Gateway™

User Guide

Gateway Layer-2 Managed Ethernet Switch

Contents

1 Introducing the Gateway Layer-2 Managed Switch 1

Features 2
- Ports 2
- Performance 2
- Management 3
- Switch stacking 3

Unpacking your switch 4
Setting up your switch 4
- Desktop or shelf installation 5
- Rack installation 5
- Power on 6
- Power failure 7

Identifying components 7
- Front panel 7
- Rear panel 8
- Side panels 8
- LED indicators 9

2 Connecting the Switch 11

Switch to end node 12
Switch to hub or switch 13
Switch stack connections 13

3 Layer-2 Switch Management Concepts 15

Local console management 16
- Diagnostic (console) port (RS-232 DCE) 16

Stacking versus standalone operation 17
- Managing switch stacks 19

Switch IP address 23
SNMP network management 25
- SNMP Versions 1, 2, and 3 25

Forwarding and filtering 27
- MAC address aging time 28
- Filtering and access profile masking 28

802.1w Rapid Spanning Tree 29
- Port transition states 29

Link aggregation 30
- Static vs. LACP link aggregation 31

VLANs 32
- VLAN implementation 32

Multicasting 37

4 Web-Based Switch Management 41

Configuring the switch 42
Getting started 42
Web-based manager's user interface 43
Areas of the user interface 44
Managing user accounts 45
Saving changes 47
Resetting the switch 48
Restarting the switch 49
Configuring the switch 50
Setting the IP address 51
Setting and viewing basic switch information 53
Setting advanced switch information 55
Configuring individual switch ports 56
Setting up port mirroring 58
Using IGMP 59
Using Spanning Tree Protocol (STP) 63
Using forwarding filtering 66
Creating, modifying, and deleting VLANs 71
Setting the port bandwidth 75
Simple Network Time Protocol (SNTP) settings 76
Setting port security 80
Using 802.1p priority queuing (QoS) 81
Using MAC notification 87
Using Link Aggregation Control Protocol (LACP) 89
Using access profiles 92
Using system log servers 100
PAE Access Entity 102
Management 109
Setting up a switch for remote management 110
Managing user accounts 110
Using SNMPV3 111
Monitoring 122
Viewing Port Utilization 123
Viewing packet statistics 124
Viewing errors 130
Viewing packet size 134
Viewing the MAC address forwarding table 137
Viewing the IGMP Snooping Group 138
Viewing IGMP Snooping forwarding table 139
Viewing VLAN status 140
Viewing router port 140
Viewing port access control information 142
Maintenance 143
Using TFTP services 143
Viewing switch history 146

Performing a Ping test 147
Saving changes 147
Rebooting the switch 147
Logging out 148

5 Technical Support 149

Telephone numbers 150

A Safety, Regulatory, and Legal Information 151

Index 157

Chapter 1

Introducing the Gateway Layer-2 Managed Switch

- Features
- Unpacking and setting up
- Identifying components

Features

The Gateway managed switch is designed for easy installation and high performance in an environment where traffic on the network and the number of users increase continuously. Features of this switch include:

Ports

- 24 or 48 high performance NWay ports all operating at 10/100/1000 Mbps with Auto-MDIX (Medium Dependent Interface crossover) function for connecting to end stations, servers, and hubs.
- All ports can auto-negotiate (NWay) between 10/100/1000 Mbps, half-duplex, or full-duplex and flow control for half-duplex ports.
- RS-232 DCE (Distributed Computing Environment) Diagnostic port (console port) for setting up and managing the switch through a connection to a console terminal or computer using a terminal emulation program.

Performance

- 24 or 48 built-in 10/100 Mbps ports + 2 SPF/mini-GBIC (7601 series)
- 24 or 48 built-in 10/100/1000 Mbps ports + 4 SPF/mini-GBIC (7801 series)
- Switch-stacking configuration: 8 units per stack + 8 GBIC ports
- 8.8 Gbps switching fabric capacity (7601 series)
- 35.7 Mpps switch fabric (7801 series)
- Auto MDI/MDIX uplink for all twisted-pair ports
- Supports 802.1Q VLAN, IGMP snooping, 802.1p Priority Queues, and port mirroring
- Multi-layer ACL and QoS control
- 802.1x port-based and MAC-based access control
- Asymmetric VLAN support
- Simple Network Time Protocol support
- Multicast filtering per port
- Per-port bandwidth control
- IEEE 802.3z compliant for all Gigabit ports (optional)
- IEEE 802.3x compliant Flow Control support for all Gigabit ports (optional)

Management

- RS-232 console port for out-of-band network management using a console terminal or computer
- IEEE 802.1w Rapid Spanning Tree Algorithm Protocol for creation of alternative backup paths and prevention of network loops
- SNMP (v.1, v.2, v.3) Agent
- IEEE 802.1X support
- Port security
- Fully configurable either in-band or out-of-band control through console serial connection
- Flash memory for software upgrades. This can be done in-band using TFTP (Trivial File Transfer Protocol) or out-of-band through the console. Download the latest switch firmware from the Gateway Web site
- Built-in SNMP (Simple Network Management Protocol) management:
  - Bridge MIB (RFC 1493)
  - MIB-II (RFC 1213)
  - Mini-RMON MIB (RFC 1757) - four groups
  - 802.1p MIB (RFC 2674)
  - IF MIB (RFC 2233)
  - Ether-Like MIB (RFC 1643)
- Supports Web-based management
- CLI management support
- TFTP support
- BOOTP support
- DCHP client support

Switch stacking

The Gateway managed switch can be used as a standalone switch or as a stacked switch using the Gigabit combo ports. As many as eight switches can be stacked and managed as a unit with a single IP address.

Management for the entire stack is done through the master switch.

You can add switches later as needed.

Fast Ethernet technology

100Mbps Fast Ethernet (or 100BASE-T) is a standard specified by the IEEE 802.3 LAN committee. It is an extension of the 10Mbps Ethernet standard with the ability to transmit and receive data at 100Mbps, while maintaining the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Ethernet protocol.

Gigabit Ethernet technology

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

Unpacking your switch

Open the shipping carton of the switch and carefully unpack its contents. The carton should contain the following items:

- One Gateway 24-port or 48-port Fast Ethernet Layer 2 managed switch
- Mounting kit: two mounting brackets and screws
- Four rubber feet with adhesive backing
- One AC power cord
- A CD containing this user guide

If any item is found missing or damaged, contact Gateway for replacement.

Setting up your switch

Use the following guidelines when choosing a place to install the switch:

- The surface must support at least 6.6 pounds (3 kg).
- The power outlet should be within 6 feet (1.82 meters) of the switch.
- Make sure that there is adequate heat dissipation from and adequate ventilation around the switch. Do not place heavy objects on the switch.

Desktop or shelf installation

To install the switch on a desktop or shelf:

- Attach the rubber feet on the bottom at each corner of the switch.

Important

Allow adequate space for ventilation between the device and the objects around it.

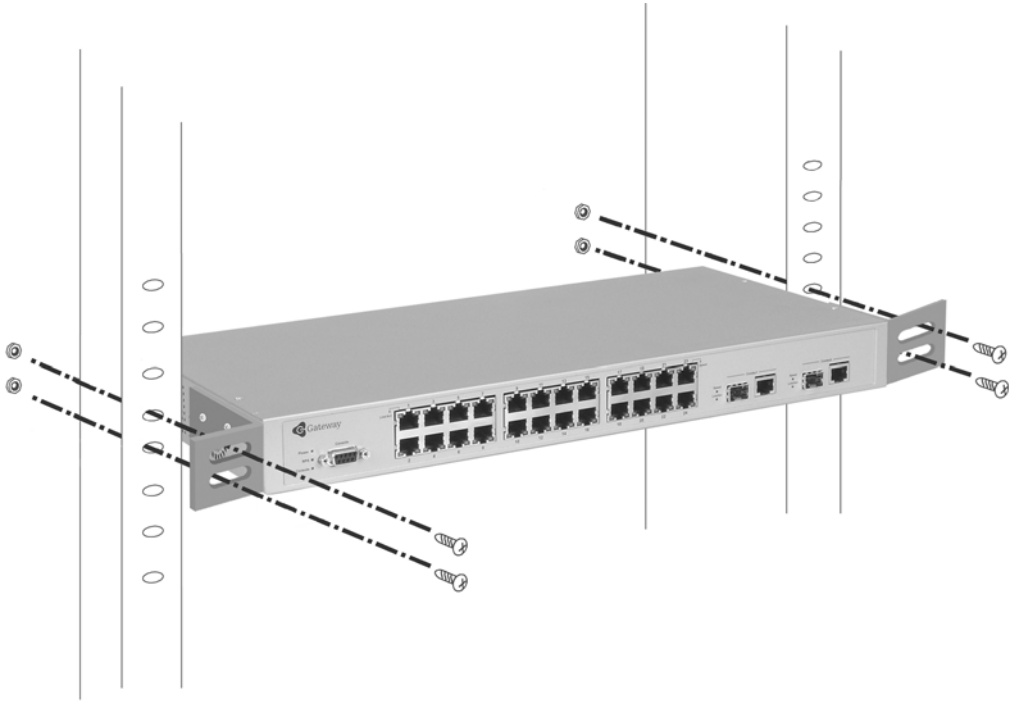
Rack installation

The Gateway managed switch can be mounted in an EIA standard-sized, 19-inch rack, which can be placed in a wiring closet with other equipment.

To install the switch in a rack:

1. Attach the mounting brackets on the switch's side panels (one on each side) and secure them with the screws provided.

2 Use the screws provided with the equipment rack to mount the switch on the rack.



Power on

The Gateway managed switch can be used with an AC power supply of 100 - 240 VAC, 50 - 60 Hz. The power switch is located at the rear of the unit adjacent to the AC power connector and the system fan. The switch's power supply will adjust to the local power source automatically and can be turned on without having any or all LAN segment cables connected.

After the power switch is turned on, the LED indicators should respond as follows:

- All LED indicators will momentarily blink. This blinking of the LED indicators represents a reset of the system.
- The power LED indicator is always on after the power is turned on.
- The console LED indicator will blink while the switch loads on-board software and performs a self-test. It will remain on if there is a connection at the RS-232 port, otherwise this LED indicator is off.
- The 100 M LED indicator can remain on or off depending on the transmission speed.

Important

Visually inspect the power cord and see that it is secured to the AC power connector.

Power failure

As a precaution in the event of a power failure, unplug the switch. When the power supply is restored, plug the switch back in.

Identifying components

Front panel

The front panel of the switch consists of LED indicators, an RS-232 communication port, 24 or 48 (10/100 Mbps) Ethernet/Fast Ethernet ports, and four Gigabit combination ports.

Features include:

- Comprehensive LED indicators display the status of the switch and the network (see "LED indicators" on page 9).
- An RS-232 DCE console port for setting up and managing the switch using a connection to a console terminal or computer using a terminal emulation program.
- Twenty-four high-performance, NWay Ethernet ports all of which operate at 10/100 Mbps with Auto-MDIX function for connections to end stations, servers, and hubs. All ports can auto-negotiate between 10 Mbps or 100 Mbps, full or half duplex, and flow control.

Rear panel

The rear panel of the switch contains an AC power connector.

The AC power connector is a standard three-pronged connector that supports the power cord. Plug one end of the provided power cord into this socket, and the other end of the cord into a power outlet. Supported input voltages range from 100 ~ 240 VAC at 50 ~ 60 Hz.

Side panels

The right side panel of the switch contains two system fans (see the top part of the following illustration). The left side panel contains heat vents.

The system fans are used to dissipate heat. The sides of the system also provide heat vents to serve the same purpose. Do not block these openings, and leave at least six inches of space at the rear and sides of the switch for adequate ventilation.

Caution

Without adequate heat dissipation and air circulation, system components might overheat, which could lead to system failure.

LED indicators

The LED indicators on the switch include Power, Console, and Link/Act. The following illustration shows a close-up of the Gigabit in and Gigabit out ports and the LED indicators.

- **Power** - This indicator on the front panel should be lit during the Power-On Self Test (POST). It will turn green approximately two seconds after the switch is powered on to indicate the ready state of the device.
- **RPS** - This indicator is orange when the RPS (Redundant Power Supply) is in standby mode. It turns green when the RPS is triggered.
- **Console** - This indicator is green when the switch is being managed through out-of-band/local console management through the RS-232 console port using a straight-through serial cable.
- **Act/Link/Speed** - These indicators are located to the left and right of each port. The right-side indicator lights when the port has a link of 100 Mbps. The Link indicator will not light for 10 Mbps links. The LEDs blink whenever there is reception or transmission of data occurring at a port.

Chapter 2

Connecting the Switch

- Switch to end node
- Switch to hub or switch
- Switch stack connections

Switch to end node

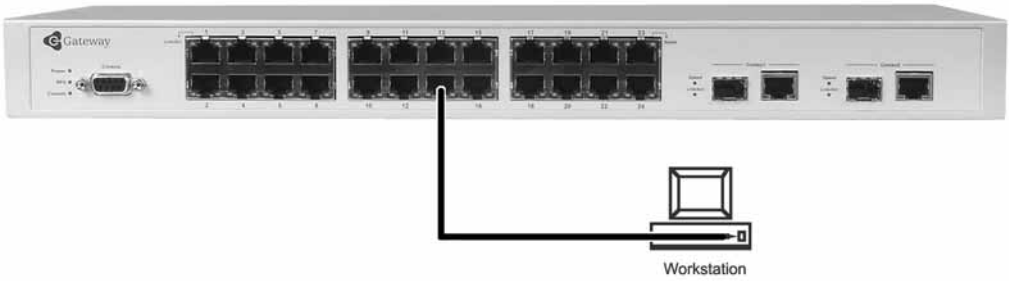
End nodes include computers outfitted with a 10, 100, or 10/100 Mbps RJ-45 Ethernet/Fast Ethernet NIC (Network Interface Card) and most routers.

An end node can be connected to the switch using a two-pair Category 3, 4, or 5 UTP/STP (unshielded twisted pair/shielded twisted pair) straight cable.

Important

Be sure to use Category 5 UTP or STP cabling for 100 Mbps Fast Ethernet connections. Connections to the Gigabit combo ports must also use Category 5e.

The end node should be connected to any of the twenty-four ports or any of the forty-eight ports of the Gateway managed switch.



The LED indicators for the port that the end node is connected to are lit according to the capabilities of the NIC. If LED indicators are not illuminated after making a connection, check the computer's LAN card, the cable, switch conditions, and connections. The following LED indicator states are possible for an end node to switch connection:

- The 100 LED indicator lights for a 100 Mbps and stays off for 10 Mbps.
- The Link/Act LED indicator lights after hooking up a computer that is turned on.

Switch to hub or switch

Switch to hub or switch to switch connections can be accomplished at any port in either straight-through cable or a crossover cable because the switch supports Auto-MDIX function.

- A 10BASE-T hub or switch can be connected to the switch using two-pair Category 3, 4, or 5 UTP/STP cable.
- A 100BASE-TX hub or switch can be connected to the switch using two-pair Category 5 UTP cable.
- A 1000BASE-T connections use two-pair Category 5e UTP cable.

Switch stack connections

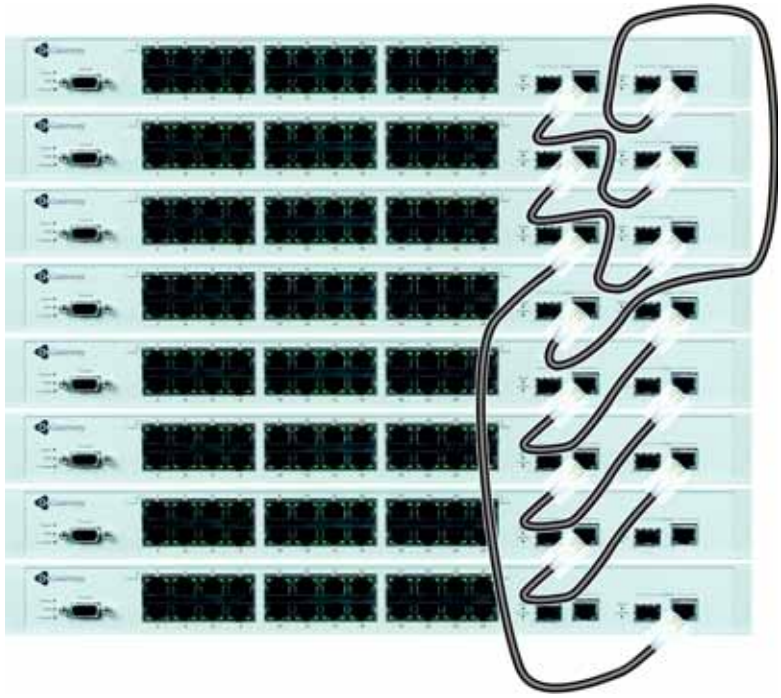
As many as eight Gateway managed switches can be stacked into a switch stack that can then be configured and managed as a single unit. The management agent of the master switch can configure and manage all of the switches in a switch stack using a single IP address (the IP address of the master switch).

Important

Stacking mode is configured using the CLI command **config stacking mode**. The default settings allow the switch to function as a standalone device or as a member of a stacked group.

The IEEE 1394 compliant cable must be connected from a Gigabit *in* port on one switch to a Gigabit *out* port on the next switch in the stack. The last two switches (at the top and bottom of the stack) must also be connected from the Gigabit *in* port on one switch to the Gigabit *out* port on the other switch. In this way, a loop is made such that all of the switches in the switch stack have the *in* stacking port connected to another switch's *out* stacking port.

An example stacking port interconnection is shown in the following illustration:



Important

If a link between stacked switches fails the stacked group must be connected to work around the failed link. As with any changes in the composition of the stacked switch group, the new stacking relationship must be negotiated. Any change to the composition of a stacked switch group or any failure of a stacking port will cause the entire stack to restart and negotiate the new stacking composition.

10BASE-T device

For a 10BASE-T device, the switch's LED indicators should display the following:

- 100 LED speed indicator is off.
- Link/Act indicator is on.

100BASE-TX device

For a 100BASE-TX device, the switch's LED indicators should display the following:

- 100 LED speed indicator is on.
- Link/Act is on.

Chapter 3

Layer-2 Switch Management Concepts

- Local console management
- Stacking versus stand alone operation
- Switch IP address
- SNMP network management
- Forwarding and filtering
- 802.1w Rapid Spanning Tree
- Link aggregation, VLANs, and multicasting

Local console management

A local console is a terminal or a workstation running a terminal emulation program that is connected directly to the switch using the RS-232 serial console port on the front of the switch. A console connection is referred to as an *Out-of-Band* connection, meaning that the console is connected to the switch using a different circuit than that used for normal network communications. So, the console can be used to set up and manage the switch even if the network is down.

Local console management uses the terminal connection to operate the switch's built-in console program. A network administrator can manage, control, and monitor the switch from the console program.

The Gateway managed switch contains a processor, memory for data storage, flash memory for configuration data, operational programs, and SNMP (Simple Network Management Protocol) agent firmware. These components allow the switch to be actively managed and monitored from either the console port or the network itself (out-of-band or in-band).

Diagnostic (console) port (RS-232 DCE)

Out-of-band management requires connecting a terminal, such as a VT-100 or a computer running a terminal emulation program (such as HyperTerminal, which is automatically installed with Microsoft Windows) to the switch's RS-232 DCE (Distributed Computing Environment) console port. Switch management using the RS-232 DCE console port is called *Local Console Management* to differentiate it from management performed using management platforms, such as D-View or HP OpenView. *Web-based Management* describes management of the switch performed over the network (*in-band*) using the switch's built-in Web-based management program (see "Web-Based Switch Management" on page 41). The operations to be performed and the facilities provided by these two built-in programs are identical.

The console port is set at the factory to the following configuration:

- Baud rate: 9,600
- Data width: 8 bits
- Parity: none
- Stop bits: 1
- Flow Control: None

Make sure that the terminal or computer you are using to make this connection is configured to match these settings.

If you are having problems making this connection on a computer, make sure the emulation is set to VT-100. If you still do not see anything, try pressing **CTRL** + **R** to refresh the screen.

Stacking versus standalone operation

By default, the switch configuration settings allow it to operate as a standalone device or in a stacked group. It is not necessary to change any settings for the switch to function in either capacity. However, it is useful to understand how the stacking mode operates in the switch and the effects, if any, this can have on configuration settings in a switch when its stacking status is changed.

Stacking mode is enabled by default and can be changed using the CLI (command line interface) command **config stacking mode**. If the switch has stacking mode enabled and is correctly connected to other Gateway managed switches, a negotiation takes place after starting up the switches to determine how the switch functions in the stack. For an all-Gateway managed switch stack, any time a change occurs in the structure or composition of a stacked switch group the entire stack will restart and the negotiation process begins anew. When the stacking mode is disabled (**config stacking mode disable**), the switch only allows standalone operation. If stacking mode is disabled on a switch, it should be disconnected from a stacked group.

Stacking mode can be changed using the CLI. When a Gateway managed switch stack is first assembled, it is advisable to determine which switch will function as the master before placing the switches in a rack and connecting them. The possible stacking configuration modes are as follows:

- **Enabled**: Stacking mode is enabled by default. When enabled, the switch can operate as a standalone device or it can operate with other Gateway managed switches in a correctly connected stacked group. Stacking must be enabled for the switch function in a stacked arrangement with other Gateway managed switches. If stacking is enabled, the following modes are available:
  - **Auto**: This is the default stacking mode setting for the Gateway managed switch. In auto stacking mode the switch is eligible for stacking or it can operate as a standalone device. If a Gateway managed switch stack is connected and all units are configured to operate in auto stacking mode, the master-slave relationships is determined automatically. For Gateway managed switch stacks, the unit with the lowest MAC address becomes the master (stack number 1). The order in which slave devices appear logically in the stack (stack number 2+) is determined by how they are connected relative to the master switch. The auto mode serves to first determine if the device is stacked or standalone, then if stacked, it determines which switch is the master and the remaining stack numbers for the slave switches.

- **Master**: The auto mode described above can be overridden so that a correctly connected switch in a stack can be forced into master mode. Only one switch in a stack can act as the master and all configuration settings for the stacked group, including stacking configuration, are saved in configuration files in the master switch. The stack is managed as a single entity through the master. It can be convenient to place the master unit in the upper-most slot of a stacked group to visually distinguish it from the slave units. The master unit should be used to uplink the stack group to the backbone. If the master unit fails or is replaced for any reason, it is possible to load configuration files saved from the original master unit in order to continue operation with identical settings. See "Swapping a master from a stack" on page 23 for a description of how to swap the master unit of a stacked group. A switch configured as the stack master will maintain this status regardless of any changes that occur in the composition of the stacked group. If, for example, a connection to a slave unit or a connection between two slave units were to fail, the entire stack will restart automatically. After restarting, the designated master unit retains its status.
- **Slave**: The auto mode can be overridden to force the switch to operate in slave mode. When the switch is in slave mode, it is ineligible to function as a master and all configuration is done through the master unit. A master switch must be correctly connected to the stack for a switch to operate in slave mode.

- **Disabled**: This forces the switch to operate as a standalone device. To force standalone operation it is necessary to use the CLI command **config stacking mode disable**. A switch that has stacking mode disabled should never connect to another switch through stacking ports.

Important

Do not use stacking ports on a switch that has the stacking mode disabled.

For Gateway managed switch stacks, changes made to the composition of a switch stack group, that is, adding new switches or taking switches out of the stack, require all switches to restart. The new stacking order is negotiated to reflect the changes made to the group. If the master switch has been configured to force master status it retains this status, likewise switches forced to operate in slave mode retain the status after restarting. The restart occurs automatically if any stacking link is disconnected.

The command **show stacking** can be used to view stacking information. If stacking has been disabled, the stacking mode will be listed as standalone.

Managing switch stacks

Multiple Gateway managed switches can be connected in a stacking arrangement so that as many as eight switches are managed as a single unit with a single IP address.

The default stacking mode will establish a master switch for the stack through a negotiation process that takes place when all devices are started up. In a Gateway managed switch stack, the switches negotiate the master-slave relationship. Once the master switch is determined, the remaining switches function as slaves. The stack number of the slave switches is determined by where it is actually positioned in the stack. This can be taken into account when you are placing the switches in an equipment rack.

Keep in mind the following important considerations for stacked switch groups:

- All management of the switches in the stack is done through the master switch.
- The master switch should be used to uplink to the Ethernet backbone.
- For Gateway managed switch stacks, the master switch can be chosen automatically as each switch in a connected stack competes for status. However, you can choose a specific device and force it to operate as the master. Use the CLI command **config stacking mode enabled master** for the selected switch. Leave the remaining switches in the default auto-stacking mode.
- For Gateway managed switch stacks, if the link between any two switches fails or is disconnected, or if any switch in a stacked group fails, all of the switches in the stack will automatically reboot. Because the stack is connected as a ring, the stack will need to be reconnected to work around the failed link. Change the cabling to bypass the failed link and allow the stack to reboot. The switches will negotiate again because the composition of the stack has been altered. Read "Making changes to switch stack structure" on page 19 for more information about changes in stacked switch groups.
- A switch stack has a single IP address. If the stacking link to a given switch fails or is disconnected, that switch will loose its status in the stack and reboot as a standalone device with the IP settings it had before becoming a member of the switch stack.

Important

The Gateway managed switch maintains two separate configurations, one for standalone operation and another for stacked operation. Each configuration has identical IP settings, VLANs, link aggregation, and QoS. This dual system allows a switch to change status from standalone to stacking enabled and keep its configuration settings.

Making changes to switch stack structure

If switches are added to or taken out of a stacked group of Gateway managed switches, it is necessary to change the composition of a switch stack and rearrange the stacking connections. If a stacking link fails or if a member of a stacked group fails, the composition of the stack will necessarily change also. In such a case intervention is required to at least reconnect the stacking cable to bypass the failure. In addition to making changes to the

cable links connecting the switches in the stack, it might be necessary or desirable to change the stacking mode configuration of one or more units. A few of the following examples show how to make the changes to cable connections for Gateway managed switch stacks and if necessary, to switch stacking mode configuration settings.

