN Tagging —Defines Ethernet frame tags which carry VLAN information. It allows switches to assign end-stations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

IEEE 802.3ac
Defines frame extensions for VLAN tagging.

Internet Group Management Protocol (IGMP)
A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast router on a given subnetwork, one of the routers is elected "querier" and assumes the responsibility of keeping track of group membership.

IGMP Snooping
Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to learn IP Multicast group members.

In-Band Management
Management of the network from a station attached directly to the network.

IP Multicast Filtering
A process whereby this switch can pass multicast traffic along to participating hosts.

Layer 2
Data Link layer in the ISO 7-Layer Data Communications Protocol. This is directly related to the hardware interface for network devices and passes traffic based on MAC addresses.

Layer 3
Network layer in the ISO 7-Layer Data Communications Protocol. This layer handles the routing functions for data moving from one open system to another.

Link Aggregation
See Port Trunk.

Management Information Base (MIB)
An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

Multicast Switching
A process whereby the switch filters incoming multicast frames for services no attached host has registered for, or forwards them to all ports contained within the designated multicast VLAN group.

Open Shortest Path First (OSPF)
OSPF is a link state routing protocol that functions better over a larger network such as the Internet, as opposed to distance vector routing protocols such as RIP. It includes features such as unlimited hop count, authentication of routing updates, and Variable Length Subnet Masks (VLSM).

Out-of-Band Management
Management of the network from a station not attached to the network.

Port Mirroring
A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobtrusively.

Port Trunk
Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

Remote Monitoring (RMON)
RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.

Routing Information Protocol (RIP)
The RIP protocol attempts to find the shortest route to another device by minimizing the distance vector, or hop count, which serves as a rough estimate of transmission cost. RIP-2 is a compatible upgrade to RIP. It adds useful capabilities for subnet routing, authentication, and multicast transmissions.

Simple Network Management Protocol (SNMP)
The application protocol offering network management services in the Internet suite of protocols.

Serial Line Internet Protocol (SLIP)
Serial Line Internet Protocol, a standard protocol for point-to-point connections using serial lines.

Spanning Tree Protocol (STP)
A technology that checks your network for any loops. A loop can often occur in complicated or back-up linked network systems. Spanning-tree detects and directs data along the shortest path, maximizing the performance and efficiency of the network.

Telnet
Defines a remote communication facility for interfacing to a terminal device over TCP/IP.

Trivial File Transfer Protocol (TFTP)
A TCP/IP protocol commonly used for software downloads.

Virtual LAN (VLAN)
A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, allowing users to share information and resources as though located on the same LAN.

XModem
A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.