Important

For a switch that has already been configured with many settings already in place, it is a good idea to save the configuration files to a server before changing the stacking mode status. Configuration files can be saved using the CLI, SNMP manager, or Web manager interface.

Converting a standalone switch to a stacked switch

A switch that has previously acted in a standalone capacity can become a member of a stacked group simply by connecting it to a connected switch stack. For this example, let us assume switch A has been setup as a standalone device and has been functioning on the network. You want to join this switch with another Gateway managed switch, switch B, to form a 2-switch stack. Many configuration settings including IP settings have already been set on switch A so you will keep these and use them for the new stacked arrangement. Switch A is also uplinked to the backbone through the GBIC (gigabit interface converter) port. Switch A will stay in its position in the uppermost slot in the rack and all network connections will remain in place.

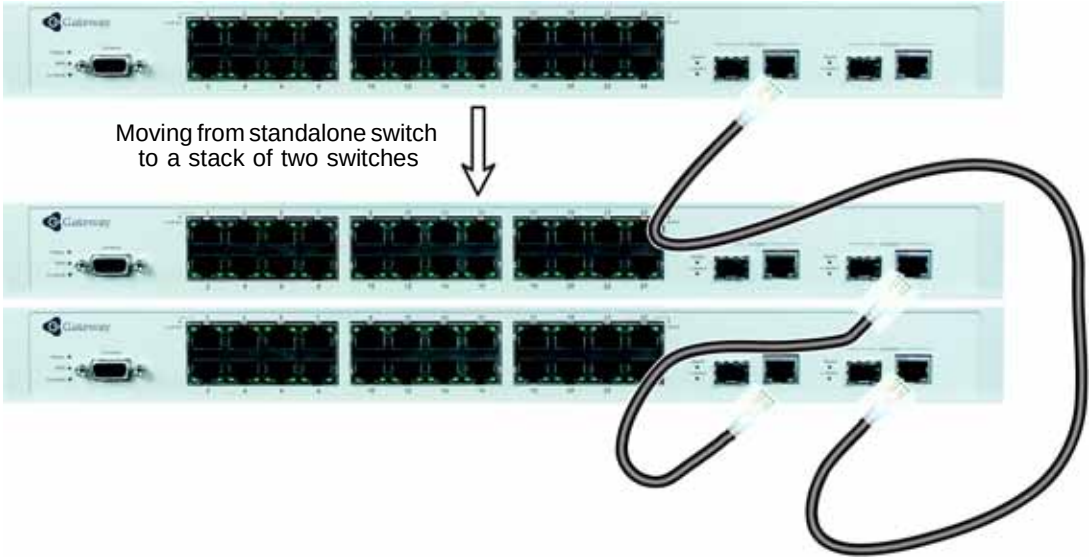
First, save the configuration files to a TFTP (Trivial File Transfer Protocol) server so they can be reloaded if any problems occur. This should be done whether or not stacking mode is changed.

Because you want to keep the same IP address and all the other settings on the standalone switch, this switch will become the master of the stack and switch B will be the slave. To make sure switch A functions as the master you will enable stacking and override the auto function.

Use the CLI to enter the command: **CONFIG STACKING MODE ENABLE MASTER**

The stacking mode for switch B is set to the default auto-stacking mode. Therefore, no changes are required. Switch B will lose configuration settings including its IP settings, so if you want to save these be sure to upload the configuration files before making the stacking connection.

Power off both devices and place switch B under switch A in the rack. It is not actually required that the slave device be placed under the master in the stack but it might be easier so that the master switch can be instantly recognized. This can prove especially convenient where multiple switch stacks are installed so it is always clear which unit should be used to uplink.

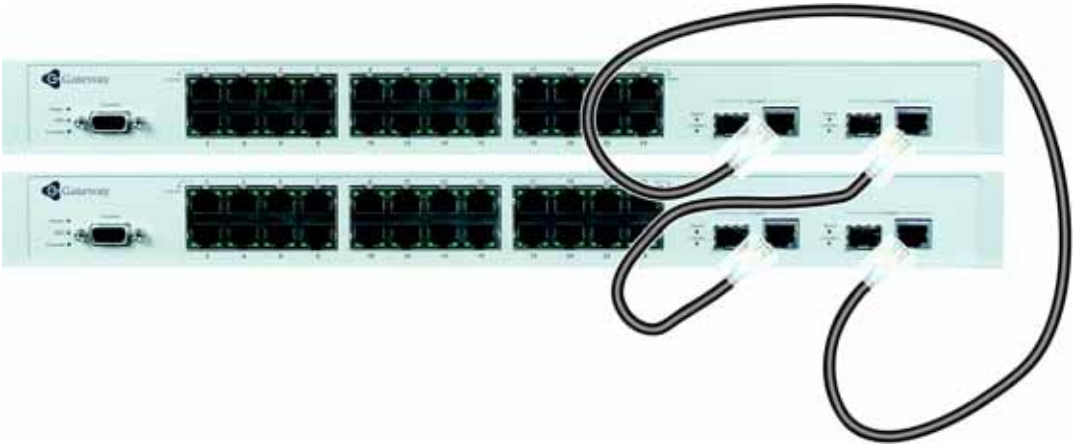


Both switches are now powered off. Switch B is placed securely in the rack and connected to switch A using the Gigabit combination ports. When both devices are powered on, they recognize the stacking connection and begin negotiating the stacking relationship. Switch A is configured to function as the master device. Switch B automatically assumes slave status. Switch A keeps its IP settings and its other configurations remain unchanged. The stack can now be configured as a single entity.

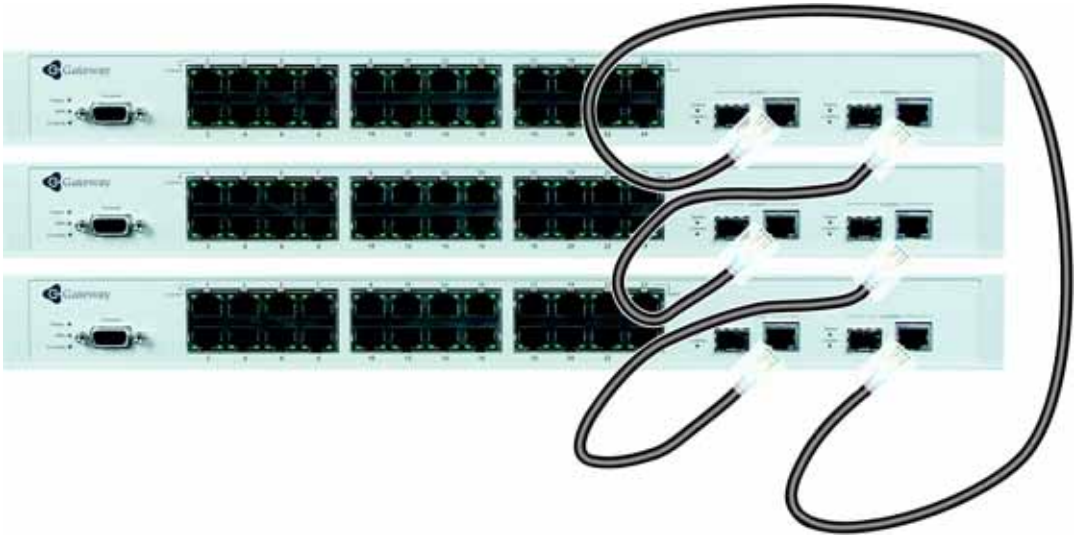
Adding a switch to a stack

Adding a new slave device to a switch stack is a simple procedure. If you are swapping an existing switch, label each Ethernet cable attached to the device being swapped so they can be placed in the same port number in the replacement device.

To add a new slave to a stack, place the new unit in the next available slot below the stack. Power off all switches in the stack and make the necessary changes to the stacking cable connections. Use the following illustrations as a guide.



Moving from a stack of two switches
to a stack of three switches



Switch C is added to the existing stack where switch A is the designated master. Power off all devices and securely place switch C in the slot beneath switch B. Adjust stacking cable connections so the Gigabit *out* port on switch B connects the Gigabit *in* port on switch C and the Gigabit *out* port of switch C connects to the Gigabit *in* port of switch A.

Power on the entire stack. The new stacking arrangement is recognized and the new relationship is negotiated. Switch A retains status as the master of the stack, switch C is in auto mode and functions as a slave. The stack is ready for operation.

Swapping a master from a stack

Assume the stack arrangement in the previous example has a problem that requires the master unit, switch A, to be replaced. In this case, you can preserve all the same configuration settings by downloading the previously saved configuration files to the replacement switch.

Before disconnecting the network connections of the original master unit, label each Ethernet cable so they can be placed in the same port number in the replacement switch. Then remove the device from the rack.

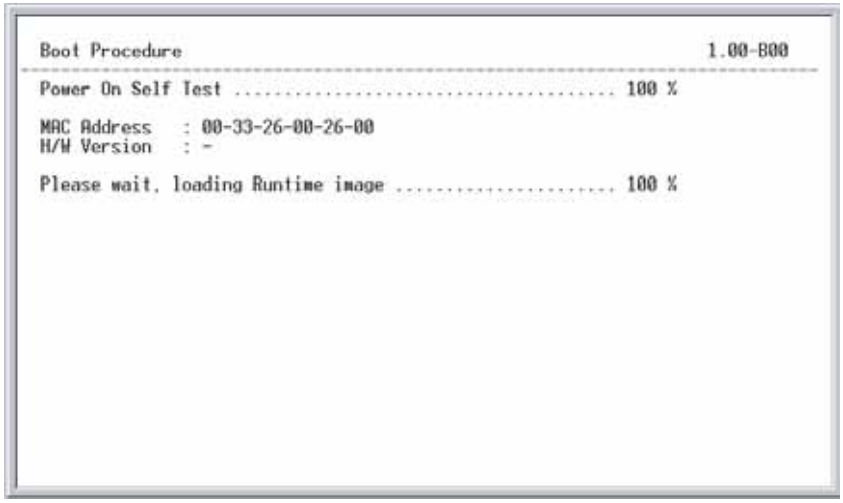
Place the replacement switch in the same slot. Power on the new switch and attach a console cable to it. Configure the new unit to be a master and save the settings. Connect the Ethernet cable needed to access the TFTP server containing the saved configuration files of the previous master unit. Download the saved configuration files using the command: **download configuration <ipaddr> <path_filename>**

Save the new settings and power off the switch. Now the stacking connections and Ethernet connections can be completed exactly as before. Reconnect the stacking cables and Ethernet connections and power on the entire stack. The stack should now function as before with all the configuration settings intact.

Switch IP address

Each switch must be assigned its own IP Address, which is used for communication with an SNMP network manager or other TCP/IP application (for example BOOTP (Bootstrap Protocol) or TFTP). The switch's default IP address is 10.90.90.90. You can change the default switch IP address to meet the specification of your networking address scheme.

The switch is also assigned a unique MAC address by the factory. This MAC address cannot be changed, and can be found from the initial boot console screen, as shown in the following illustration.



The switch's MAC address can also be found from the console program under the **Switch Information** menu item.

Setting an IP address

The IP address for the switch must be set before it can be managed with the Web-based manager. The switch IP address can be automatically set using BOOTP or DHCP (Dynamic Host Configuration Protocol) protocols, in which case the actual address assigned to the switch must be known. The IP address can alternatively be set using the CLI over the console serial port.

To set the IP address using CLI:

- Starting at the command line prompt **7601-24.2:4#**, type the command **config ipif System ipaddress XXX.XXX.XXX.XXX/YYY.YYY.YYY.YYY**. Where the Xs represent the IP address to be assigned to the IP interface named *System* and the Ys represent the corresponding subnet mask.

  -OR-

  Enter **7601-24.2:4#**, type the command **config ipif system ipaddress XXX.XXX.XXX.XXX/Z**. Where the Xs represent the IP address to be assigned to the IP interface named *System* and the Z represents the corresponding number of subnets in CIDR (Classless Inter-Domain Routing) notation.

Important

The command line prompt is based on the model number of the Gateway Managed Switch you are using.

Using this method, the switch can be assigned an IP address and subnet mask which can then be used to connect a management station to the switch's Web-based management agent.

SNMP network management

The SNMP (Simple Network Management Protocol) is an OSI (Open System Interconnection) layer 7 (the application layer) protocol for remotely monitoring and configuring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. SNMP can be used to perform many of the same functions as a directly connected console, or can be used within an integrated network management software package such as D-View.

SNMP performs the following functions:

- Sending and receiving SNMP packets using the IP protocol.
- Collecting information about the status and current configuration of network devices.
- Modifying the configuration of network devices.

The Gateway managed switch has a software program called an *agent* that processes SNMP requests, but the user program that makes the requests and collects the responses runs on a management station (a designated computer on the network). The SNMP agent and the user program both use the UDP/IP protocol to exchange packets.

SNMP Versions 1, 2, and 3

The Gateway managed switch supports SNMP versions 1, 2, and 3. The chief difference between version 3 (SNMP v.3) and versions 1 and 2 (SNMP v.1 and SNMP v.2) is that version 3 provides a substantially higher level of security than the previous versions.

In SNMP v.1 and v.2, user authentication is accomplished using *community strings*, which function like passwords. The remote user SNMP application and the router SNMP must use the same community string. SNMP packets from any station that has not been authenticated are ignored (dropped).

SNMP v.3 uses a more sophisticated authentication process that is separated into two parts. One part is to maintain a list of users and their attributes that are allowed to act as SNMP managers. The second part describes what each user on that list can do as an SNMP manager.

The switch allows groups of users to be listed and configured with a shared set of privileges. The SNMP version can also be set for a listed group of SNMP managers. Thus, you can create a group of SNMP managers that are allowed to view read-only information or receive traps using SNMP v.1 while assigning a higher level of security to another group, granting read/write privileges using SNMP v.3.

Using SNMP v.3 individual users or groups of SNMP managers can be allowed to perform or be restricted from performing specific SNMP management functions. The functions allowed or restricted are defined using the OID (Object Identifier) associated with a specific MIB (Management Information Base).

An additional layer of security is available for SNMP v.3 in that SNMP messages can be encrypted using HMAC-SHA-96 or HMAC-MDA-96 authentication levels.

Using traps

Traps are messages that alert network personnel of events that occur on the switch. The events can be as serious as a reboot (someone accidentally turned off the switch), or less serious like a port status change. The switch generates traps and sends them to the trap recipient (or network manager).

Trap recipients are special users of the network who are given certain rights and access in overseeing the maintenance of the network. Trap recipients will receive traps sent from the switch. They must immediately take certain actions to avoid future failure or breakdown of the network.

You can also specify which network managers can receive traps from the switch. This can be done by entering a list of the IP addresses of authorized network managers. You can further specify the SNMP version to use for authentication. As many as four trap recipient IP addresses, and four corresponding SNMP community strings can be entered.

The following are trap types the switch can send to a trap recipient:

- **Cold Start** - This trap signifies that the switch has been powered up and initialized such that software settings are reconfigured and hardware systems are rebooted. A cold start is different from a factory reset in that configuration settings saved to non-volatile RAM are used to reconfigure the switch.
- **Warm Start** - This trap signifies that the switch has been rebooted. However, the POST (Power On Self-Test) is skipped using this trap.
- **Authentication Failure** - This trap signifies that someone has tried to logon to the switch using an invalid SNMP community string. The switch automatically stores the source IP address of the unauthorized user.
- **Topology Change** - This trap is sent by the switch when any of its configured ports transitions from the learning state to the forwarding state, or from the forwarding state to the blocking state. The trap is not sent if a new root trap is sent for the same transition.

- **Link Change Event** - This trap is sent whenever the link of a port changes from link up to link down or from link down to link up.
- **Port Partition** - This trap is sent whenever the port state enters the partition mode (or automatic partitioning, port disable) when more than thirty-two collisions occur while transmitting at 10 Mbps or more than sixty-four collisions occur while transmitting at 100 Mbps.
- **Broadcast\Multicast Storm** - This trap is sent whenever the port reaches the threshold (in packets per second) set globally for the switch. Counters are maintained for each port, and separate counters are maintained for broadcast and multicast packets. The switch's default setting is 128 kpps for both broadcast and multicast packets.

Using MIBs

Management and counter information are stored in the switch in the MIB (Management Information Base). The switch uses the standard MIB-II Management Information Base module. Consequently, values for MIB objects can be retrieved from any SNMP-based network management software. In addition to the standard MIB-II, the switch also supports its own proprietary enterprise MIB as an extended Management Information Base. These MIBs can also be retrieved by specifying the MIB's OID (Object-Identifier) at the network manager. MIB values can be either read-only or read-write.

Read-only MIB variables can be either constants that are programmed into the switch or variables that change while the switch is in operation. Examples of read-only constants are the number of port and type of ports. Examples of read-only variables are the statistics counters such as the number of errors that have occurred, or how many kilobytes of data have been received and forwarded through a port.

Read-write MIBs are variables usually related to user-customized configurations. Examples of these are the switch's IP Address, Spanning Tree Algorithm parameters, and port status.

Forwarding and filtering

The switch enters the relationship between destination MAC or IP addresses and the Ethernet port or gateway router the destination resides on into its forwarding table. This information is then used to forward packets. This reduces the traffic congestion on the network, because packets, instead of being transmitted to all ports, are transmitted to the destination port only.

For example, if Port 1 receives a packet destined for a station on Port 2, the switch transmits that packet through Port 2 only, and transmits nothing through the other ports. This process is referred to as *learning* the network topology.

MAC address aging time

The aging time affects the learning process of the switch. Dynamic forwarding table entries, which are made up of the source MAC addresses and their associated port numbers, are deleted from the table if they are not accessed within the aging time.

The aging time can be from 10 to 1,000,000 seconds with a default value of 300 seconds. A very long aging time can result in dynamic forwarding table entries that are out-of-date or no longer exist. This can cause incorrect packet forwarding decisions by the switch.

If the aging time is too short, many entries can be aged-out too soon. This will result in a high percentage of received packets whose source addresses cannot be found in the forwarding table, in which case the switch will broadcast the packet to all ports, negating many of the benefits of having a switch.

Static forwarding entries are not affected by the aging time.

Filtering and access profile masking

The Gateway managed switch can use a form of manually configured packet filtering to segment the network and control communication between segments. It can also filter packets off the network for intrusion control. Filtering is done by setting up an access profile mask.

The access profile mask uses information contained in packet headers to determine whether the packet is forwarded or filtered (dropped). The forwarding decision is made first by examining header information, looking at the VLAN (virtual LAN) or MAC (Media Access Control) address.

Additional criteria are applied to the forwarding decision. Depending on what header information is being examined, forwarding is permitted or denied based on the packet's source or destination, its protocol classification, DiffServ code, 802.1p level, or VLAN.

Routine packet filtering

Some filtering is done automatically by the switch in the course of other routing functions. These routine functions include:

- Dynamic filtering as a function of automatic learning and aging of MAC addresses.
- The 802.1d and 802.1w Spanning Tree Protocols filter packets based on topology to prevent loops.
- Filtering done for VLAN integrity.

Some filtering requires the manual entry of information into a filtering table. *MAC address filtering* is the manual entry of specific MAC addresses to be filtered from the network. Packets sent from one manually entered MAC address can be filtered from the network. The entry can be specified as either a source, a destination, or both.

802.1w Rapid Spanning Tree

The switch implements two versions of the STP (Spanning Tree Protocol), the RSTP (Rapid Spanning Tree Protocol) as defined by the IEEE 802.1w specification and a version compatible with the IEEE 802.1d STP. RSTP can operate with legacy equipment implementing IEEE 802.1d. However, the advantages of using RSTP will be lost.

The IEEE 802.1w RSTP evolved from the 802.1d STP standard. RSTP was developed in order to overcome some limitations of STP that impede the function of some recent switching innovations, in particular, certain Layer-3 functions that are increasingly handled by Ethernet switches. The basic function and much of the terminology is the same as STP. Most of the settings configured for STP are also used for RSTP. This section introduces some new spanning tree concepts and illustrates the main differences between the two protocols.

Port transition states

An essential difference between the two protocols is in the way ports transition to a forwarding state and then in the way this transition relates to the role of the port (forwarding or not forwarding) in the topology. RSTP combines the transition states disabled, blocking, and listening used in 802.1d and creates a single state discarding. In either case, ports do not forward packets in the STP port transition states *disabled*, *blocking*, or *listening*. In the RSTP port state *discarding* there is no functional difference. The port is not active in the network topology. The following table compares how the two protocols differ regarding the port state transition.

802.1d STP	802.1w RSTP	Forwarding?	Learning?
Disabled	Discarding	No	No
Blocking	Discarding	No	No
Listening	Discarding	No	No
Learning	Learning	No	Yes
Forwarding	Forwarding	Yes	Yes

Both protocols calculate a stable topology in the same way. Every segment will have a single path to the *root bridge*. All bridges listen for BPDU (bridge protocol data unit) packets. However, BPDU packets are sent more frequently (with every Hello packet). BPDU packets are sent even if a BPDU packet was not received. Therefore, each link between bridges are sensitive to the status of the link. Ultimately this difference results in faster detection of failed links, and thus faster topology adjustment. A drawback of 802.1d is this absence of immediate feedback from adjacent bridges.

RSTP is capable of more rapid transition to a forwarding state (it no longer relies on timer configurations) RSTP compliant bridges are sensitive to feedback from other RSTP compliant bridge links. Ports do not need to wait for the topology to stabilize before transitioning to a forwarding state. In order to allow this rapid transition, the protocol introduces two new variables: the edge port and the point-to-point (P2P) port.

Edge port

The edge port is a configurable designation used for a port that is directly connected to a segment where a loop cannot be created. An example would be a port connected directly to a single workstation. Ports that are designated as edge ports transition to a forwarding state immediately without going through the listening and learning states. An edge port loses its status if it receives a BPDU packet, immediately becoming a normal spanning tree port.

P2P port

A P2P port is also capable of rapid transition. P2P ports can be used to connect to other bridges. Under RSTP, all ports operating in full-duplex mode are considered to be P2P ports, unless manually overridden through configuration.

802.1d/802.1w compatibility

RSTP can interoperate with legacy equipment and is capable of automatically adjusting BPDU packets to 802.1d format when necessary. However, any segment using 802.1 STP will not benefit from the rapid transition and rapid topology change detection of RSTP. The protocol also provides for a variable used for migration in the event that legacy equipment on a segment is updated to use RSTP.

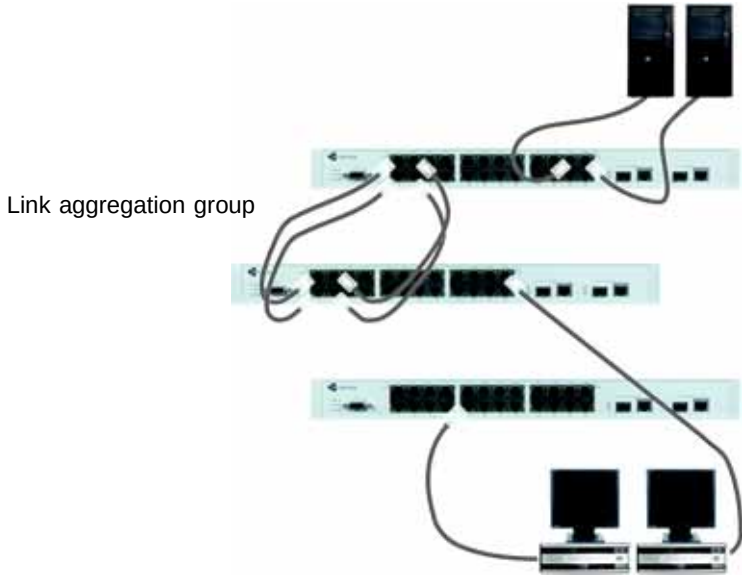
Link aggregation

Link aggregation is used to combine a number of ports together to make a single high-bandwidth data pipeline. The participating ports are called members of a link aggregation group, with one port designated as the master port of the group. Because all members of the link aggregation group must be configured to operate in the same manner, the configuration of the master port is applied to all members of the link aggregation group. Thus, when configuring the ports in a link aggregation group, you only need to configure the master port.

The Gateway managed switch supports link aggregation groups, which can include from two to eight switch ports each, except for a Gigabit link aggregation group which consists of the two Gigabit Ethernet ports of the front panel. These ports are the two 1000BASE-SX, -LX, -TX, or GBIC ports contained on the front-panel.

Static vs. LACP link aggregation

Gateway managed switch firmware supports the option of designating LACP compliant ports for link aggregation groups. IEEE 802.1ad LACP (Link Aggregation Control Protocol) is used to negotiate a dynamic aggregated link between this switch and another network device. For static aggregated links (the default port setting for link agregation is static), the linked switches must be manually configured and do not allow dynamic changes to the aggregated port group. For dynamic aggregated links (designated LACP-compliant ports), the switches must comply with LACP to allow negotiation of the aggregated link. Dynamic link aggregation can be negotiated if one port group is configured to be the *active* group while the other port group is designated as a *passive* group.



Data transmitted to a specific host (destination address) will always be transmitted over the same port in a link aggregation group. This allows packets in a data stream to arrive in the same order they were sent. An aggregated link connection can be made with any other switch that maintains host-to-host data streams over a single link aggregate port. Switches that use a load-balancing scheme that sends the packets of a host-to-host data stream over multiple link aggregation ports cannot have an aggregated connection with the Gateway managed switch.

VLANs

A VLAN (virtual LAN) is a collection of end nodes grouped by logic rather than physical location. End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are located physically on the network. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded only to members of the VLAN on which the broadcast was initiated.

VLAN implementation

The following rules are important to keep in mind when setting up VLANs on your network:

- No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLANs without a network device performing a routing function between the VLANs.
- The Gateway managed switch supports only IEEE 802.1Q VLANs. The port untagging function can be used to remove the 802.1Q tag from packet headers to maintain compatibility with devices that are tag unaware.
- The switch's default is to assign all ports to a single 802.1Q VLAN named DEFAULT_VLAN.
- The DEFAULT_VLAN has a VID = 1.
- The Gateway managed switch supports asymmetric VLANs. The member ports of VLANs can be overlapped. See "Asymmetric VLANs" on page 36.

IEEE 802.1Q VLANs

Some relevant terms:

- **Tagging** - The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging** - The act of stripping 802.1Q VLAN information out of the packet header.
- **Ingress port** - A port on a switch where packets are flowing into the switch and VLAN decisions must be made.
- **Egress port** - A port on a switch where packets are flowing out of the switch, either to another switch or to an end station, and tagging decisions must be made.

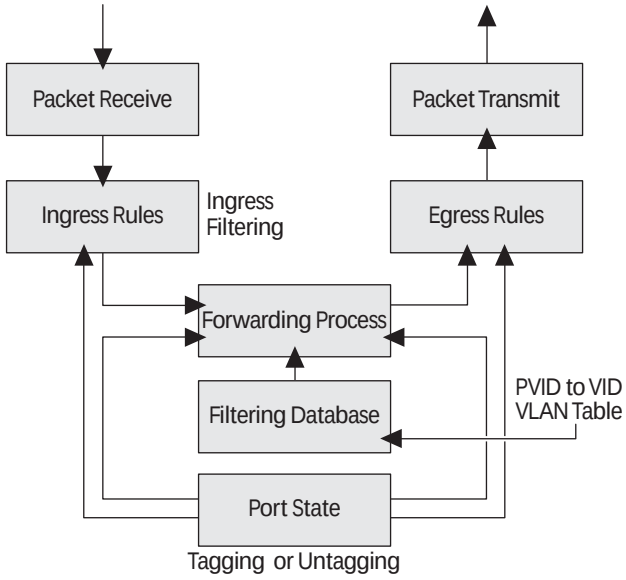
IEEE 802.1Q (tagged) VLANs are implemented on the Gateway managed switch. 802.1Q VLANs require tagging, which enables the VLANs to span an entire network (assuming all switches on the network are IEEE 802.1Q-compliant).

Any port can be configured as either tagging or untagging. The untagging feature of IEEE 802.1Q VLANs allow VLANs to work with legacy switches that don't recognize VLAN tags in packet headers. The tagging feature allows VLANs to span multiple 802.1Q VLAN compliant switches through a single physical connection and allows spanning tree to be enabled on all ports and work normally.

802.1Q VLAN packet forwarding

Packet forwarding decisions are made based on the following three types of rules:

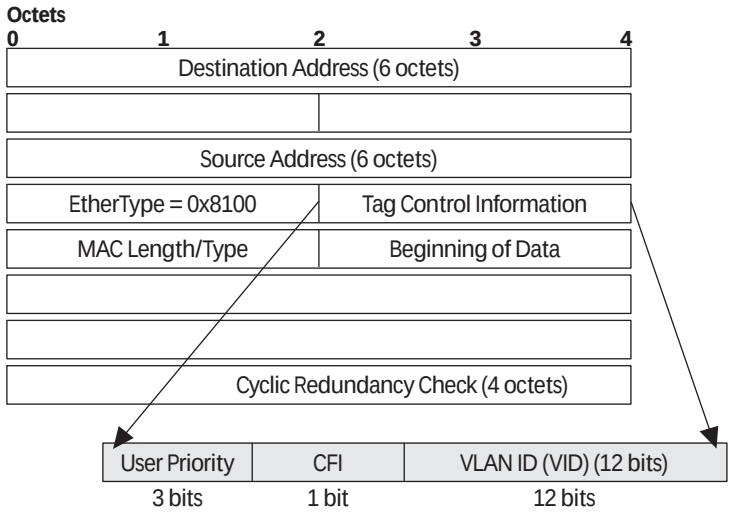
- **Ingress rules** - rules relevant to the classification of received frames belonging to a VLAN.
- **Forwarding rules between ports** - decides to filter or forward the packet.
- **Egress rules** - determines if the packet must be sent tagged or untagged.



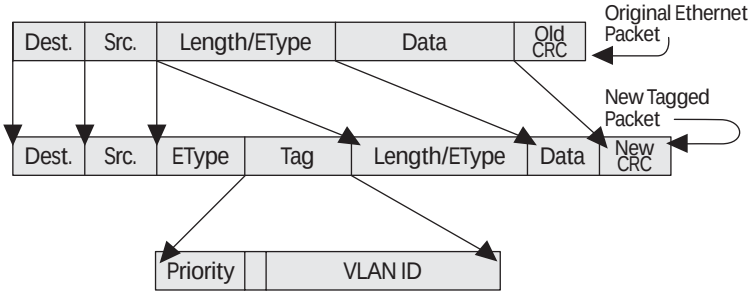
802.1Q VLAN tags

The following illustration shows the 802.1Q VLAN tag. There are four additional octets inserted after the source MAC address. Their presence is indicated by a value of 0x8100 in the EtherType field. When a packet's EtherType field is equal to 0x8100, the packet carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following two octets and consists of three bits of user priority, one bit of CFI (Canonical Format Identifier, which is used for encapsulating token ring packets so they can be carried across Ethernet backbones) and twelve bits of VID (VLAN ID). The three bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is twelve bits long, 4094 unique VLANs can be identified.

The tag is inserted into the packet header making the entire packet longer by four octets. All of the information contained in the packet originally is retained.



The EtherType and VLAN ID are inserted after the MAC source address, but before the original EtherType/Length or Logical Link Control. Because the packet is now a bit longer than it was originally, the CRC (Cyclic Redundancy Check) must be recalculated.



Port VLAN ID

Packets that are tagged (are carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with the VLAN information intact. This allows 802.1Q VLANs to span network devices (including the entire network, if all network devices are 802.1Q compliant).

Unfortunately, not all network devices are 802.1Q compliant. These devices are referred to as tag-unaware. 802.1Q devices are referred to as tag-aware.

Prior to the adoption 802.1Q VLANs, port-based and MAC-based VLANs were in common use. These VLANs relied upon a PVID (Port VLAN ID) to forward packets. A packet received on a given port would be assigned that port's PVID and then be forwarded to the port

that corresponded to the packet's destination address (found in the switch's forwarding table). If the PVID of the port that received the packet is different from the PVID of the port that is to transmit the packet, the switch will drop the packet.

Within the switch, different PVIDs mean different VLANs. (Remember that two VLANs cannot communicate without an external router.) So, VLAN identification based on the PVIDs cannot create VLANs that extend outside a given switch (or switch stack).

Every physical port on a switch has a PVID. 802.1Q ports are also assigned a PVID, for use within the switch. If no VLANs are defined on the switch, all ports are then assigned to a default VLAN with a PVID equal to 1. Untagged packets are assigned the PVID of the port on which they were received. Forwarding decisions are based on this PVID, in so far as VLANs are concerned. Tagged packets are forwarded according to the VID contained within the tag. Tagged packets are also assigned a PVID. The VID is used instead of the PVID to make packet forwarding decisions.

Tag-aware switches must keep a table to relate PVIDs within the switch to VIDs on the network. The switch will compare the VID of a packet to be transmitted to the VID of the port that is to transmit the packet. If the two VIDs are different, the switch will drop the packet. Because of the existence of the PVID for untagged packets and the VID for tagged packets, tag-aware and tag-unaware network devices can coexist on the same network.

A switch port can have only one PVID, but can have as many VIDs as the switch has memory in its VLAN table to store them.

Because some devices on a network can be tag-unaware, a decision must be made at each port on a tag-aware device before packets are transmitted. (Should the packet to be transmitted have a tag or not?) If the transmitting port is connected to a tag-unaware device, the packet should be untagged. If the transmitting port is connected to a tag-aware device, the packet should be tagged.

Tagging and untagging

Every port on an 802.1Q compliant switch can be configured as tagging or untagging.

Ports with tagging enabled will put the VID number, priority, and other VLAN information into the header of all packets that flow into and out of it. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. The VLAN information in the tag can then be used by other 802.1Q compliant devices on the network to make packet forwarding decisions.

Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into and out of those ports. If the packet does not have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

Ingress filtering

A port on a switch where packets are flowing into the switch and VLAN decisions must be made is referred to as an ingress port. If ingress filtering is enabled for a port, the switch will examine the VLAN information in the packet header (if present) and decide whether or not to forward the packet.

If the packet is tagged with VLAN information, the ingress port will first determine if the ingress port itself is a member of the tagged VLAN. If it is not, the packet will be dropped. If the ingress port is a member of the 802.1Q VLAN, the switch then determines if the destination port is a member of the 802.1Q VLAN. If it is not, the packet is dropped. If the destination port is a member of the 802.1Q VLAN, the packet is forwarded and the destination port transmits it to its attached network segment.

If the packet is not tagged with VLAN information, the ingress port will tag the packet with its own PVID as a VID (if the port is a tagging port). The switch then determines if the destination port is a member of the same VLAN (has the same VID) as the ingress port. If it does not, the packet is dropped. If it has the same VID, the packet is forwarded and the destination port transmits it on its attached network segment.

This process is referred to as ingress filtering and is used to conserve bandwidth within the switch by dropping packets that are not on the same VLAN as the ingress port at the point of reception. This eliminates the subsequent processing of packets that will just be dropped by the destination port.

Asymmetric VLANs

The Gateway managed switch supports Asymmetric VLANs implementation for more efficient use of shared resources, such as server or gateway devices. An asymmetric VLAN can be set up to allow a server (or several servers) to communicate with several clients through a single physical link on the switch. At the same time, however, the clients are not allowed to link to each other directly. For example, asymmetric VLANs can be set up so that the network e-mail server can be accessed by all e-mail clients. All e-mail clients can send and receive data packets through the port connected to the e-mail server, but they are not allowed to send and receive data to the remaining ports. The e-mail server can freely associate with all ports, that is, all clients connected to the switch.

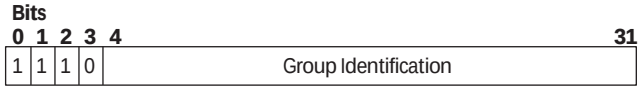
The key difference between conventional 802.1q VLAN implementation (symmetric VLANs) and asymmetric VLANs is in how address mapping is handled. Symmetric VLANs use separate address tables so there is no address sharing between VLANs. Asymmetric VLANs can use a single, shared address table. Address sharing, however, takes place in only one direction. In the example in the preceding paragraph, the VLAN created for the port connected to the e-mail server has the entire address table at its disposal so that any address can be mapped to its port (PVID).

Multicasting

Multicasting is a group of protocols and tools that enable a single source point to send packets to groups of multiple destination points with persistent connections that last for some amount of time. The main advantage to multicasting is a decrease in the network load compared to broadcasting.

Multicast groups

Class D IP addresses are assigned to a group of network devices that comprise a multicast group. The most significant four bits of a Class D address are set to *1110*. The following 28 bits is referred to as the *multicast group ID*. Some of the range of Class D addresses are registered with the IANA (Internet Assigned Numbers Authority) for special purposes. For example, the block of multicast addresses ranging from 224.0.0.1 to 224.0.0.225 is reserved for use by routing protocols and some other low-level topology discovery and maintenance protocols.



Some of the reserved IP multicast addresses are as follows:

Address	Assignment
224.0.0.0	Base Address (reserved)
224.0.0.1	All Systems on this subnet
224.0.0.2	All Routers on this subnet
224.0.0.3	Unassigned
224.0.0.4	DVMRP (Distance-Vector Multicast Routing Protocol) Routers
224.0.0.5	OSPF (Open Shortest Path First) IGP (interior gateway protocol) Routers
224.0.0.6	OSPF IGP Designated Routers
224.0.0.7	ST Routers
224.0.0.8	ST Hosts
224.0.0.9	All RIP2 (Routing Information Protocol) Routers
224.0.0.10	All IGRP Routers
224.0.0.11	Mobile Agents

Address	Assignment
224.0.0.12	DHCP (Dynamic Host Configuration Protocol) Servers and Relay Agents
224.0.0.13	All PIM (Protocol-Independent Multicast) Routers
224.0.0.14	RSVP (Resource Reservation Setup Protocol) Encapsulation
224.0.0.15	All CBT (Class-Based Threshold) Routers
224.0.0.16	Designated Sbm (Subnetwork Bandwidth Manager)
224.0.0.17	All Sbms
224.0.0.18	VRRP (Virtual Router Redundancy Protocol)
224.0.0.19 through 224.0.0.225	Unassigned
224.0.0.21	DVMRP on MOSPF (Multicast Open Shortest Path First)

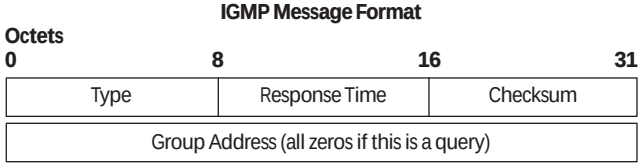
Internet Group Management Protocol (IGMP)

End users that want to receive multicast packets must be able to inform nearby routers that they want to become a multicast group member of the group these packets are being sent to. The IGMP (Internet Group Management Protocol) is used by multicast routers to maintain multicast group membership. IGMP is also used to coordinate between multiple multicast routers that can be present on a network by electing one of the multicast routers as the *querier*. This router then keeps track of the membership of multicast groups that have active members on the network. IGMP is used to determine whether the router should forward multicast packets it receives to the subnetworks it is attached to or not. A multicast router that has received a multicast packet will check to determine if there is at least one member of a multicast group that has requested to receive multicast packets from this source. If there is one member, the packet is forwarded. If there are no members, the packet is dropped.

IGMP Versions 1 and 2

Users that want to receive multicast packets need to be able to join and leave multicast groups. This is accomplished using IGMP.

IGMP Message Format



The IGMP type codes are shown in the following table:

Type	Meaning
0x11	Membership Query (if Group Address is 0.0.0.0)
0x11	Specific Group Membership Query (if Group Address is present)
0x12	Membership Report (version 1)
0x16	Membership Report (version 2)
0x17	Leave a Group (version 2)

Multicast routers use IGMP to manage multicast group memberships:

- An IGMP *report* is sent by a user's computer to join a group.
- IGMP version 1 does not have an explicit *leave* message. Group members have an expiration timer, and if this timer expires before a query response is returned, the member is dropped from the group.
- IGMP version 2 introduces an explicit *leave* report. When a user wants to leave a group, this report is sent to the multicast router (for IGMP version 2).
- Multicast routers send IGMP queries (to the all-hosts group address: 224.0.0.1) periodically to see whether any group members exist on their subnetworks. If there is no response from a particular group, the router assumes that there are no group members on the network, and multicast packets are not forwarded.

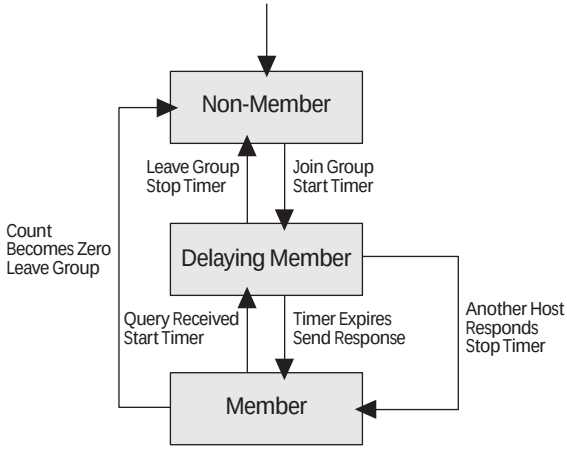
The TTL (Time to Live) field of query messages is set to 1 so that the queries do not get forwarded to other subnetworks.

IGMP version 2 introduces a few extensions to IGMP version 1, such as the election of a single multicast querier for each network, explicit *leave* reports, and queries that are specific to a particular multicast group.

The router with the lowest IP address is elected as the querier. The explicit group leave message is added to decrease latency, and routers can ask for membership reports from a particular multicast group ID.

The transition states a host will go through to join or leave a multicast group are shown in the following illustration.

IGMP State Transitions



Chapter 4

Web-Based Switch Management

- Using the interface
- Configuring the switch
- Managing the switch
- Monitoring the switch
- Maintaining the switch

Configuring the switch

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

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

Important

This Web-based management module does not accept Chinese language input (or other languages requiring 2 bytes per character).

Getting started

The first step in getting started in using Web-based management for your switch is to secure a browser. A Web browser is a program which allows a person to read hypertext, for example, Netscape Navigator or Microsoft Internet Explorer. Follow the installation instructions for your browser.

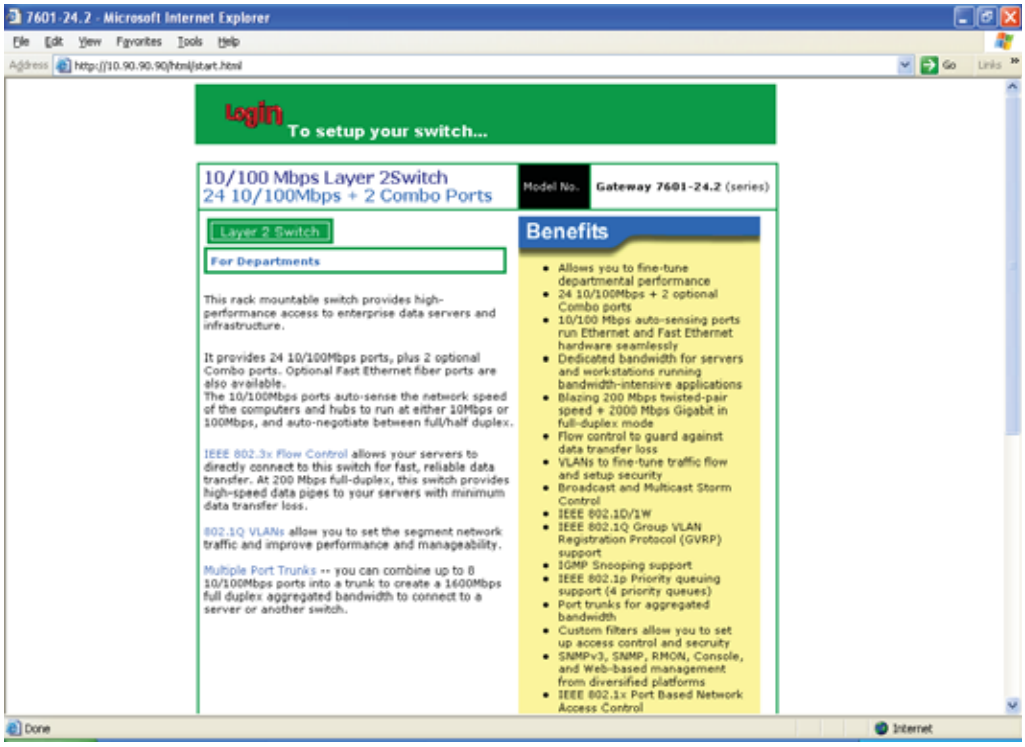
The second step is to configure an IP interface on the switch. This can be done manually using the console or automatically using BOOTP (Bootstrap Protocol) / DHCP (Dynamic Host Configuration Protocol).

To begin managing your switch, run the browser you have installed on your computer and point it to the IP address you have defined for the device. The URL in the address bar should read something like: http://123.123.123.123, where the numbers 123 represent the IP address of the switch.

Important

The factory default IP address for the switch is 10.90.90.90 with a netmask of 255.0.0.0.

On the screen that opens, click **Login**. The management module's main screen opens.



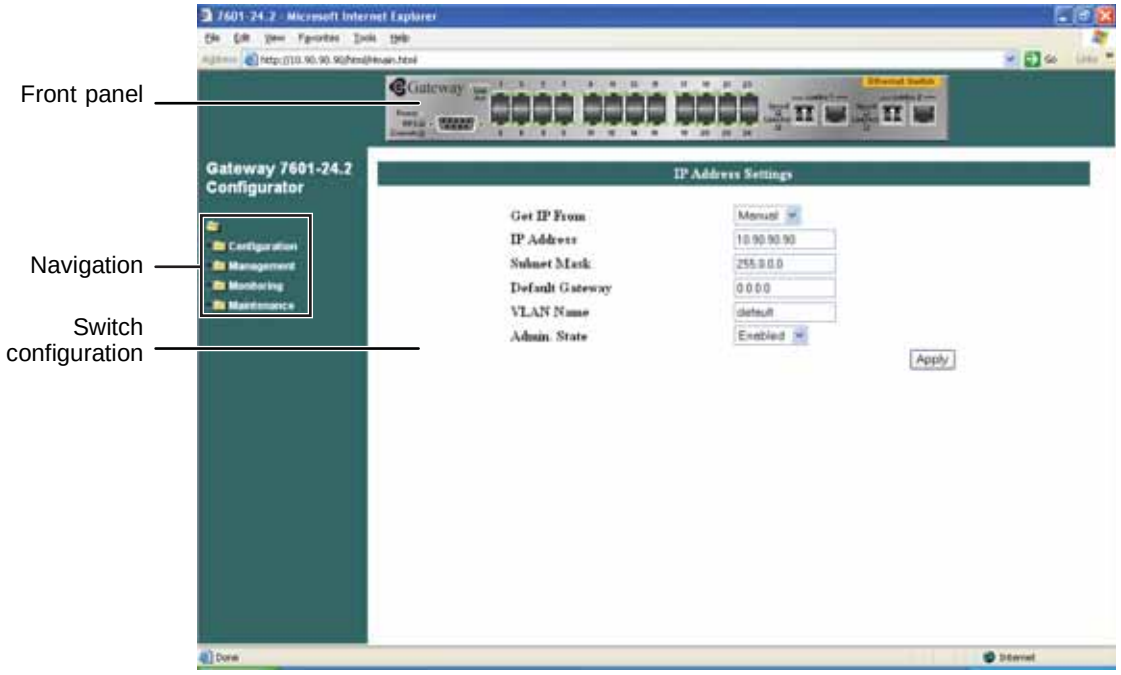
The switch management features available in the Web-based manager are explained in this chapter.

Web-based manager's user interface

The user interface provides access to various switch configuration and management screens, allows you to view performance statistics, and permits you to graphically monitor the system status.

Areas of the user interface

The following illustration shows the user interface.



The user interface is divided into three distinct areas as described in the following table.

Area	Function
Front panel	Presents a graphical near real-time image of the front panel of the switch. This area displays the switch's ports and expansion modules, showing port activity, duplex mode, or flow control, depending on the specified mode. Various areas of the illustration can be selected for performing management functions, including the ports, expansion modules, management module, or the case.
Navigation	Folders, subfolders and hyperlinks for the selection of command sets and menus.
Switch configuration	Presents switch information based on your selection and the entry of configuration data.

This section, arranged by topic, describes how to perform common monitoring and configuration tasks on the Gateway managed switch using the Web-based manager. You can perform any of the tasks described in the following sections.

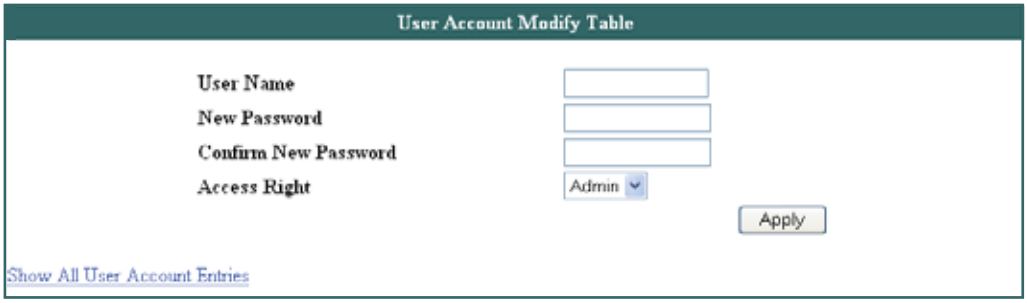
Managing user accounts

One of the first things you should do when logging onto the switch for the first time is to create a new user account.

To add a user:

1 In the left pane, click **Management**, then click **User Accounts.** The *User Account Management* screen opens.

2 Click **Add** to add a user. The *User Account Modify Table* screen opens.



3 Type the new user name in the **User Name** field.

4 Type an initial password in the **New Password** field.

5 Retype the password in the **Confirm New Password** field.

6 Click the arrow button to open the **Access Right** list, then select whether the new user should have *Admin* or *User* privileges. Some menu selections available to users with Admin privileges might not be available to those with User privileges.

The following table summarizes the Admin and User privileges:

Switch Configuration	Privilege	
Management	**Admin**	**User**
Configuration	Yes	Read Only
Network Monitoring	Yes	Read Only

Switch Configuration Management	Privilege Admin	User
Community Strings and Trap Stations	Yes	Read Only
Update Firmware and Configuration Files	Yes	No
System Utilities	Yes	Ping Only
Factory Reset	Yes	No
Reboot Switch	Yes	No
User Account Management		
Add/Update/Delete User Accounts	Yes	No
View User Accounts	Yes	No

7 Click **Apply** to make the user addition effective.

A listing of all user accounts and access levels is shown on the *User Account Management* screen. This list is updated when **Apply** is clicked.

Important

Apply makes changes to the switch configuration for the current session only. All changes (including user additions or updates) must be entered into non-volatile ram using the **Save Changes** command on the **Maintenance** menu (if you want these changes to be permanent).

8 After establishing a user account, save the changes by following the steps in "Saving changes" on page 47.

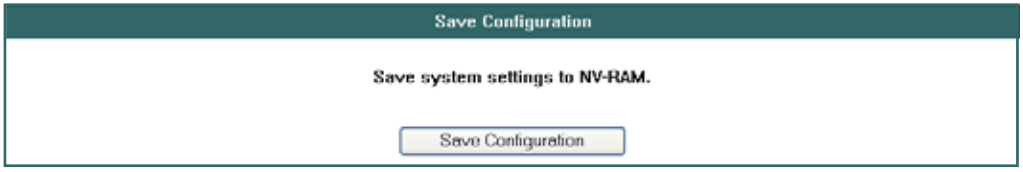
Saving changes

The Gateway managed switch has two levels of memory: normal RAM and non-volatile or NV-RAM. Configuration changes are made effective by clicking the **Apply** button. When this is done, the settings will be immediately applied to the switching software in RAM, and will immediately take effect.

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

To save changes and permanently retain configuration changes:

1. In the left pane, click **Maintenance**, then click **Save Changes**. The *Save Configuration* screen opens.



2. Click **Save Configuration** to save the current switch configuration in NV-RAM. You are notified when the changes have been saved.

3. Click **OK** to continue.

After the switch configuration settings have been saved to NV-RAM, they become the default settings for the switch. These settings will be used every time the switch is rebooted.

Resetting the switch

The factory reset function has several options when resetting the switch. Some of the current configuration parameters can be retained while resetting all other configuration parameters to their factory defaults.

Important

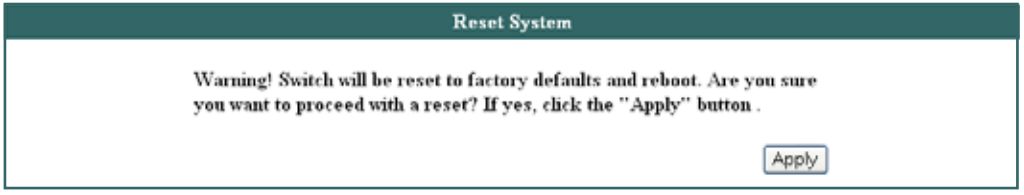
Only the *Reset System* option enters the factory default parameters into the switch's non-volatile RAM and then restarts the switch. All other options enter the factory defaults into the current configuration but do not save this configuration. *Reset System* returns the switch's configuration to the state it was when it left the factory.

To reset the switch:

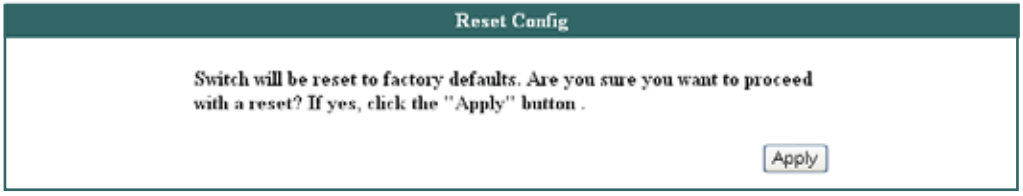
1. In the left pane, click **Maintenance**, **Reboot Services**, then click one of the following:

   - **Reset** gives the option of retaining the switch's user accounts and history log while resetting all other configuration parameters to their factory defaults. If the switch is reset with this option, and **save changes has not been executed**, the switch returns to the last saved configuration when rebooted.

   - The **Reset System** option resets all configuration parameters to their factory defaults, saves these parameters to the switch's non-volatile RAM, and then restarts the switch. This option is equivalent to *Reset Config* (see the following illustration) followed by **Save Changes**.



- The **Reset Config** option resets all configuration parameters to their factory defaults without saving these default values to the switch's non- volatile RAM. If the switch is reset with this option, and **save changes has not been executed**, the switch returns to the last saved configuration when rebooted.



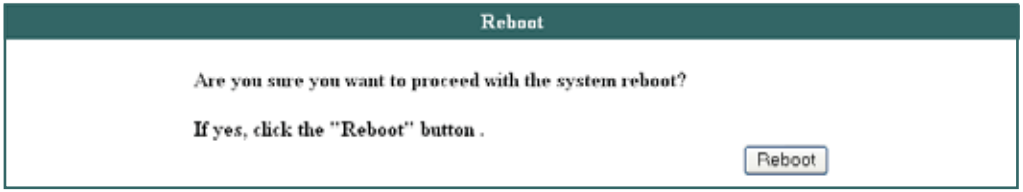
2 Click **Apply** to reset the switch. You are notified when the server is reset.

3 Click **OK** to continue.

Restarting the switch

To reboot the switch:

1 In the left pane, click **Maintenance**, **Reboot Services**, then click **Reboot**. The *Reboot* screen opens.



2 Click **Reboot** to restart the switch.

Configuring the switch

Use the screens and folders contained in the **Configuration** folder to configure the switch. The hyperlinked screens and folders contained in the **Configuration** folder include:

- *IP Address* - See "Setting the IP address" on page 51
- *Switch Information* - See "Setting and viewing basic switch information" on page 53
- *Advanced Settings* - See "Setting advanced switch information" on page 55
- *Port Configuration* - See "Configuring individual switch ports" on page 56
- *Port Mirroring* - See "Setting up port mirroring" on page 58
- *IGMP* - See "Using IGMP" on page 59
  - *IGMP Snooping* - See "Configuring IGMP snooping" on page 59
  - *Static Router Ports Entry* - See "Configuring static router port settings" on page 61
- *Spanning Tree* - See "Using Spanning Tree Protocol (STP)" on page 63
  - *STP Switch Settings* - See "Configuring Spanning Tree Protocol on the switch" on page 63
  - *STP Port Settings* - See "Configuring Spanning Tree Protocol on a port" on page 65
- *Forwarding Filtering* - See "Using forwarding filtering" on page 66
  - *Unicast Forwarding* - See "Adding or modifying unicast forwarding" on page 66
  - *Multicast Forwarding* - See "Adding or modifying multicast forwarding" on page 68
  - *Multicast Port Filtering Mode* - See "Modifying the Multicast Port Filtering Mode" on page 70
- *VLANs* - See "Creating, modifying, and deleting VLANs" on page 71
  - *Static VLAN Entry* - See "Adding or modifying a 802.1Q VLAN" on page 71
  - *Port VLAN ID (PVID)* - See "Modifying Port VLAN ID (PVID) settings" on page 73
- *Port Bandwidth* - See "Setting the port bandwidth" on page 75
- *SNTP Settings* - See "Simple Network Time Protocol (SNTP) settings" on page 76
  - *Current Time Setting* - See "Setting the current time" on page 77
  - *Time Zone and DST* - See "Setting the time zone and Daylight Savings Time" on page 78
- *Port Security* - See "Setting port security" on page 80
- *QoS* - See "Using 802.1p priority queuing (QoS)" on page 81

- *Traffic Control* - See “Managing traffic control” on page 85
- *802.1p Default Priority* - See “Assigning default priority” on page 83
- *802.1p User Priority* - See “Assigning user priority” on page 84
- *Scheduling* - See “Configuring QoS output scheduling” on page 82
- *Traffic Segmentation* - See “Managing traffic segmentation” on page 86

- *MAC Notification* - See “Using MAC notification” on page 87
  - *Global Settings* - See “Turning MAC notifications on or off globally” on page 87
  - *Port Settings* - See “Turning MAC notifications on or off on a port” on page 88
- *LACP* - See “Using Link Aggregation Control Protocol (LACP)” on page 89
  - *Link Aggregation* - See “Using link aggregation” on page 90
  - *LACP Port* - See “Enabling LACP” on page 89
- *Access Profile Table* - See “Using access profiles” on page 92
- *System Log Servers* - See “Using system log servers” on page 100
- *PAE Access Entity* - See “PAE Access Entity” on page 102
  - *Configure Authentication* - See “Configuring existing 802.1X port settings” on page 103
  - *Port Capability Settings* - See “Configuring port capability settings” on page 105
  - *Initialize Port(s)* - See “Initializing ports” on page 106
  - *Reauthenticate Port(s)* - See “Reauthenticating port(s)” on page 107
  - *Radius Server* - See “Using a RADIUS server” on page 108

Setting the IP address

The switch needs to have an IP address assigned to it so that an In-Band network management system (for example, the Web manager or Telnet) client can find it on the network. The *IP Address Settings* screen allows you to change the settings for the Ethernet interface used for in-band communication.

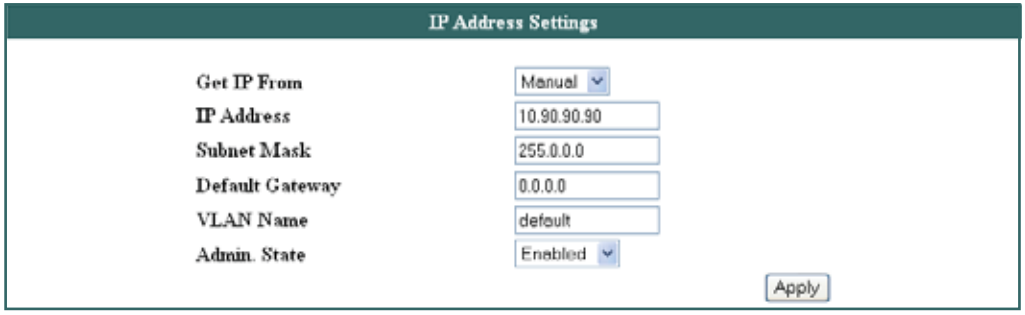
To use the BOOTP or DHCP protocols to assign the switch an IP address, subnet mask, and default gateway address. Use the **Get IP From** drop-down list to choose **Manual**, **BOOTP**, or **DHCP**. This selects how the switch is assigned an IP address on the next reboot.

Important

The factory default IP address for the switch is 10.90.90.90 with a subnet mask of 255.0.0.0 and a default gateway of 0.0.0.0.

To set the switch's IP address:

1 In the left pane, click **Configuration**, then click **IP Address**. The *IP Address Settings* screen opens.



2 Click the arrow button to open the **Get IP From** list, then select one of the following:

- **BOOTP** - The switch will send out a BOOTP broadcast request when it is powered up. The BOOTP protocol allows IP addresses, network masks, and default gateways to be assigned by a central BOOTP server. If this option is set, the switch will first look for a BOOTP server to provide it with this information before using the default or previously entered settings.
- **DHCP** - The switch will send out a DHCP broadcast request when it is powered up. The DHCP protocol allows IP addresses, network masks, and default gateways to be assigned by a DHCP server. If this option is set, the switch will first look for a DHCP server to provide it with this information before using the default or previously entered settings.
- **Manual** - Allows the entry of an IP address, Subnet Mask, and a Default Gateway for the switch. These fields should be of the form XXX.XXX.XXX.XXX, where each XXX is a number (represented in decimal form) between 0 and 255. This address should be a unique address on the network assigned for use by the network administrator. The fields which require entries under this option are: **IP Address**, **Subnet Mask**, **Default Gateway**, **VLAN Name**, and **Admin. State**.

3 If you selected **Manual** in Step 2, type the appropriate IP address in the **IP Address** field.

4 If you selected **Manual** in Step 2, type the subnet mask in the **Subnet Mask** field. This value is a bitmask that determines the extent of the subnet that the switch is on. It should be of the form XXX.XXX.XXX.XXX, where each XXX is a number (represented in decimal form) between 0 and 255. The value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network, but custom subnet masks are allowed.

5 If you selected **Manual** in Step 2, and f you want to access the switch from a different subnet from the one it is installed on, type the IP address of the gateway in the **Default Gateway** field. If you will manage the switch from the subnet on which it is installed, you can leave the default address in this field. This value is an IP address that determines where packets with a destination address outside the current subnet should be sent. This is usually the address of a router or a host acting as an IP gateway. If your network is not part of an intranet or you do not want the switch to be accessible outside your local network, you can leave this field unchanged.

6 Type the VLAN name in the **VLAN Name** field. This allows the entry of a VLAN name from which a management station (a computer) is allowed to manage the switch using TCP/IP (in-band or over the network). Management stations that are on VLANs other than the one entered in the **VLAN Name** field are not able to manage the switch in-band unless their IP addresses are entered in the **Security IP Management** table (see "Setting up a switch for remote management" on page 110). The default VLAN is named *default* and contains all of the switch's ports. There are no entries in the *Management Station IP Addresses* table, by default, so any management station can access the switch.

7 Click the arrow button to open the **Admin. State** list, then select **enabled** or **disabled**. This setting allows the IP interface named *System* to be enabled or disabled.

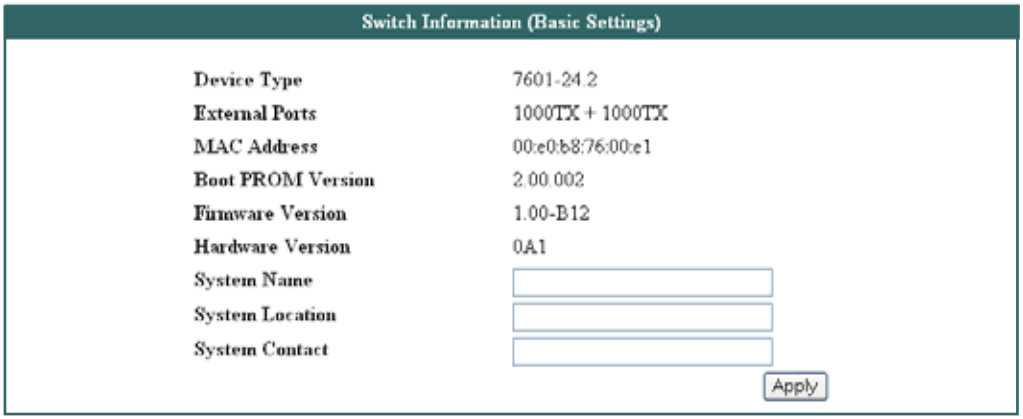
8 Click **Apply** to make the changes effective.

Setting and viewing basic switch information

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

To set and view basic switch settings:

1 In the left pane, click **Configuration**, then click **Switch Information**. The *Switch Information (Basic Settings)* screen opens.



You can view the following fields on this screen:

- **Device Type** - Shows the model number of the switch.
- **External Ports** - Shows the speed of the combination ports.
- **MAC Address** - Shows the factory-assigned MAC address of the switch.
- **Boot PROM Version** - Shows the switch's boot PROM version. You might need this information for tracking updates or troubleshooting the switch.
- **Firmware Version** - Shows the switch's firmware version. You might need this information for tracking updates or troubleshooting the switch.
- **Hardware Version** - Shows the switch's hardware version. You might need this information for tracking updates or troubleshooting the switch.

2 Type the name of the switch or network system in the **System Name** field.

3 Type the location of the switch or network system in the **System Location** field.

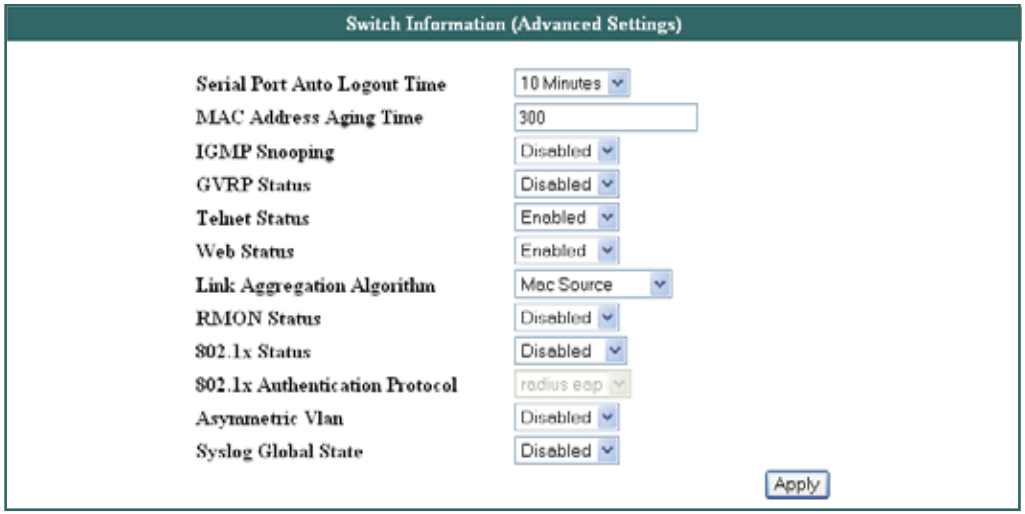
4 Type the name and telephone number of the system administrator in the **System Contact** field. Gateway recommends that the person responsible for the maintenance of the network system this switch is located on be listed here.

5 Click **Apply** to make the changes effective.

Setting advanced switch information

To set advanced switch settings:

1. In the left pane, click **Configuration**, then click **Advance Settings**. The *Switch Information (Advanced Settings)* screen opens.



2. Click the arrow button to open the **Serial Port Auto Logout Time** list, then select the amount of time for the serial port to logout. Options include 2 minutes, 5 minutes, 10 minutes, 15 minutes, or never.

3. Type the length of time a learned MAC address will remain in the forwarding table without being accessed (how long a learned MAC address is allowed to remain idle) in the **MAC Address Aging Time** field. The aging time can be set to any value between 10 and 1,000,000 seconds. For more information, see "MAC address aging time" on page 28.

4. Click the arrow button to open the **IGMP Snooping** list, then select **Enabled** to turn on IGMP (Internet Group Management Protocol) snooping globally or **Disabled** to turn off IGMP snooping globally. IGMP snooping allows the switch to read the Multicast Group IP address and the corresponding MAC address from IGMP packets that pass through the switch. For more information, see "Using IGMP" on page 59.

5. Click the arrow button to open the **GVRP Status** list, then select **Enabled** to turn on GVRP (GARP (Generic Attribute Registration Protocol) VLAN Registration Protocol) on the switch globally or **Disabled** to turn off GVRP on the switch globally. For more information, see "Modifying Port VLAN ID (PVID) settings" on page 73.

6. Click the arrow button to open the **Telnet Status** list, then select **Enabled** to allow the switch to be accessed using Telnet or select **Disabled** to not allow the switch to be accessed using Telnet.

7. Click the arrow button to open the **Web Status** list, then select **Enabled** to allow the switch to be accessed using a Web browser or select **Disabled** to not allow the switch to be accessed using a Web browser.

8. Click the arrow button to open the **Link Aggregation Algorithm** list, then select one of the following: **IP Src & Dest**, **IP Destination**, **IP Source**, **Mac Src & Dest**, **Mac Destination**, or **Mac Source**.

9. Click the arrow button to open the **RMON Status** list, then select **Enabled** to turn on RMON or select **Disabled** to turn off RMON.

10. Click the arrow button to open the **802.1x Status** list, then select one of the following: **Disabled** (disable 802.1x port access control), **Port Base**, or **Mac Base**.

11. Click the arrow button to open the **802.1x Authentication Protocol** list, then select the protocol being used.

12. Click the arrow button to open the **Asymmetric Vlan** list, then select **Enabled** to turn on Asymmetric VLAN support or select **Disabled** to turn off Asymmetric VLAN support. For more information, see "Asymmetric VLANs" on page 36.

13. Click the arrow button to open the **Syslog Global State** list, then select **Enabled** to turn on Syslog Global State or select **Disabled** to turn off Syslog Global State.

14. Click **Apply** to make the changes effective.

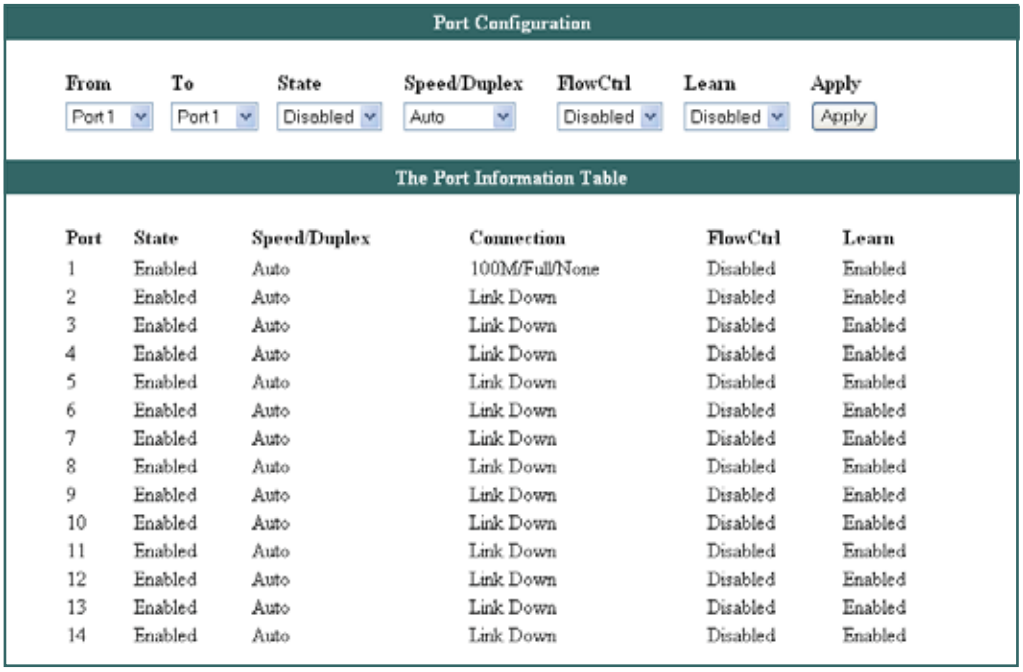
Configuring individual switch ports

Individual switch ports can be configured using the *Port Configuration* screen.

You can enable or disable the selected port and use the **Speed/Duplex** pull-down menu to select the speed and duplex/half-duplex state of the port. The **Auto** setting allows the port to automatically determine the fastest settings the port on the device connected to the switch can handle, and then use those settings. The other options for ports 1-24 or 1-48 are **100M/Full**, **100M/Half**, **10M/Full**, and **10M/Half**. For combo ports 25 and 26, or 49 and 50, the options are **1000/Full**, **100M/Full**, **100M/Half**, **10M/Full**, and **10M/Half**.

To configure individual switch ports:

1 In the left pane, click **Configuration**, then click **Port Configuration**. The *Port Configuration* screen opens.



Port Configuration

From	To	State	Speed/Duplex	FlowCtrl	Learn	Apply
Port 1	Port 1	Disabled	Auto	Disabled	Disabled	Apply

The Port Information Table

Port	State	Speed/Duplex	Connection	FlowCtrl	Learn
1	Enabled	Auto	100M/Full/None	Disabled	Enabled
2	Enabled	Auto	Link Down	Disabled	Enabled
3	Enabled	Auto	Link Down	Disabled	Enabled
4	Enabled	Auto	Link Down	Disabled	Enabled
5	Enabled	Auto	Link Down	Disabled	Enabled
6	Enabled	Auto	Link Down	Disabled	Enabled
7	Enabled	Auto	Link Down	Disabled	Enabled
8	Enabled	Auto	Link Down	Disabled	Enabled
9	Enabled	Auto	Link Down	Disabled	Enabled
10	Enabled	Auto	Link Down	Disabled	Enabled
11	Enabled	Auto	Link Down	Disabled	Enabled
12	Enabled	Auto	Link Down	Disabled	Enabled
13	Enabled	Auto	Link Down	Disabled	Enabled
14	Enabled	Auto	Link Down	Disabled	Enabled

2 Click the arrow button to open the **From** and **To** lists, then select the consecutively numbered group of ports to be configured.

3 If you are turning on the port, click the arrow button to open the **State** list, then select **Enabled**.

-OR-

If you are turning off the port, click the arrow button to open the **State** list, then select **Disabled**.

4 If you are changing the speed or duplex/half-duplex state of the port, click the arrow button to open the **Speed/Duplex** list, then select one of the following:

- **Auto** - auto-negotiation between 10 and 100 Mbps devices, full- or half-duplex. The **Auto** setting allows the port to automatically determine the fastest settings the device the port is connected to can handle, and then to use those settings. There is no automatic adjustment of port settings with any option other than **Auto**.
- **1000/Full**, **100M/Full**, **100M/Half**, **10M/Full**, or **10M/Half**.

5 Click the arrow button to open the **FlowCtrl** list, then select **Enabled** to enable flow control or **Disabled** to disable flow control.

6 Click the arrow button to open the **Learn** list, then select **Enabled** to enable learning or **Disabled** to disable learning.

7 Click **Apply** to make the changes effective.

Setting up port mirroring

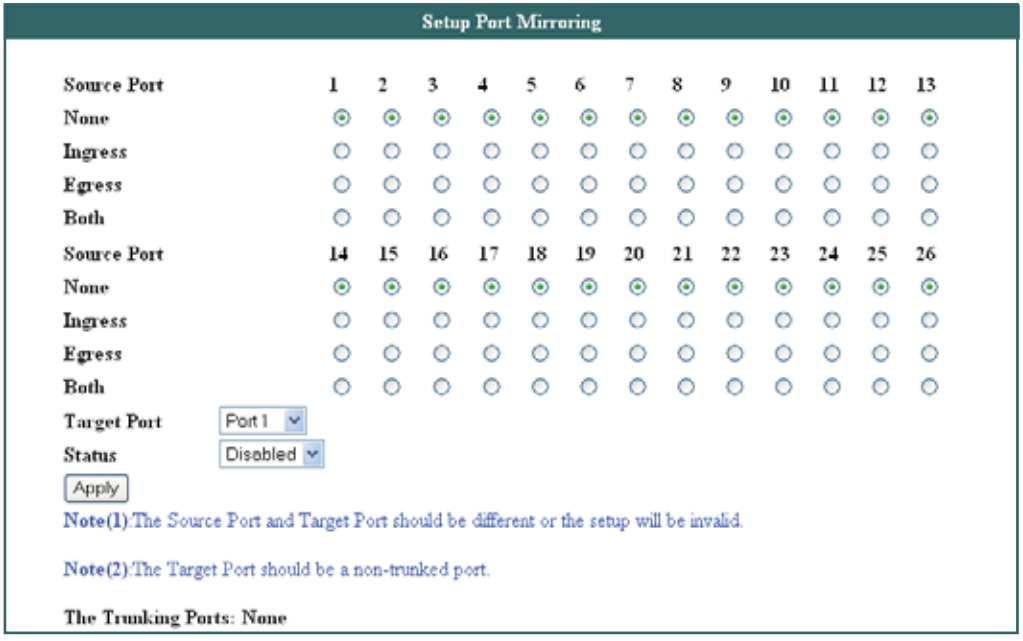
The target port is where information will be duplicated and sent for capture and network analysis. This is the port where a network analyzer would be attached to capture packets duplicated from the source port.

Caution

A faster port (a Gigabit Ethernet port, for example) should not be mirrored to a slower port (one of the 48 Fast Ethernet ports), because many packets will be dropped.

To turn on port mirroring:

1 In the left pane, click **Configuration**, then click **Port Mirroring**. The *Setup Port Mirroring* screen opens.



2 Under the **Source Port** (the source of the packets to be duplicated and forwarded to the *Target* Port), click one of the following:

- **None** - Selecting this option prevents any packets from either being received or transmitted.
- **Ingress** - Selecting this option mirrors only received packets.
- **Egress** - Selecting this option mirrors only transmitted packets.
- **Both** - Selecting this option mirrors both received and transmitted packets.

3 Click the arrow button to open the **Target Port** list, then select the port is where information will be duplicated and sent for capture and network analysis.

Important The Source Port must be different than the Target Port.

4 Click the arrow button to open the **Status** list, then select **Enabled**.

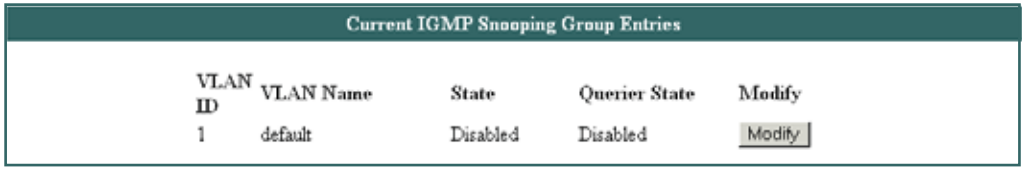
5 Click **Apply** to make the changes effective.

Using IGMP

Configuring IGMP snooping

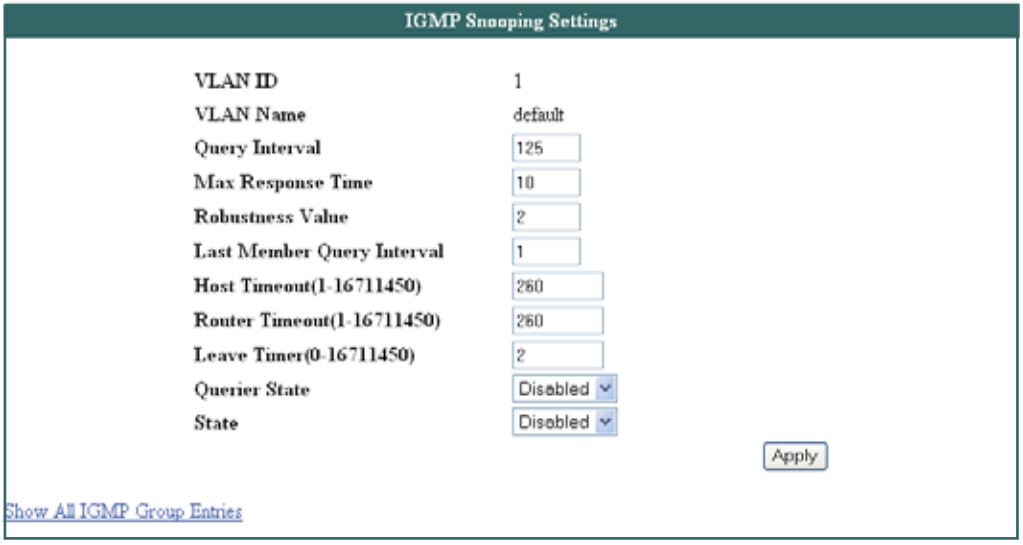
To view current IGMP snooping group entries:

- In the left pane, click **Configuration**, **IGMP**, then click **IGMP snooping**. The *Current IGMP Snooping Group Entries* screen opens.



To edit current IGMP snooping group entries:

1 In the left pane, click the button in the **Modify** column next to the VLAN entry on the *Current IGMP Snooping Group Entries* screen. The *IGMP Snooping Settings* screen opens.



You can view the following fields on this screen:

- **VLAN ID** - Shows the entry of the VLAN ID for which IGMP Snooping is to be configured.
- **VLAN Name** - Shows the entry of the name of the VLAN for which IGMP Snooping is to be configured.

2 Type the length of time between sending IGMP queries in the **Query Interval** field. Type a value between 1 and 65535 seconds. The default value is 125 seconds.

3 Type the maximum amount of time allowed before sending an IGMP response report in the **Max Response Time** field. Type a value between 1 and 25 seconds. The default value is 10 seconds.

4 Type a tuning variable that allows for VLANs that are expected to lose a large number of packets in the **Robustness Value** field. Type a value between 1 and 255 with larger values being specified for VLANs that are expected to lose larger numbers of packets. The default value is 2.

5 Type the maximum amount of time between group-specific query messages, including those sent in response to leave group messages in the **Last Member Query Interval** field. The default is 1 second.

6 Type the maximum amount of time a host can be a member of a multicast group without the switch receiving a host membership report in the **Host Timeout** field. The default is 260 seconds.

7 Type the maximum amount of time a router will remain in the switch's forwarding table without receiving a membership report in the **Router Timeout** field. The default is 260 seconds.

8 Type the maximum amount of time between the switch receiving a leave group message from a host and the switch issuing a group membership query in the **Leave Timer** field. If the switch does not receive a response from the group membership query before the Leave Timer expires, the forwarding table entry for the multicast address is deleted from the switch's forwarding table. The default is 2 seconds.

9 Click the arrow button to open the **Querier State** list, then select **Enabled** or **Disabled**.

10 Click the arrow button to open the **State** list, then select **Enabled** or **Disabled** to enable or disable IGMP Snooping for the specified VLAN.

11 Click **Apply** to make the changes effective.

Configuring static router port settings

A static router port is a port that has a multicast router attached to it. Generally, this router would have a connection to a WAN or to the Internet. Establishing a router port will allow multicast packets coming from the router to be propagated through the network, as well as allowing multicast messages (IGMP) coming from the network to be propagated to the router.

A router port has the following behavior:

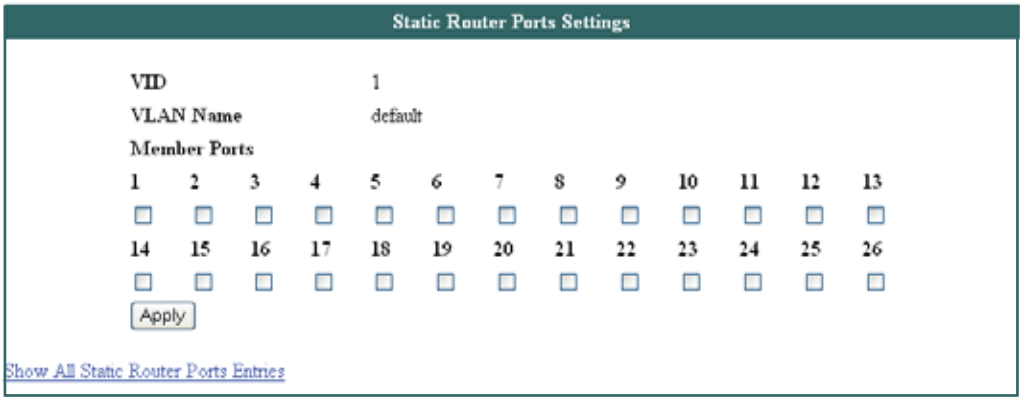
- All IGMP Report packets will be forwarded to the router port.
- IGMP queries (from the router port) will be flooded to all ports.
- All UDP multicast packets will be forwarded to the router port. Because routers do not send IGMP reports or implement IGMP snooping, a multicast router connected to the router port of the Layer 2 switch would not be able to receive UDP data streams unless the UDP multicast packets were all forwarded to the router port.

To view current static router port settings:

- In the left pane, click **Configuration**, **IGMP**, then click **Static Router Port Settings**. The *Current Static Router Ports Entries* screen opens.

To edit current static router port settings:

1. To edit an static entry on the switch, click the button in the **Modify** column next to to the VLAN entry on the *Current Static Router Ports Entries* screen. The *Static Router Ports Settings* screen opens.



You can view the following fields on this screen:

- **VLAN ID** - Displays the entry of the VLAN ID the static router port belongs to.
- **VLAN Name** - Displays the name of the VLAN the static router port belongs to.

2. Click to select a check box under the **Member Port** that is a static router port.
3. Click **Apply** to make the changes effective.

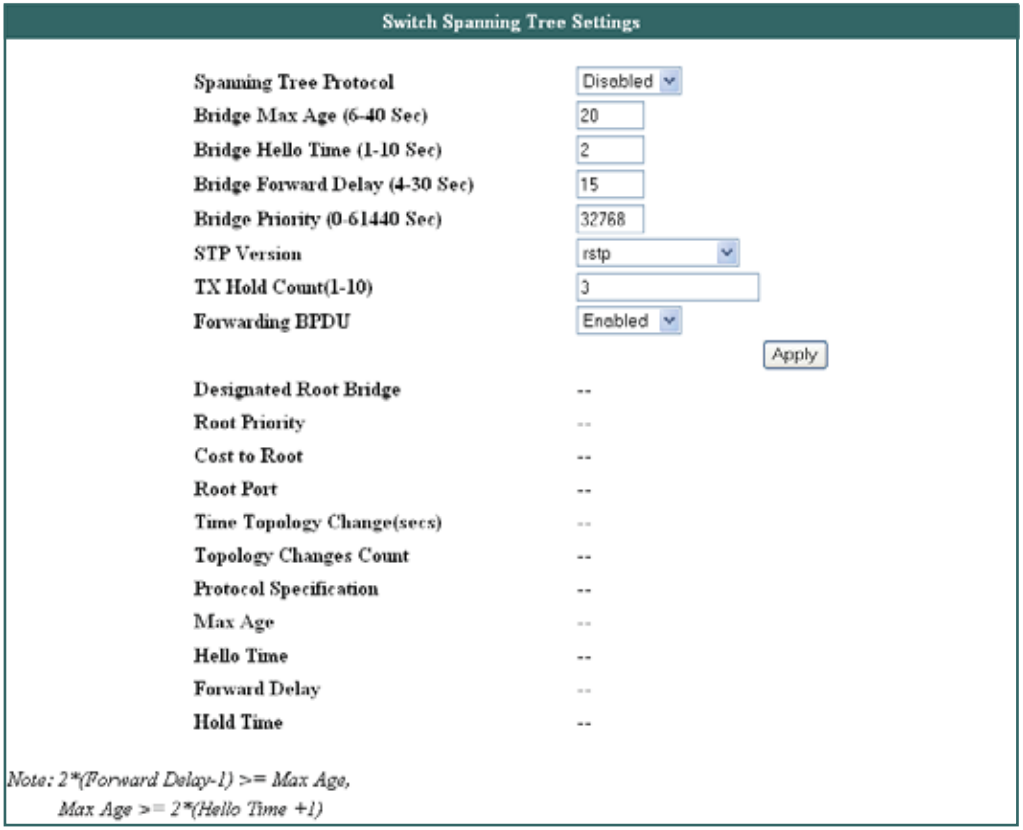
Using Spanning Tree Protocol (STP)

STP (Spanning Tree Protocol) operates on two levels: on the switch level, the settings are globally implemented. On the port level, the settings are implemented on a user-defined group of ports basis. For more information about the Spanning Tree Protocol, see "802.1w Rapid Spanning Tree" on page 29.

Configuring Spanning Tree Protocol on the switch

To configure Spanning Tree Protocol on the switch level:

1. In the left pane, click **Configuration**, **Spanning Tree**, then click **STP Switch Settings**. The *Switch Spanning Tree Settings* screen opens.



Important

The factory default setting should cover the majority of installations. It is advisable to keep the default settings as set at the factory unless it is absolutely necessary to change them.

2 Click the arrow button to open the **Spanning Tree Protocol** list, then select **Enabled** or **Disabled**. This will enable or disable the Spanning Tree Protocol (STP), globally, for the switch.

3 At the end of the Bridge Max. Age, if a BPDU has still not been received from the root bridge, your switch will start sending its own BPDU to all other switches for permission to become the root bridge. If it turns out that your switch has the lowest Bridge Identifier, it will become the root bridge. Type a value between 6 to 40 seconds in the **Bridge Max Age (6-40 Sec)** field. The default value is 20 seconds.

4 Type the interval between two transmissions of BPDU packets sent by the root bridge to tell all other switches that it is indeed the root bridge in the **Bridge Hello Time (1-10 Sec)** field. Type a value between 1 to 10 seconds. The default value is 2 seconds.

Important

The Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur.

Observe the following formulas when setting the above parameters:

Max. Age <= 2 x (Forward Delay - 1 second)

Max. Age >=2 x (Hello Time + 1 second)

5 Type the time any port on the switch spends in the listening state while moving from the blocking state to the forwarding state in the **Bridge Forward Delay (4-30 sec)** field. Type a value between 4 to 30 seconds. The default value is 15 seconds.

6 The value in the **Bridge Priority (0- 65535 Sec)** field is used in the voting process between switches on the network to determine which switch will be the root switch. A low number indicates a high priority, and a high probability that this switch will be elected as the root switch. Type a value between 0 to 65535. The default value is 32768.

7 Type the maximum number of Hello packets transmitted per interval in the **TX Hold Count(1-10)** field. Type a value between 1 to 10. The default value is 3.

8 Click the arrow button to open the **STP Version** list, then select **RSTP** or **STP Compatibility**. RSTP is fully compatible with IEEE 802.1d. STP and will function with legacy equipment.

9 Click the arrow button to open the **Forwarding BPDU** list, then select **Enabled** or **Disabled**. This allows you to control whether or not to forward Bridge Protocol Data Units. Disabling this setting can be useful if, for example, the present switch has been designated as the root bridge and you do not want that status to change.

10 Click **Apply** to make the changes effective.

Configuring Spanning Tree Protocol on a port

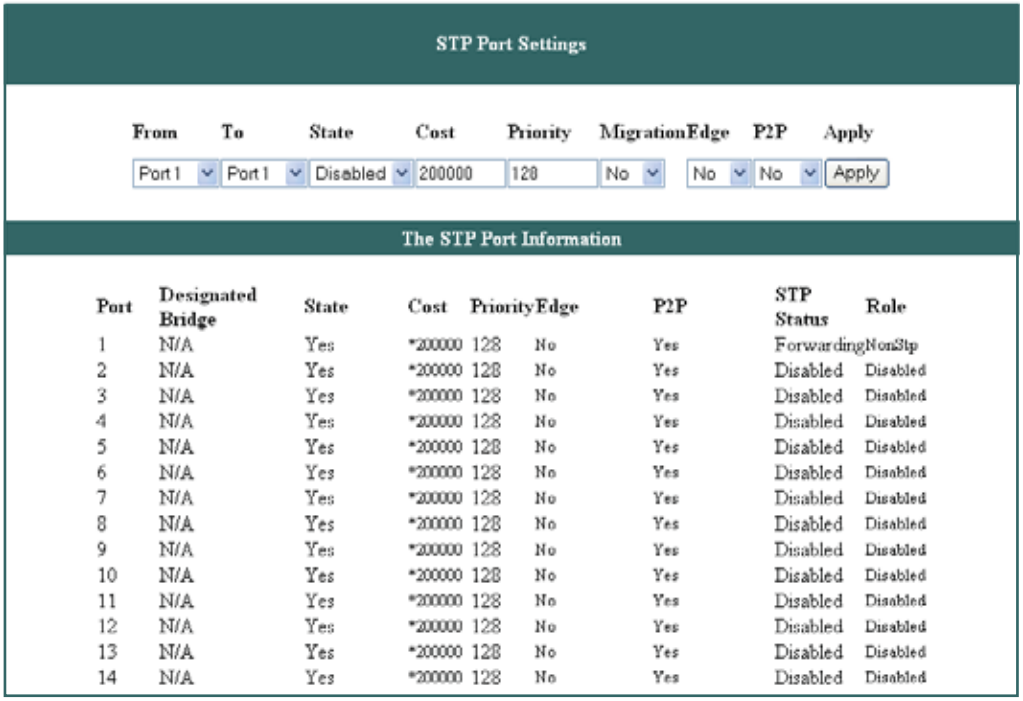
In addition to setting Spanning Tree parameters for use on the switch level, the switch allows for the configuration of a group of ports. This STP Group will use the switch-level parameters entered above, with the addition of Port Priority and Port Cost.

The STP Group spanning tree works in the same way as the switch-level spanning tree, but the root bridge concept is replaced with a root port concept. A root port (a port of the group that is elected on the basis of port priority and port cost) is to be the connection to the network for the group. Redundant links will be blocked, just as redundant links are blocked on the switch level.

The STP on the switch level blocks redundant links between switches (and similar network devices). The port level STP will block redundant links within the STP Group.

To configure Spanning Tree Protocol on the port level:

1. In the left pane, click **Configuration**, **Spanning Tree**, then click **STP Port Settings**. The *Switch Spanning Tree Settings* screen opens.



2. Click the arrow button to open the **From** and **To** lists, then select the consecutively numbered group of ports that will make up the STP Group.

3. Click the arrow button to open the **State** list, then select **Enabled** or **Disabled**. Enabled turns on STP on the selected ports.

4. Type a value between 1 and 200000 in the **Cost** field. The default value is 200000. The lower the Port Cost number, the greater the probability the port will be chosen to forward packets.

5. Type a value between 0 and 240 in the **Priority** field. The default value is 128. The lower the Port Priority number, the greater the probability the port will be chosen as the Root Port.

6. Click the arrow button to open the **Migration** list, then select **Yes** or **No**. Choosing **Yes** will enable the port to migrate from 802.1d STP status to 802.1w RSTP status. RSTP can coexist with standard STP. However, the benefits of RSTP are not realized on a port where an 802.1d network connects to an 802.1w enabled network. Migration should be enabled (**Yes**) on ports connected to network stations or segments that will be upgraded to 802.1w RSTP on all or some portion of the segment.

7. Click the arrow button to open the **Edge** list, then select **Yes** or **No**. Choosing **Yes** designates the port as an edge port. Edge ports cannot create loops. However, an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU (bridge protocol data unit) packets. If a BPDU packet is received, it automatically loses edge port status. **No** indicates the port does not have edge port status.

8. Click the arrow button to open the **P2P** list, then select **Yes** or **No**. Choosing **Yes** indicates a point-to-point (p2p) shared link. These are similar to edge ports. However, they are restricted in that a p2p port must operate in full-duplex. Like edge ports, p2p ports transition to a forwarding state rapidly thus benefiting from RSTP.

9. Click **Apply** to make the changes effective.

Using forwarding filtering

Adding or modifying unicast forwarding

Unicast MAC addresses can be statically entered into the switch's MAC Address Forwarding Table. These addresses will never age out.

To add or modify a unicast MAC address into the switch's forwarding table:

1 In the left pane, click **Configuration**, **Forwarding Filtering**, then click **Unicast Forwarding**. The *Setup Static Unicast Forwarding Table* screen opens.

2 Type the VLAN ID of the VLAN the *MAC address* is a member of in the **VLAN ID** field. This field displays the VLAN ID the currently selected MAC address is a member of when modifying an existing entry.

3 Type the MAC address of an end station that will be entered into the switch's static forwarding table when adding a new entry in the **MAC Address** field. This field displays the currently selected MAC address when modifying an existing entry.

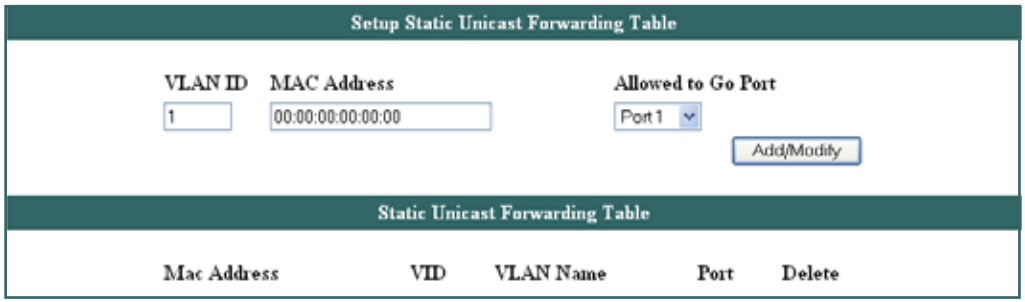
4 Click the arrow button to open the **Allowed to Go Port** list, then select the port number on which the MAC address entered above resides.

5 Click **Add/Modify** to add or modify the unicast MAC address.

Deleting unicast forwarding

To delete a unicast MAC address from the switch's forwarding table:

1 In the left pane, click **Configuration**, **Forwarding Filtering**, then click **Unicast Forwarding**. The *Setup Static Unicast Forwarding Table* screen opens.



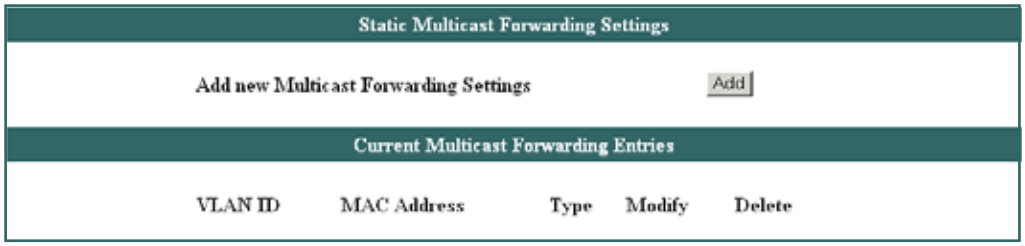
2 Click the button in the **delete** column next to the VLAN entry you want to delete.

Adding or modifying multicast forwarding

Multicast MAC addresses can be statically entered into the switch's MAC Address Forwarding Table. These addresses will never age out.

To add or modify a multicast MAC address into the switch's forwarding table:

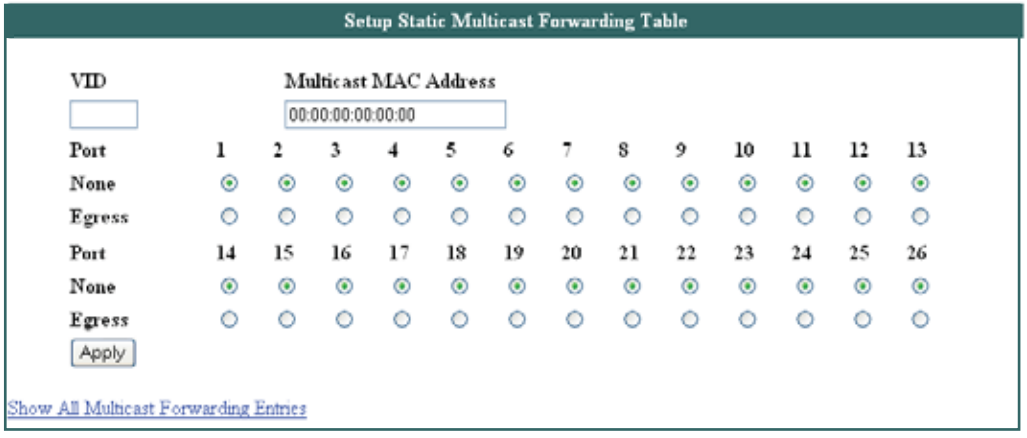
1 In the left pane, click **Configuration**, **Forwarding Filtering**, then click **Multicast Forwarding**. The *Static Multicast Forwarding Settings* screen opens.



2 To add a new multicast MAC address to the switches forwarding table, click **Add**. The *Setup Static Multicast Forwarding Table* screen opens.

-OR-

To modify an existing multicast MAC address, click the button in the **Modify** column next to next to the VLAN entry you want to modify. The *Setup Static Multicast Forwarding Table* screen opens.



3 Type the VLAN ID of the VLAN the *MAC address* is a member of in the **VID** field.

4 Type the multicast MAC address of an end station that will be entered into the switch's static forwarding table in the **Multicast MAC Address** field.

5 Click to select **None** or **Egress** under the **Port** number on which the MAC address entered above resides.

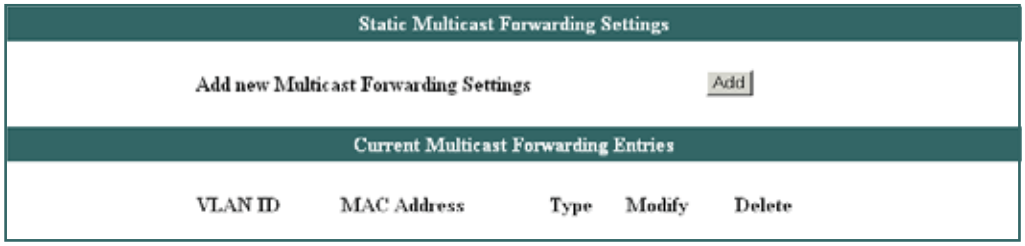
- **None** - Specifies the port as having no forwarding filtering.
- **Egress** - Specifies the port as being a source of multicast packets originating from the MAC address specified above.

6 Click **Apply** to make the changes effective.

Deleting multicast forwarding

To delete a multicast MAC address from the switch's forwarding table:

1 In the left pane, click **Configuration**, **Forwarding Filtering**, then click **Multicast Forwarding**. The *Static Multicast Forwarding Settings* screen opens.



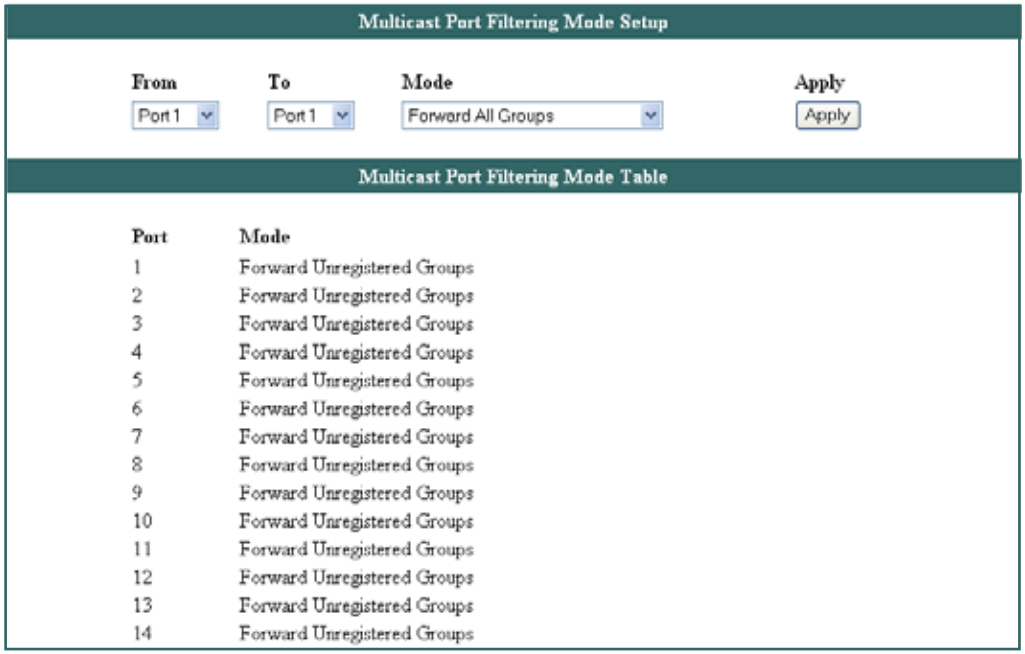
2 Click the button in the **Delete** column next to the VLAN entry you want to delete.

Modifying the Multicast Port Filtering Mode

This screen configures the multicast filtering and forwarding for specified ports.

To modify the multicast port filtering mode:

1 In the left pane, click **Configuration**, **Forwarding Filtering**, then click **Multicast Port Filtering Mode**. The *Multicast Port Filtering Mode Setup* screen opens.



2 Click the arrow button to open the **From** and **To** lists, then select the consecutively numbered group of ports that will have the multicast port filtering mode modified.

3 Click the arrow button to open the **Mode** list, then select one of the following:

- **Forward All Groups** - Forward all multicast packets. No filtering takes places because multicast packets from unregistered and registered multicast groups are forwarded in the specified port group.
- **Forward Unregistered Groups** - Forward only multicast packets from unregistered multicast groups. Multicast packets from registered groups are dropped.
- **Filter Unregistered Groups** - Filter all multicast packets from unregistered multicast groups. Multicast packets from registered groups are forwarded.

4 Click **Apply** to make the changes effective.

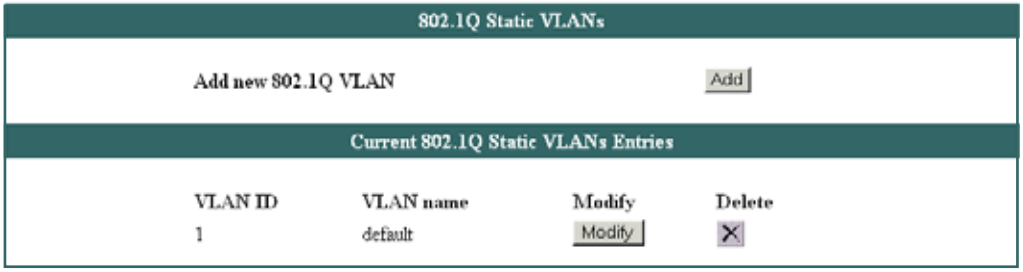
Creating, modifying, and deleting VLANs

The VLAN menu adds an entry to edit the VLAN definitions and to configure the port settings for IEEE 802.1Q VLAN support.

Adding or modifying a 802.1Q VLAN

To add a new 802.1Q VLAN or modify an existing 802.1Q VLAN:

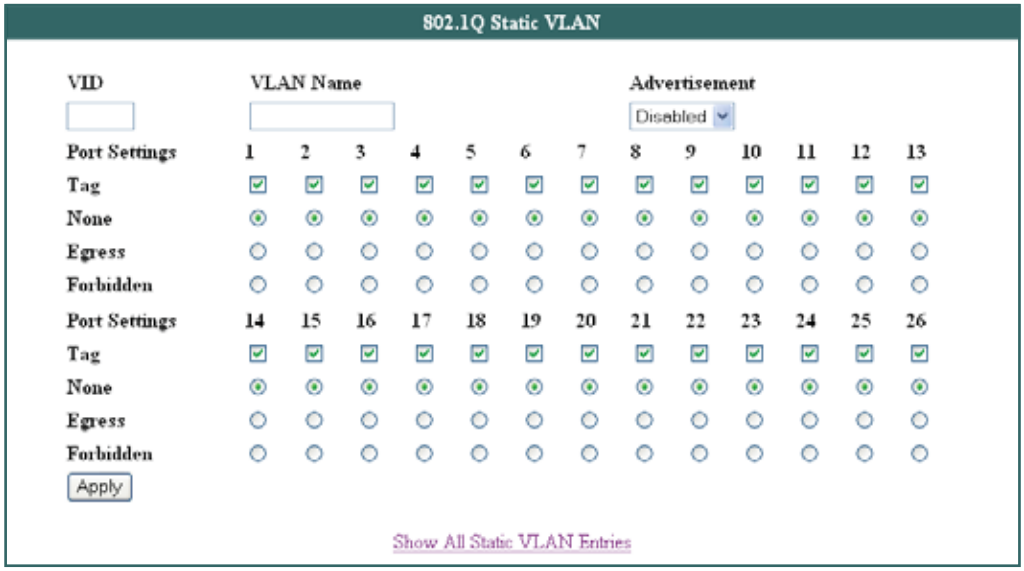
1 In the left pane, click **Configuration**, **VLANs**, then click **Static VLAN Entry**. The *802.1Q Static VLANs* screen opens.



2 To add a new 802.1Q VLAN, click **Add**. The *802.1Q Static VLAN* screen opens.

-OR-

To modify an existing 802.1Q VLAN, click the button in the **Modify** column next to the VLAN entry you want to modify. The *802.1Q Static VLAN* screen opens.



3 Type a VLAN ID in the **VLAN ID (VID)** field on the *Add* screen. This field displays the VLAN ID of an existing VLAN in the *Modify* screen. VLANs can be identified by either the VID or the VLAN name.

4 Type a name for the new VLAN in the **VLAN Name** field on the *Add* screen. You can edit the VLAN name in the *Modify* screen.

5 Click the arrow button to open the **Advertisement** list, then select **Enabled** or **Disabled** advertising. Advertising allows members to join this VLAN through GVRP.

6 Click to select the options under the **Port** number of the VLAN. Options include:

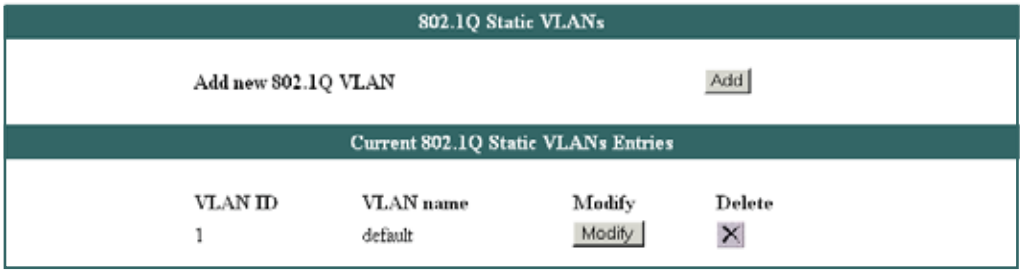
- **Tagged** - Allows an individual port to be specified as Tagging. A check in the Tagged field specifies the port as a Tagging member of the VLAN. When an untagged packet is transmitted by the port, the packet header is changed to include the 32-bit tag associated with the VID (VLAN Identifier). When a tagged packet exits the port, the packet header is unchanged. For more information about VLAN identifiers, see "Modifying Port VLAN ID (PVID) settings" on page 73.
- **None** - Allows an individual port to be specified as None. When an untagged packet is transmitted by the port, the packet header remains unchanged. When a tagged packet exits the port, the tag is stripped and the packet is changed to an untagged packet.
- **Egress** - specifies the port as being a static member of the VLAN. Egress Member Ports are ports that will be transmitting traffic for the VLAN. These ports can be either tagged or untagged.
- **Forbidden** - specifies the port as not being a member of the VLAN and the port is forbidden from becoming a member of the VLAN dynamically.

7 Click **Apply** to make the changes effective.

Deleting a 802.1Q VLAN

To delete an existing 802.1Q VLAN:

1 In the left pane, click **Configuration**, **VLANs**, then click **Static VLAN Entry**. The *802.1Q Static VLANs* screen opens.



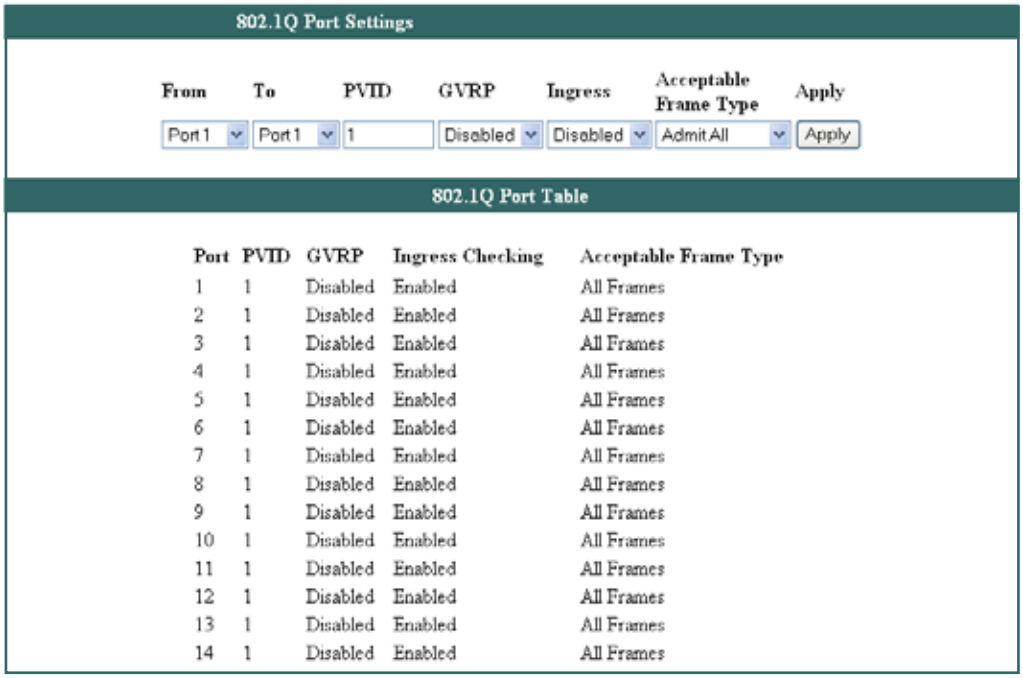
2 Click the button in the **Delete** column next to the VLAN entry you want to delete.

Modifying Port VLAN ID (PVID) settings

The 802.1Q Port Settings screen allows you to determine whether the switch will share its VLAN configuration information with other GVRP-enabled switches. In addition, Ingress can be used to limit traffic by filtering incoming packets whose PVID does not match the PVID of the port.

To enable or disable GVRP on the switch:

1 In the left pane, click **Configuration**, **VLANs**, then click **Port VLAN ID (PVID)**. The *802.1Q Port Settings* screen opens.



2 Click the arrow button to open the **From** and **To** lists, then select the consecutively numbered group of ports that will have GVRP enabled or disabled.

3 Type the Port VLAN Identifier in the **PVID** field. A Port VLAN Identifier is a classification mechanism that associates a port with a specific VLAN and is used to make forwarding decisions for untagged packets received by the port. For example, if port #2 is assigned a PVID of 3, then all untagged packets received on port #2 will be assigned to VLAN 3. This number is generally the same as the VID number assigned to the port in the Modify 802.1Q VLANs menu (see "Adding or modifying a 802.1Q VLAN" on page 71).

4 Click the arrow button to open the **GVRP** list, then select **Enabled** or **Disabled**. The Group VLAN Registration Protocol (GVRP) enables the port to dynamically become a member of a VLAN.

5 Click the arrow button to open the **Ingress** list, then select **Enabled** or **Disabled**. Enables the port to compare the VID tag of an incoming packet with the PVID number assigned to the port. If the two are different, the port filters (drops) the packet.

6 Click the arrow button to open the **Acceptable Frame Type** list, then select **Admit all** or **Tagged only**.

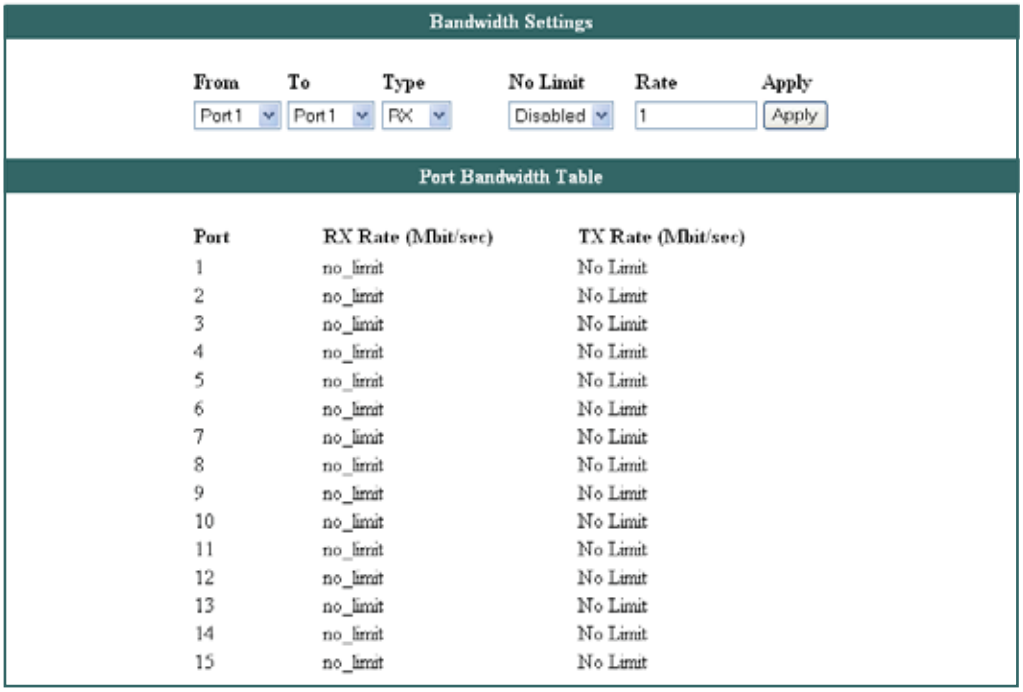
7 Click **Apply** to make the changes effective.

Setting the port bandwidth

The *Bandwidth Settings* screen allows you to set and display the ingress bandwidth and egress bandwidth of specified ports on the switch.

To set the bandwidth of a port:

1 In the left pane, click **Configuration**, then click **Port Bandwidth**. The *Bandwidth Settings* screen opens.



2 Click the arrow button to open the **From** and **To** lists, then select the consecutively numbered group of ports you want to set the bandwidth on.

3 Click the arrow button to open the **Type** list, then select the type of packets being received and/or transmitted by the switch.

4 Click the arrow button to open the **No Limit** list, then select **Enabled** or **Disabled**. If **No Limit** is set to **Enabled**, the switch will not permit you to set the bandwidth rate manually.

5 If **No Limit** is **Disabled,** type the bandwidth rate in MBit/sec in the **Rate** field.

6 Click **Apply** to make the changes effective.

Simple Network Time Protocol (SNTP) settings

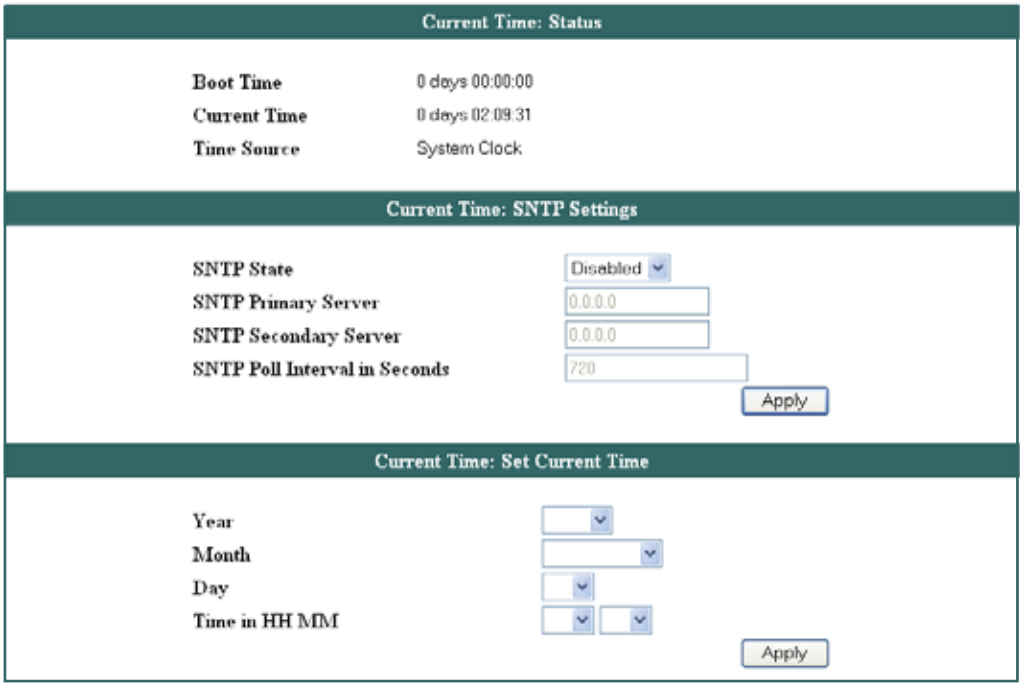
Your switch supports SNTP (Simple Network Time Protocol), an adaptation of the NPT (Network Time Protocol). NTP is used to synchronize computer clocks in the global Internet. It provides comprehensive mechanisms to access national time and frequency dissemination services, organize the time-synchronization subnet, and adjust the local clock in each participating subnet peer.

The access paradigm is identical to the UDP/TIME Protocol and, in fact, it is usually easy to adapt a UDP/TIME client implementation to operate using SNTP. Moreover, SNTP is also designed to operate in a dedicated server configuration including an integrated radio clock. With careful design and control of the various latencies in the system, it is possible to deliver time accurate to the order of microseconds.

Setting the current time

To enable SNTP on the switch:

1. In the left pane, click **Configuration**, **SNTP**, then click **Current Time Settings**. The *Current Time* screen opens.



2. Click the arrow button to open the **SNTP State** list, then select **Enabled**.
3. Type the IP address of the relay of the SNTP primary server in the **SNTP Primary Server** field.
4. Type the IP address of the relay of the SNTP secondary server in the **SNTP Secondary Server** field.
5. Type the SNTP polling interval in the **SNTP Poll Interval in Seconds** field. The default setting of 720 seconds is usually fine for most network configurations. A greater polling frequency will draw more network resources.
6. Click the arrow button to open the **Year** list, then select current year.
7. Click the arrow button to open the **Month** list, then select current month.
8. Click the arrow button to open the **Day** list, then select current day.

9 Click the arrow button to open the **Time in HH MM** lists, then select current time.

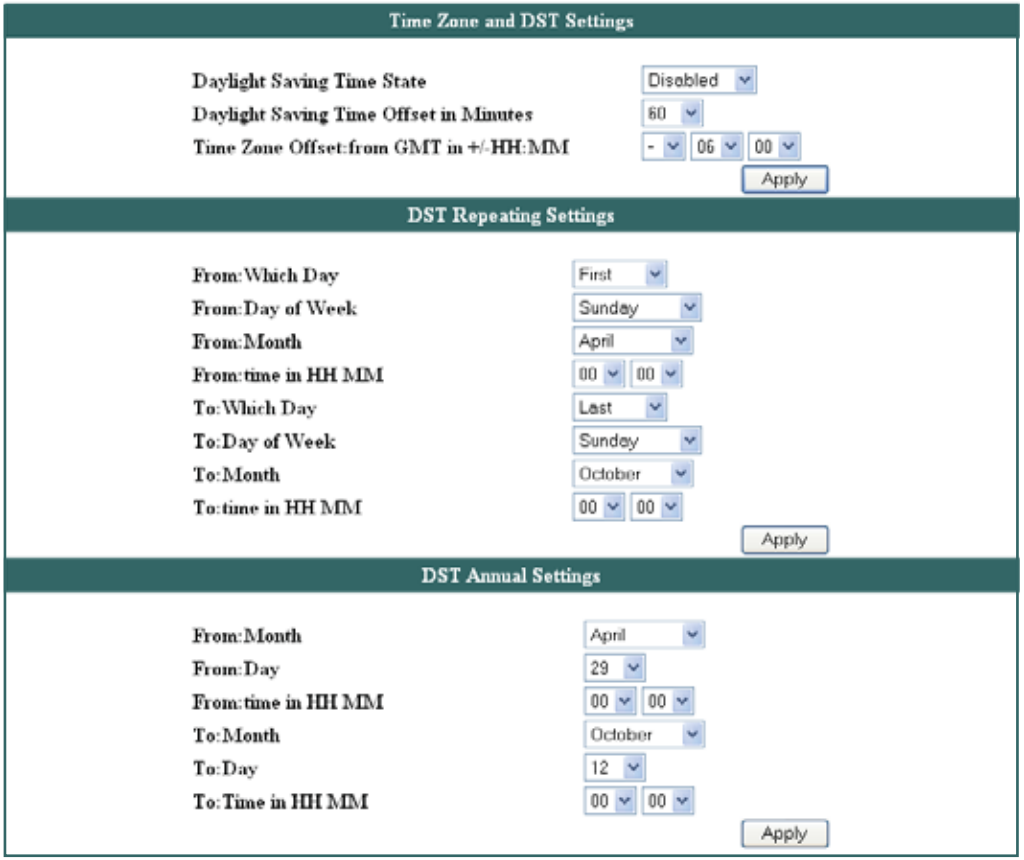
10 Click **Apply** to make the changes effective.

Setting the time zone and Daylight Savings Time

The *Time Zone and DST* screen allows you to set the Daylight Savings Time.

To make time zone and daylight savings time changes to the SNTP configuration:

1 In the left pane, click **Configuration**, **SNTP**, then click **Time Zone and DST**. The *Time Zone and DST* screen opens.



2 Click the arrow button to open the **Daylight Saving Time State** list, then select **Enabled**.

3 Click the arrow button to open the **Daylight Saving Time Offset in Minutes** list, then select the number of minutes that Daylight Saving Time is different than standard time.

4. Click the arrow button to open the **Time Zone Offset from GMT in +/- HH:MM** lists, then select to add (**+**) or subtract (**-**) time to adjust for the time zone relative to GMT.

5. If Daylight Savings Time begins and ends on a different date each year, complete the following steps:

   a. Click the arrow button to open the **From Which Day** list, then select the week of the month that Daylight Savings Time begins.

   b. Click the arrow button to open the **From Day of Week** list, then select the day of the week that Daylight Savings Time begins.

   c. Click the arrow button to open the **From Month** list, then select the month that Daylight Savings Time begins.

   d. Click the arrow button to open the **From Time in HH:MM** lists, then select the time of day that Daylight Savings Time begins. Time is expressed using a 24-hour clock with the hour and minute only.

   e. Click the arrow button to open the **To Which Day** list, then select the week of the month that Daylight Savings Time ends.

   f. Click the arrow button to open the **To Day of Week** list, then select the day of the week that Daylight Savings Time ends.

   g. Click the arrow button to open the **To Month** list, then select the month that Daylight Savings Time ends.

   h. Click the arrow button to open the **To Time in HH:MM** lists, then select the time of day that Daylight Savings Time ends. Time is expressed using a 24-hour clock with the hour and minute only.

6. If Daylight Savings Time begins and ends on the same date each year, complete the following steps:

   a. Click the arrow button to open the **From Month** list, then select the month that Daylight Savings Time begins.

   b. Click the arrow button to open the **From Day** list, then select the day that Daylight Savings Time begins.

   c. Click the arrow button to open the **From Time in HH:MM** lists, then select the time of day that Daylight Savings Time begins. Time is expressed using a 24-hour clock with the hour and minute only.

   d. Click the arrow button to open the **To Month** list, then select the month that Daylight Savings Time ends.

   e. Click the arrow button to open the **To Day** list, then select the day that Daylight Savings Time ends.

f Click the arrow button to open the **To Time in HH:MM** lists, then select the time of day that Daylight Savings Time ends. Time is expressed using a 24-hour clock with the hour and minute only.

7 Click **Apply** to make the changes effective.

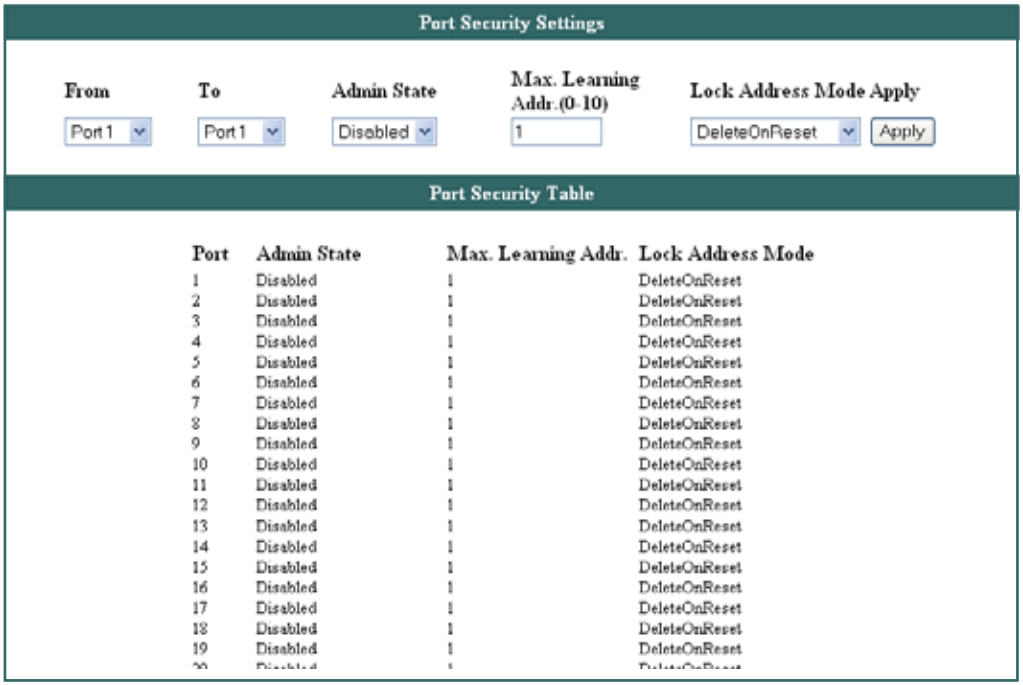
Setting port security

A given port's (or a range of port's) dynamic MAC address learning can be locked such that the current source MAC addresses entered into the MAC address forwarding table can not be changed once the port lock is enabled. The port can be locked by changing the **Admin State** pull-down menu to **Enabled**, and clicking **Apply**.

This is a security feature that prevents unauthorized computers (with source MAC addresses unknown to the switch prior to locking the port or ports) from connecting to the switch's locked ports and gaining access to the network.

To set the port security:

1 In the left pane, click **Configuration**, then click **Port Security**. The *Port Security Settings* screen opens.



2. Click the arrow button to open the **From** and **To** lists, then select the consecutively numbered group of ports on the switch for configuration.

3. Click the arrow button to open the **Admin State** list, then select **Enabled** or **Disabled**. This selection allows the selected port(s) dynamic MAC address learning to be locked such that new source MAC addresses cannot be entered into the MAC address table for the locked port or group of ports.

4. Type the maximum number of addresses that can be learned for the port in the **Max Learning Address.(0-10)** field. The port can be restricted to 10 or less MAC addresses that are allowed for dynamically learned MAC addresses in the forwarding table.

5. Click the arrow button to open the **Lock Address Mode** list, then select **Delete On Timeout** to clear dynamic entries for the ports on timeout of the FDB (Forwarding Data Base). Specify **Delete On Reset** to delete all FDB entries, including static entries after a system reset or rebooting.

6. Click **Apply** to make the changes effective.

Using 802.1p priority queuing (QoS)

Your switch supports 802.1p priority queuing. The switch has four priority queues. These priority queues are numbered from 0 (lowest priority queue) to 3 (highest priority queue). The eight priority queues specified in IEEE 802.1p (Q0 to Q7) are mapped to the switch's priority queues as follows:

- Q2 and Q1 are assigned to the switch's Q0 queue.
- Q3 and Q0 are assigned to the switch's Q1 queue.
- Q5 and Q4 are assigned to the switch's Q2 queue.
- Q7 and Q6 are assigned to the switch's Q3 queue.

The switch's four priority queues are emptied in a round-robin fashion, beginning with the highest priority queue and proceeding to the lowest priority queue before returning to the highest priority queue.

For strict priority-based scheduling, any packets residing in the higher priority queues are transmitted first. Only when these queues are empty, are packets of lower priority transmitted.

The weighted-priority based scheduling alleviates the main disadvantage of strict priority-based scheduling in that lower priority queues get starved of bandwidth by providing a minimum bandwidth to all queues for transmission. This is accomplished by configuring the maximum number of packets allowed to be transmitted from a given

priority queue and the maximum amount of time a given priority queue will have to wait before being allowed to transmit its accumulated packets. This establishes a Class of Service (CoS) for each of the switch's four hardware priority queues.

The possible range for maximum packets is: 0 to 255 packets.

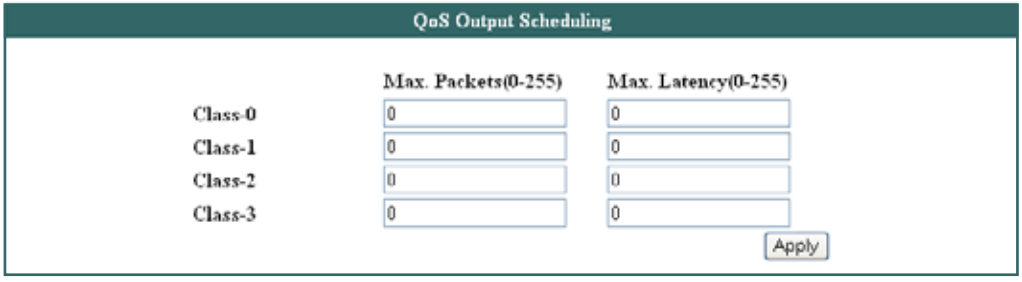
The possible range for maximum latency is: 0 to 255 (in increments of 16 microseconds each).

Remember that your switch has four priority queues (and thus four Classes of Service) for each port on the switch.

Configuring QoS output scheduling

To configure QoS output scheduling:

1. In the left pane, click **Configuration**, **QoS**, then click **Scheduling**. The *QoS Output Scheduling* screen opens.



2. Type the number of packets that a queue will transmit before surrendering the transmit buffer to the next lower priority queue in a round-robin fashion in the **Max. Packets (O-255)** field.

3. Type the maximum amount of time that a queue will have to wait before being given access to the transmit buffer in the **Max. Latency (0-255)** field. The **Max. Latency (0-255)** is a priority queue timer. When the timer expires, the round-robin method is temporarily halted. The priority queue that the timer was set for has access to the transmit buffer.

   There is a small amount of additional latency introduced because the priority queue that is transmitting at the time the **Max. Latency(0-255)** time expires will finish transmitting its current packet before giving up the transmit buffer.

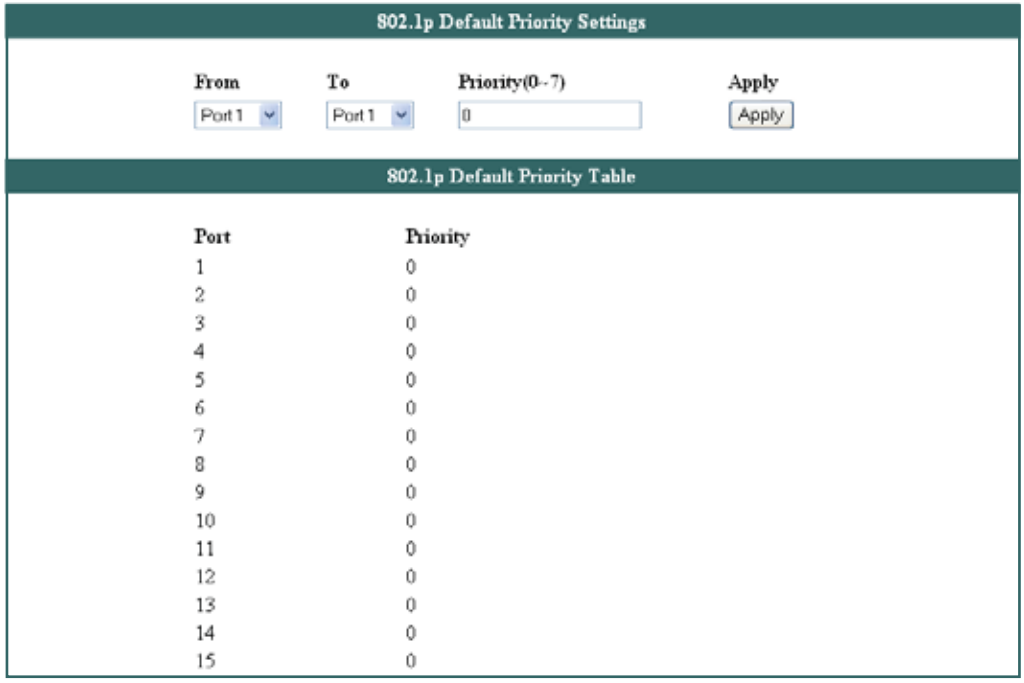
4. Click **Apply** to make the changes effective.

Assigning default priority

The switch allows the assignment of a default 802.1p priority to each port on the switch. This screen allows you to assign a default 802.1p priority to any given port on the switch. The priority queues are numbered from 0 the lowest priority to 7 the highest priority.

To assign default priority on the switch:

1. In the left pane, click **Configuration**, **QoS**, then click **802.1p Default Priority**. The *802.1p Default Priority Settings* screen opens.



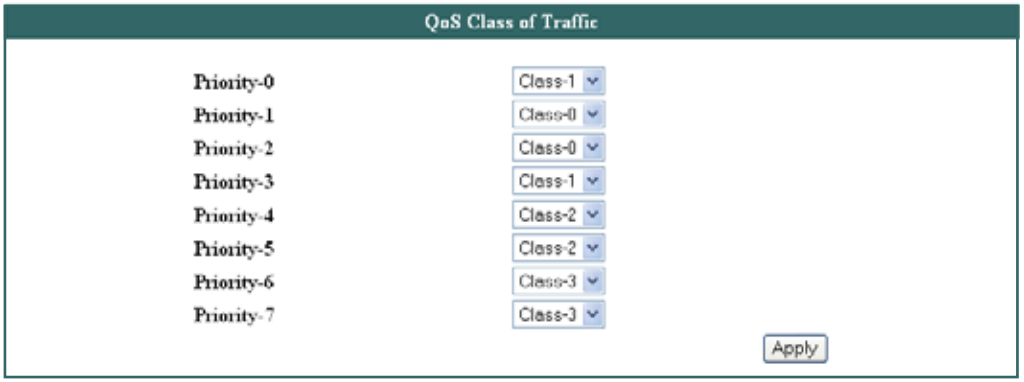
2. Click the arrow button to open the **From** and **To** lists, then select the consecutively numbered group of ports on the switch for priority assignment.
3. Type the new default priority in the **Priority** field. The priority queues are numbered from 0 (lowest priority) to 7 (highest priority).
4. Click **Apply** to make the changes effective.

Assigning user priority

Your switch allows the assignment of a Class of Traffic to each of the 802.1p priorities. Once you have assigned a maximum number of packets and a maximum latency to a given Class of Service on the switch, you can then assign this class to each of the eight levels of 802.1p priorities.

To assign a class of traffic to each of the 802.1p priorities:

1. In the left pane, click **Configuration**, **QoS**, then click **802.1p User Priority**. The *QoS Class of Traffic* screen opens.



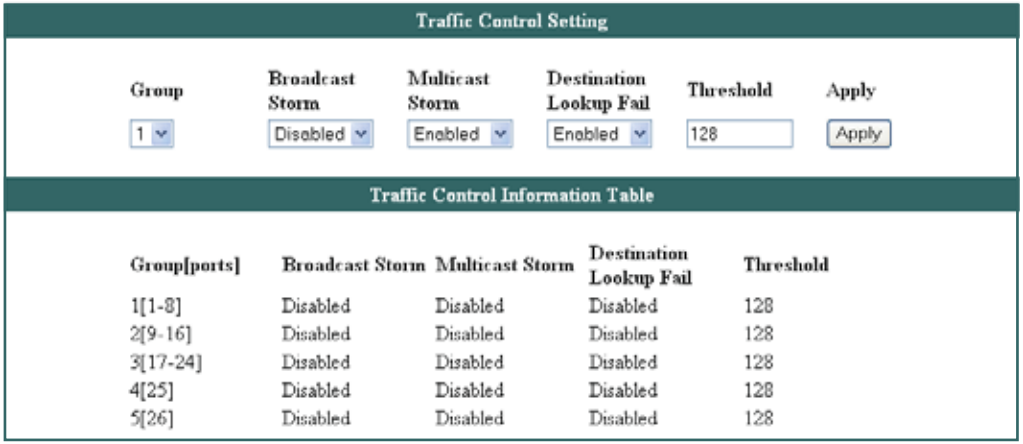
2. Click the arrow button to open the **Priority-0** through **Priority-7** lists, then select the Class of Service for each priority assignment.
3. Click **Apply** to make the changes effective.

Managing traffic control

This screen allows you to manage traffic control on the switch.

To manage traffic control on the switch:

1. In the left pane, click **Configuration**, **QoS**, then click **Traffic control**. The *Traffic Control Setting* screen opens.



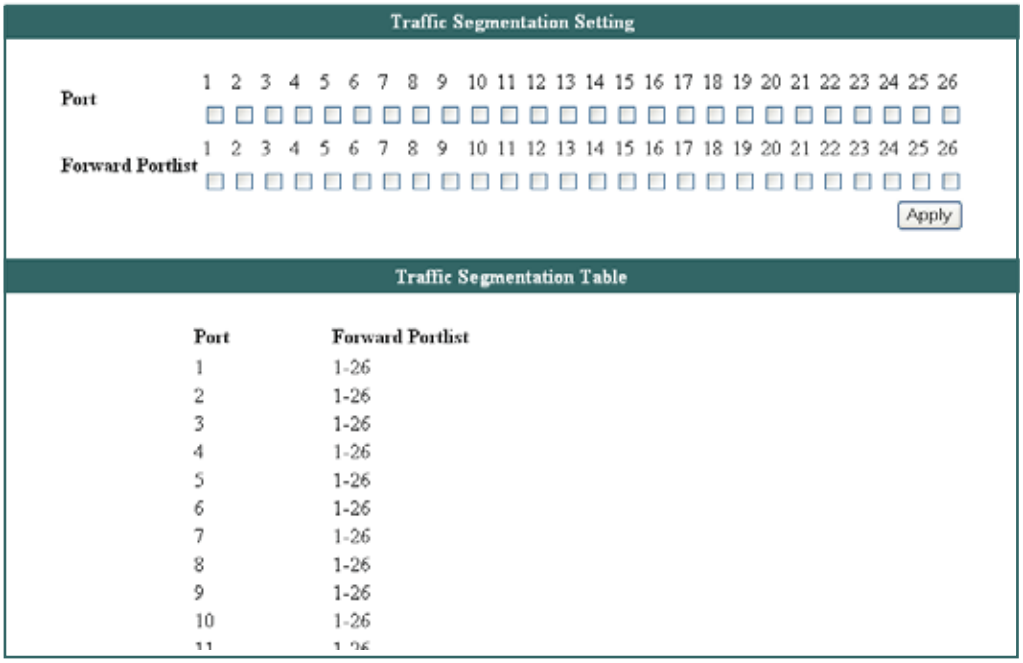
2. Click the arrow button to open the **Group** list, then select the desired group of ports.
3. Click the arrow button to open the **Broadcast Storm** list, then select **Enabled** or **Disabled**. This enables or disables, globally, the switch's reaction to Broadcast storms, triggered at the threshold set in the **Threshold** field.
4. Click the arrow button to open the **Multicast Storm** list, then select **Enabled** or **Disabled**. This globally enables or disables the switch's reaction to Multicast storms that are triggered at the threshold set in the **Threshold** field.
5. Click the arrow button to open the **Destination Lookup Fail** list, then select **Enabled** or **Disabled**. This globally enables or disables the switch's reaction to Destination Address Unknown storms that are triggered at the threshold set in the **Threshold** field.
6. Type the value in units of packets per second, beyond which the ingress port for that block discards packets in the **Threshold** field. Each port contains three counters, one each for Broadcast, Multicast, and Destination Lookup Fail packets. The counters are cleared every second. If the counter for a particular type of packet exceeds this threshold within one second, then further packets of that type will be dropped.
7. Click **Apply** to make the changes effective.

Managing traffic segmentation

This screen allows you to manage traffic segmentation on the switch.

To manage traffic segmentation on the switch:

1. In the left pane, click **Configuration**, **QoS**, then click **Traffic Segmentation**. The *Traffic Segmentation Setting* screen opens.



2. Click to select the source port number in the **Port** check boxes.
3. Click to select the ports that you want to segment in the **Forward Portlist** check boxes.

   For example, if you check **5** in the **Port** check boxes and **5** through **8** in the **Forward Portlist** check boxes, packets from port 5 will only be forwarded to ports 5 through 8. Packets to port 9 will be dropped.
4. Click **Apply** to make the changes effective.

Using MAC notification

MAC address notification is used to monitor MAC addresses learned and entered into the forwarding database.

Turning MAC notifications on or off globally

You can configure the MAC notification global settings.

To configure the MAC notification global settings:

1. In the left pane, click **Configuration**, **MAC Notification**, then click **Global Settings**. The *MAC Notification Global Settings* screen opens.

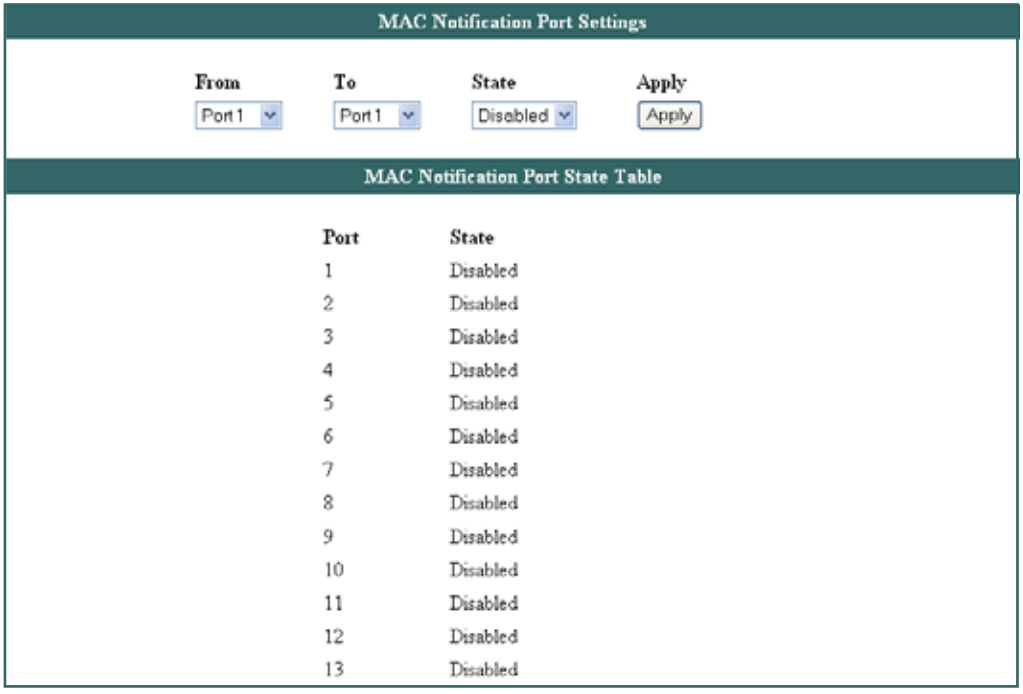
2. Click the arrow button to open the **State** list, then select **Enabled** or **Disabled** MAC notification.
3. Type the time in seconds between notifications in the **Interval** field.
4. Type the maximum number of entries listed in the history log used for notification in the **History Size** field. As many as 500 entries can be specified.
5. Click **Apply** to make the changes effective.

Turning MAC notifications on or off on a port

You can configure the MAC notifications on a port-to-port basis.

To configure the MAC notification global settings:

1. In the left pane, click **Configuration**, **MAC Notification**, then click **Port Settings**. The *MAC Notification Global Settings* screen opens.



2. Click the arrow button to open the **From** and **To** lists, then select the consecutively numbered group of ports on the switch to turn MAC notifications on or off.
3. Click the arrow button to open the **State** list, then select **Enabled** or **Disabled** MAC notification.
4. Click **Apply** to make the changes effective.

Using Link Aggregation Control Protocol (LACP)

The Link Aggregation Control Protocol (LACP) provides for the formation of a single Layer-2 link from two or more standard Ethernet member links through automatic member link activation using the Link Aggregation Control Protocol. LACP provides a robust means of assuring that both ends of the link are up and agree to be members of the aggregation before the link member is activated.

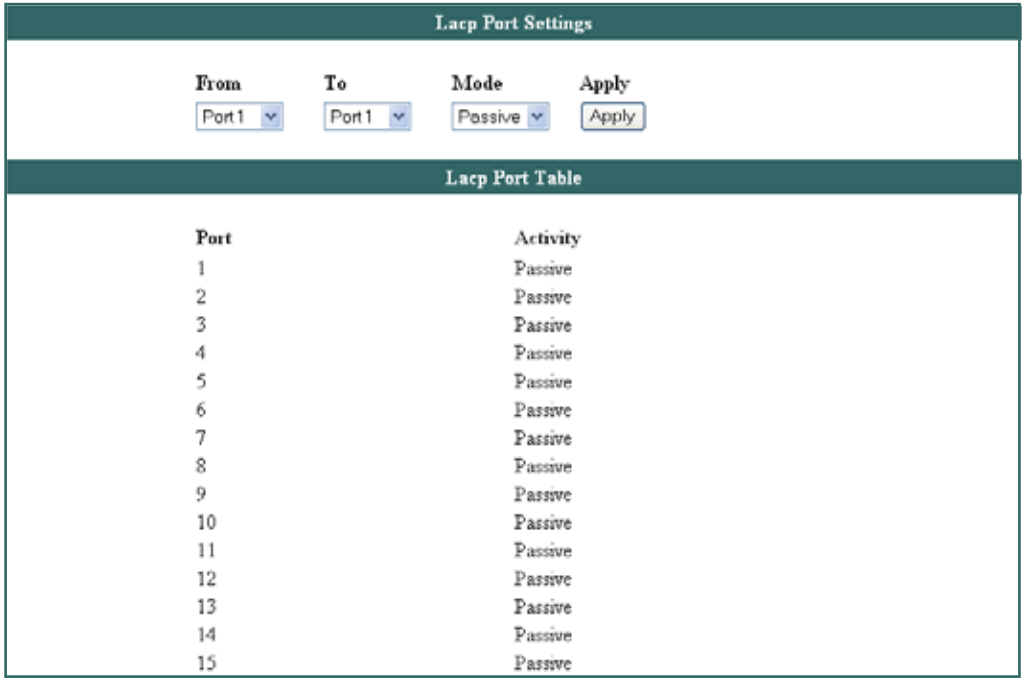
Enabling LACP

LACP must be enabled at both ends of the link to be operational. Should LACP not be available at both ends of the link, 802.3ad provides a manual aggregation that only requires both ends of the link be in a link up state. Because manual aggregation provides for the activation of a member link without performing the LACP message exchanges, it should not be considered as reliable and robust as an LACP negotiated link.

LACP automatically determines which member links can be aggregated and then aggregates them. It provides for the controlled addition and removal of physical links for the link aggregation such that no frames are lost or duplicated.

To enable LACP:

1 In the left pane, click **Configuration**, **LACP**, then click **Lacp Port**. The *Lacp Port Settings* screen opens.



2 Click the arrow button to open the **From** and **To** lists, then select the consecutively numbered group of ports on the switch to enable LACP.

3 Click the arrow button to open the **Mode** list, then select **Passive** or **Active**.

4 Click **Apply** to make the changes effective.

Using link aggregation

Link aggregation allows several ports to be grouped together and to act as a single link. This gives a bandwidth that is a multiple of a single link's bandwidth.

Link aggregation is most commonly used to link a bandwidth intensive network device or devices, such as a server, to the backbone of a network.

The switch allows the creation of as many as six link aggregation groups, each group consisting of as many as eight links (ports). All of the ports in the group must be members of the same VLAN. Further, the aggregated links must all be of the same speed and should be configured as full-duplex.

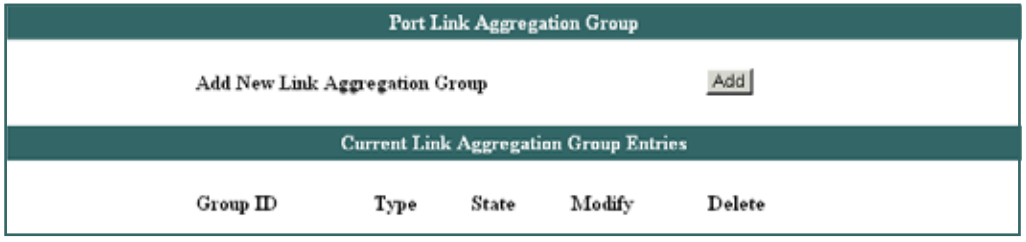
The configuration of the *Master Port* in the group becomes the configuration for all of the ports in the aggregation group. All configuration options, including the VLAN configuration, that can be applied to the Master Port are applied to the entire link aggregation group.

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

The Spanning Tree Protocol will treat a link aggregation group as a single link. STP will use the port parameters of the Master Port in the calculation of port cost and in determining the state of the link aggregation group. If two redundant link aggregation groups are configured on the switch, STP will block one entire group (in the same way STP will block a single port that has a redundant link).

To add a new link aggregation group or modify an existing link aggregation group:

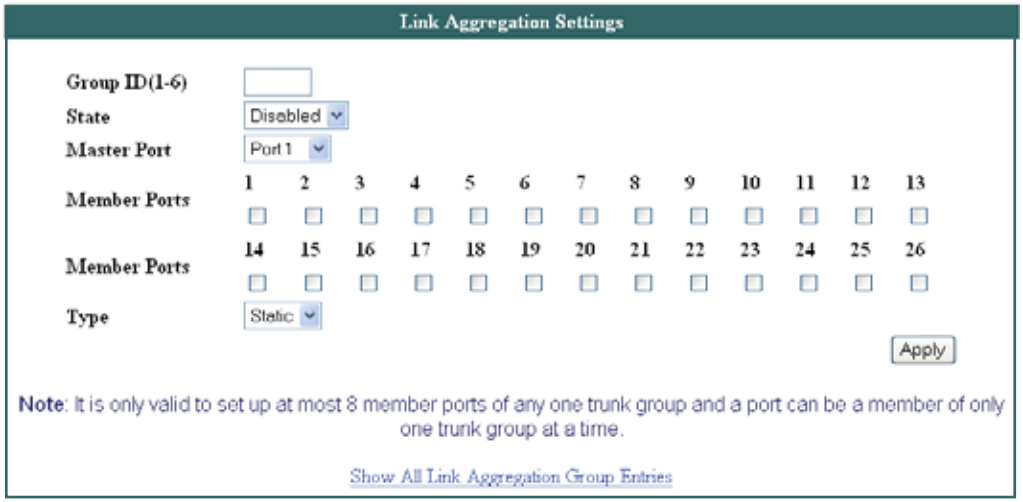
1 In the left pane, click **Configuration**, **LACP**, then click **Link Aggregation**. The *Port Link Aggregation Group* screen opens.



2 To add a new link aggregation group, click **Add**. The *Link Aggregation Settings* screen opens.

-OR-

To modify an existing link aggregation group, click the button in the **Modify** column next to the group ID you want to modify. The *Link Aggregation Settings* screen opens.



3 When adding a new group, type a number used to identify the link aggregation group in the **Group ID (1-6)** field. Displays the Group ID of the currently selected link aggregation group when editing an existing entry.

4 Click the arrow button to open the **State** list, then select **Enabled** or **Disabled**. This is used to turn a link aggregation group on or off. This is useful for diagnostics, to quickly isolate a bandwidth intensive network device, or to have an absolute backup link aggregation group that is not under automatic control.

5 Click the arrow button to open the **Master Port** list, then select the Master port of link aggregation group.

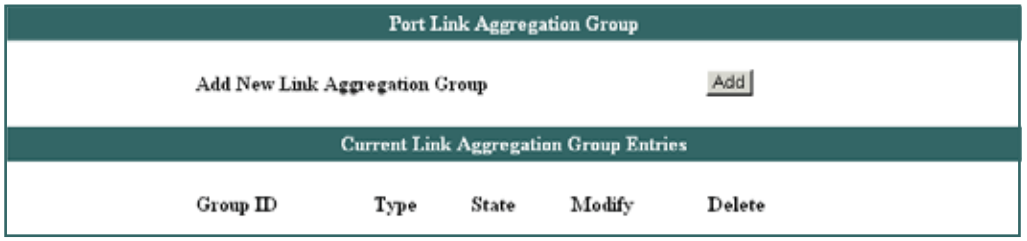
6 Click to select the **Member Port** checkboxes of the ports that make up the link aggregation group.

7 Click the arrow button to open the **Type** list, then select **Static** or **LACP**.

8 Click **Apply** to make the changes effective.

To delete an existing link aggregation group:

1 In the left pane, click **Configuration**, **LACP**, then click **Link Aggregation**. The *Port Link Aggregation Group* screen opens.



2 Click the button in the **Delete** column next to the Group ID entry you want to delete.

Using access profiles

Access profiles allow you to establish criteria to determine whether the switch will forward packets based on the information contained in each packet's header. These criteria can be specified on a basis of VLAN, MAC address, or IP address.

Creating an access profile is divided into two basic parts. The first is to specify which part or parts of a frame the switch will examine, such as the MAC source address or the IP destination address. The second part is entering the criteria the switch will use to determine what to do with the frame.

Adding or modifying an Ethernet access profile mask

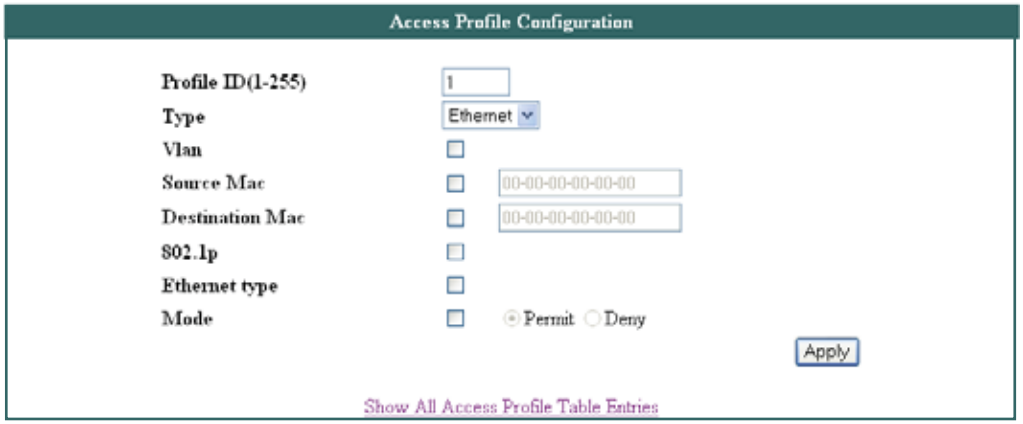
Important

If you are add or modifying an Internet access profile, go to "Adding or modifying an Internet access profile mask" on page 94.

To add or modify an Ethernet access profile mask:

1. In the left pane, click **Configuration**, then click **Access Profile Table**. The *Access Profile Table* screen opens.

2. Click **Add**. The *Access Profile Configuration* screen opens.



3. Type a unique identifier number for this profile set in the **Profile ID(1-255)** field. This value can be set from 1 to 255.
4. Click the arrow button to open the **Type** list, then select **Ethernet**.
5. Click **Vlan** if you want to instruct the switch to examine the VLAN part of each packet header and use this as the, or part of the criteria for forwarding.
6. Click **Source MAC Mask**, then type a MAC address mask for the source MAC address.

7 Click **Destination MAC Mask**, then type a MAC address mask for the destination MAC address.

8 Click **802.1p** if you want to instruct the switch to examine the 802.1p priority value of each packet header and use this as the, or part of the criteria for forwarding.

9 Click **Ethernet type** if you want to instruct the switch to examine the Ethernet type value in each frame's header.

10 Click **Mode**, then click **Permit** to specify that the packets that match the access profile are forwarded by the switch according to any additional rule added (see "Adding an access profile rule" on page 97).

-OR-

Click **Mode**, then click **Deny** to specify that packets that do not match the access profile are not forwarded by the switch and will be filtered.

11 Click **Apply** to make the changes effective.

Adding or modifying an Internet access profile mask

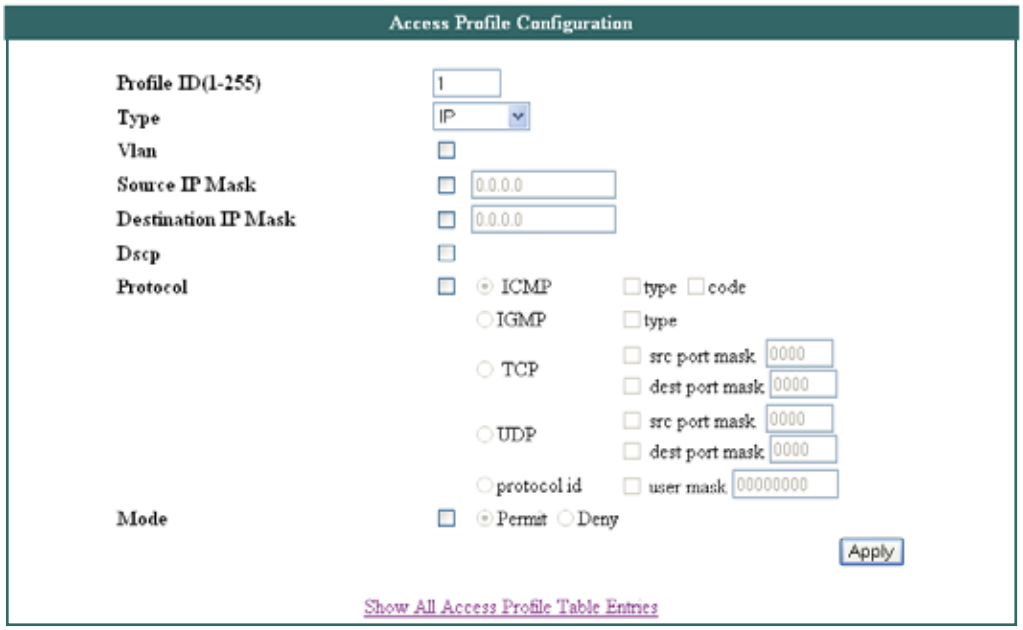
Important

If you are creating an Ethernet access profile, go to "Adding or modifying an Ethernet access profile mask" on page 93.

To add or modify an Internet access profile mask:

1 In the left pane, click **Configuration**, then click **Access Profile Table**. The *Access Profile Table* screen opens.

2 Click **Add**. The *Access Profile Configuration* screen opens.



3 Type a unique identifier number for this profile set in the **Profile ID(1-255)** field. This value can be set from 1 to 255.

4 Click the arrow button to open the **Type** list, then select **IP**.

5 Click **Vlan** if you want to instruct the switch to examine the VLAN part of each packet header and use this as the criteria, or part of the criteria for forwarding.

6 Click **Source IP Mask**, then type an IP address mask for the source IP address.

7 Click **Destination IP Mask**, then type an IP address mask for the destination IP address.

8 Click **Dscp** if you want the switch to examine the DiffServ Code part of each packet header and use this as the criteria, or part of the criteria for forwarding.

9 Click **Protocol** if you want the switch to examine the protocol type value in each frame's header. You must then specify what protocol(s) to include according to the following guidelines:

a Click **ICMP** if you want the switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header.

Click **type** to further specify that the access profile will apply an ICMP type value.

-OR-

Click **code** to further specify that the access profile will apply an ICMP code value.

b Click **IGMP** to instruct the switch to examine the Internet Group Management Protocol (IGMP) field in each frame's header.

Click **type** to further specify that the access profile will apply an IGMP type value.

c Click **TCP** to use the TCP port number contained in an incoming packet as the forwarding criteria. Selecting TCP requires that you specify a source port mask and/or a destination port mask.

Click **src port mask**, then type a TCP port mask for the source port in hex form (hex 0x0-0xffff).

Click **dest port mask**, then type a TCP port mask for the destination port in hex form (hex 0x0-0xffff).

d Click **UDP** to use the UDP port number contained in an incoming packet as the forwarding criteria. Selecting UDP requires that you specify a source port mask and/or a destination port mask.

Click **src port mask**, then type a TCP port mask for the source port in hex form (hex 0x0-0xffff).

Click **dest port mask**, then type a TCP port mask for the destination port in hex form (hex 0x0-0xffff).

e Click **protocol id** to instruct the switch to examine each frame's Protocol ID field.

Click **user mask** to specify that the rule applies to the IP protocol ID and the mask options behind the IP header, then type the user mask.

10 Click **Mode**, then click **permit** to specify that the packets that match the access profile are forwarded by the switch according to any additional rule added (see "Adding an access profile rule" on page 97).

-OR-

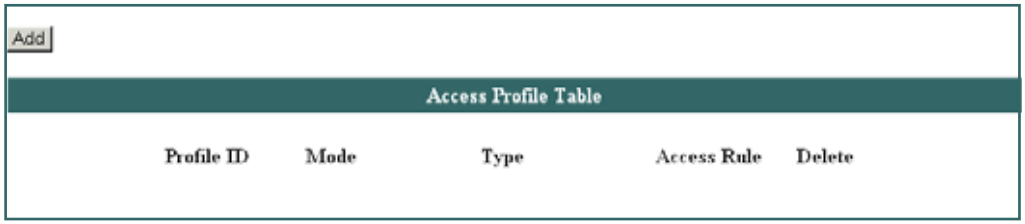
Click **Mode**, then click **deny** to specify that packets that do not match the access profile are not forwarded by the switch and will be filtered.

11 Click **Apply** to make the changes effective.

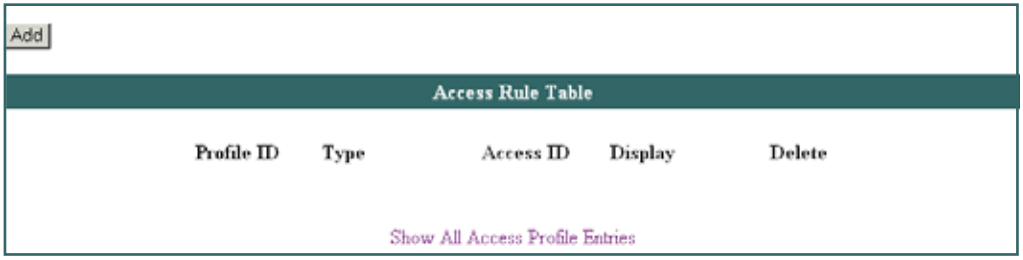
Adding an access profile rule

To add a new access profile rule:

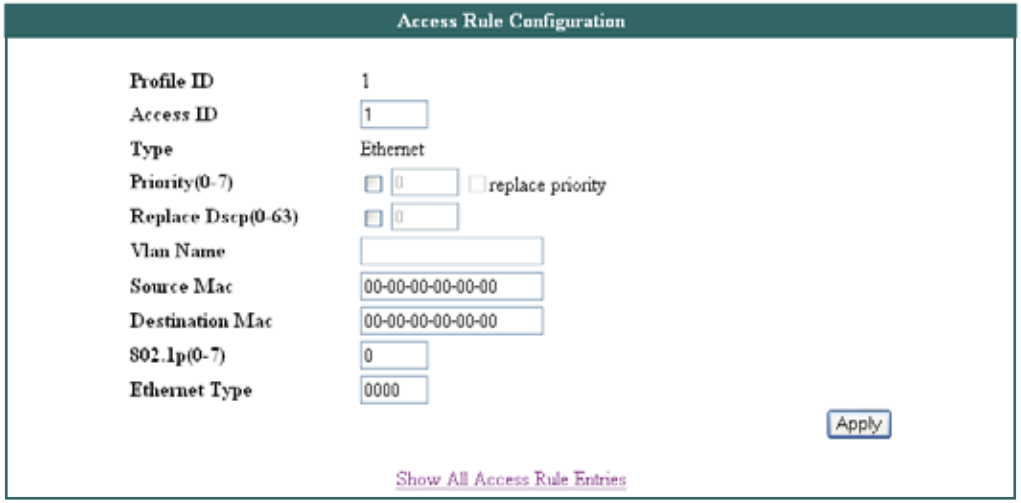
1 In the left pane, click **Configuration**, then click **Access Profile Table**. The *Access Profile Table* screen opens.



2 To add a new access profile rule, click the **Add** button. The *Access Rule Table* screen opens.



3 To add a new rule set for the access profile, click **Add**. The *Access Rule Configuration* screen opens with the **Profile ID** field showing the identifier number for this profile set. and the **Type** field showing the type (Ethernet or Internet) of this profile set.



4 Type in a unique identifier number for this access in the **Access ID** field. This value can be set from 1 to 255.

5 Click **Priority**, then type an 802.1p priority value for packets that meet the criteria in the adjacent field. A number between 0 (lowest priority) and 7 (highest priority) can be entered.

6 Click **replace priority** to instruct the switch to replace the 802.1p value (in a packet that meets the selected criteria). In this way, packets meeting the criteria can have their priority handling modified for use within the switch, and then have a different priority value assigned when they leave the switch.

7 Click **Replace Dscp** to instruct the switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.

Important

For information about other fields appearing on this screen, see "Adding or modifying an Ethernet access profile mask" on page 93 and "Adding or modifying an Internet access profile mask" on page 94.

8 Click **Apply** to make the changes effective.

To view an existing access profile rule:

1 In the left pane, click **Configuration**, then click **Access Profile Table**. The *Access Profile Table* screen opens.

2 To view an existing access profile rule, click the button in the **Modify** column next to the profile ID you want to modify. The *Access Rule Table* screen opens.

3 Click the button in the **Display** column next to the profile ID entry you want to view.

To delete an existing access profile rule:

1 In the left pane, click **Configuration**, then click **Access Profile Table**. The *Access Profile Table* screen opens.

2 To delete an existing access profile rule, click the button in the **Modify** column next to the profile ID you want to modify. The *Access Rule Table* screen opens.

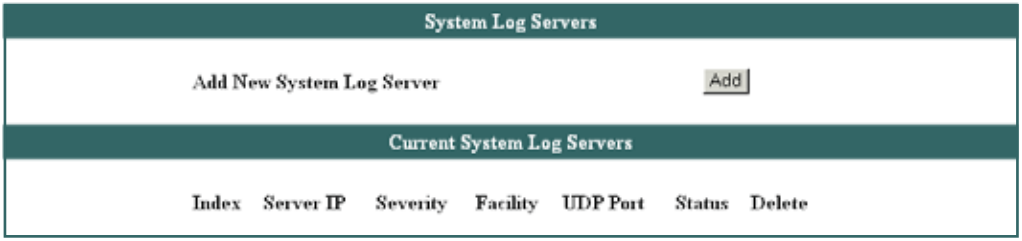
3 Click the button in the **Delete** column next to the profile ID entry you want to delete.

Using system log servers

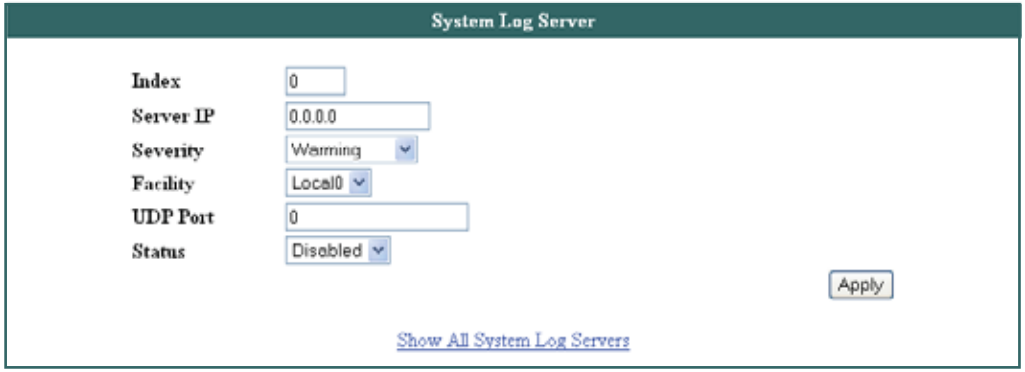
The switch can send Syslog messages to as many as four designated servers.

To add a new system log server:

1 In the left pane, click **Configuration**, then click **System Log Servers**. The *System Log Servers* screen opens.



2 Click **Add** to add a system log server. The *System Log Server* screen opens.



3 Type in the index value (1-4) of the Syslog server receiving the message in the **Index** field.

4 Type in the IP address of the Syslog server receiving the message in the **Server IP** field.

5 Click the arrow button to open the **Severity** list, then select the level of message sent. Options include: **Warning**, **Information**, or **All**.

6 Click the arrow button to open the **Facility** list, then select the facility value. Facility values range from **Local0** to **Local7**.

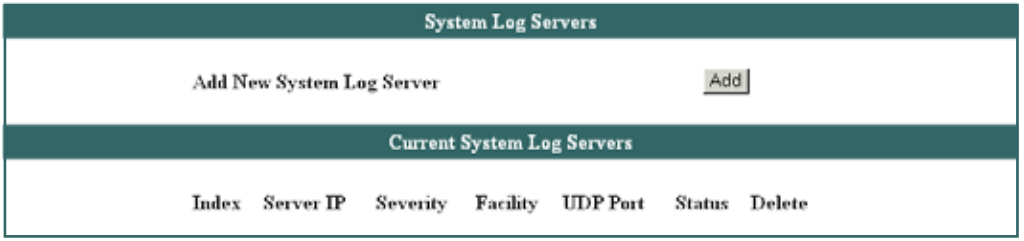
7 Type in the UDP port number used for sending Syslog messages in the **UDP Port** field. The default is 514.

8 Click the arrow button to open the **Status** list, then select **Enabled** or **Disabled** to activate or deactivate the system log server.

9 Click **Apply** to make the changes effective.

To delete a system log server:

1 In the left pane, click **Configuration**, then click **System Log Servers**. The *System Log Servers* screen opens.



2 Click the button in the **delete** column next to the system log server you want to delete.

PAE Access Entity

Your switch implements the server-side of the IEEE 802.1x Port-based Network Access Control. This mechanism is intended to allow only authorized users, or other network devices, access to network resources by establishing criteria for each port on the switch that a user or network device must meet before allowing that port to forward or receive frames.

IEEE 802.1X operation must be enabled on the switch before it will function. This is done using the 802.1x Status control on the *Switch Information (Advanced Settings)* screen (see "Setting advanced switch information" on page 55). 802.1X settings can be configured before it is enabled switch-wide.

Configuring existing 802.1X port settings

Existing 802.1X port settings are displayed and can be configured using the following screen.

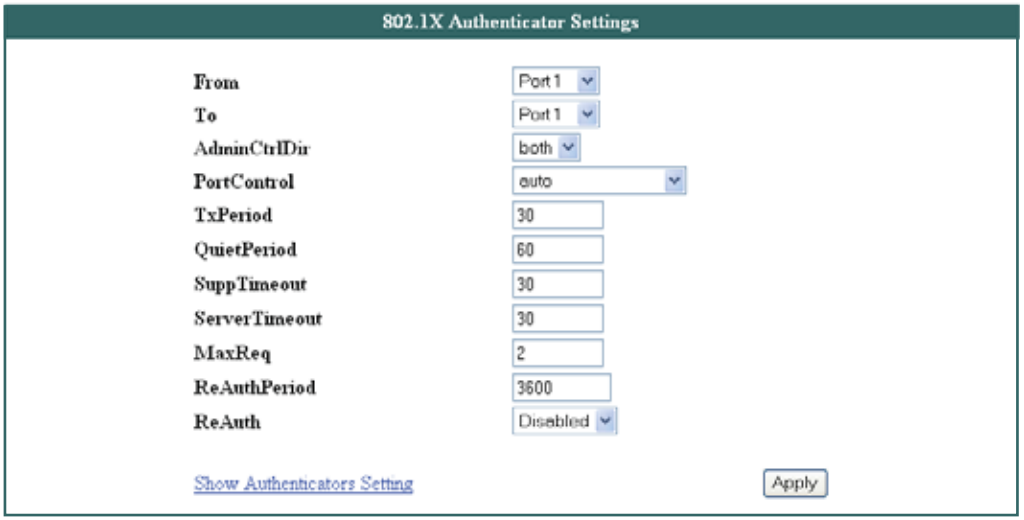
To configure 802.1X port settings:

1 In the left pane, click **Configuration**, **PAE Access Entity**, then click **Configure Authenticator**. The *802.1X Authenticator Settings* screen opens.

802.1X Authenticator Settings

Port	AdminCtrlDir	OperCtrlDir	Port Ctrl	TxPeriod	Quiet Period	Supp-Timeout	Server-Timeout	MaxReq	ReAuth Period	ReAuth Enabled
1	both	both	auto	30	60	30	30	2	3600	no
2	both	both	auto	30	60	30	30	2	3600	no
3	both	both	auto	30	60	30	30	2	3600	no
4	both	both	auto	30	60	30	30	2	3600	no
5	both	both	auto	30	60	30	30	2	3600	no
6	both	both	auto	30	60	30	30	2	3600	no
7	both	both	auto	30	60	30	30	2	3600	no
8	both	both	auto	30	60	30	30	2	3600	no
9	both	both	auto	30	60	30	30	2	3600	no
10	both	both	auto	30	60	30	30	2	3600	no
11	both	both	auto	30	60	30	30	2	3600	no
12	both	both	auto	30	60	30	30	2	3600	no
13	both	both	auto	30	60	30	30	2	3600	no
14	both	both	auto	30	60	30	30	2	3600	no
15	both	both	auto	30	60	30	30	2	3600	no
16	both	both	auto	30	60	30	30	2	3600	no
17	both	both	auto	30	60	30	30	2	3600	no
18	both	both	auto	30	60	30	30	2	3600	no

2 Click the hyperlink in the **Port** column for the port that you want to configure. The *802.1X Authenticator Settings* screen opens.



3 Click the arrow button to open the **From** and **To** lists, then select the consecutively numbered group of ports on the switch for configuration.

4 Click the arrow button to open the **AdmDir** list, then select whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction.

5 Click the arrow button to open the **PortControl** list, then select **forceAuthorized**, **forceUnauthorized** or **auto**. **ForceAuthorized** forces the authenticator of the port to become authorized. **ForceUnauthorized** forces the port to become unauthorized.

6 Type the time to wait for a response from a user to send EAP Request/Identity packets in the **TxPeriod** field.

7 Type the time interval between authentication failure and the start of a new authentication attempt in the **QuietPeriod** field.

8 Type the time to wait for a response from a user for all EAP packets, except for the Request/Identity packets in the **SuppTimeout** field.

9 Type the length of time to wait for a response from a Radius server in the **ServerTimeout** field.

10 Type the maximum number of times to retry sending packets to the user in the **MaxReq** field.

11 Type the time interval between successive re-authentications in the **ReAuthPeriod** field.

12 Click the arrow button to open the **ReAuth** list, then select to enable or disable reauthentication.

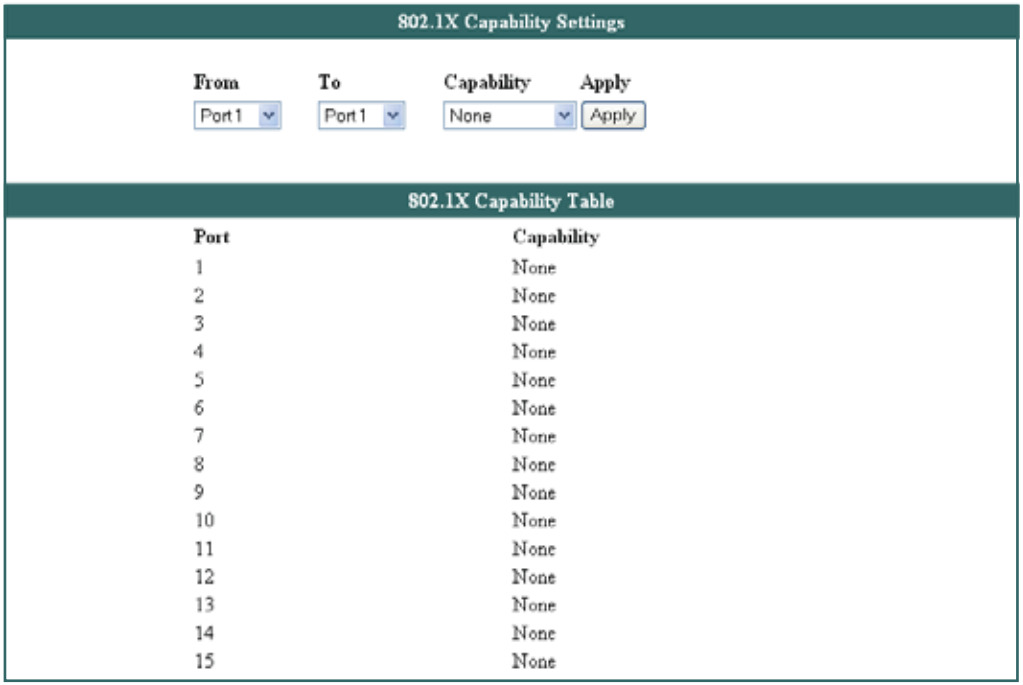
13 Click **Apply** to make the changes effective.

Configuring port capability settings

Existing 802.1x port settings are displayed and can be configured using the following screen.

To configure 802.1X port capability settings:

1 In the left pane, click **Configuration**, **PAE Access Entity**, then click **Port Capability Settings**. The *802.1X Capability Settings* screen opens.



2 Click the arrow button to open the **From** and **To** lists, then select the consecutively numbered group of ports on the switch for configuration.

3 Click the arrow button to open the **Capability** list, then select one of the following:

- **Authenticator** - A user must pass the authentication process to gain access to the network.
- **None** - The port is not controlled by the 802.1x functions.

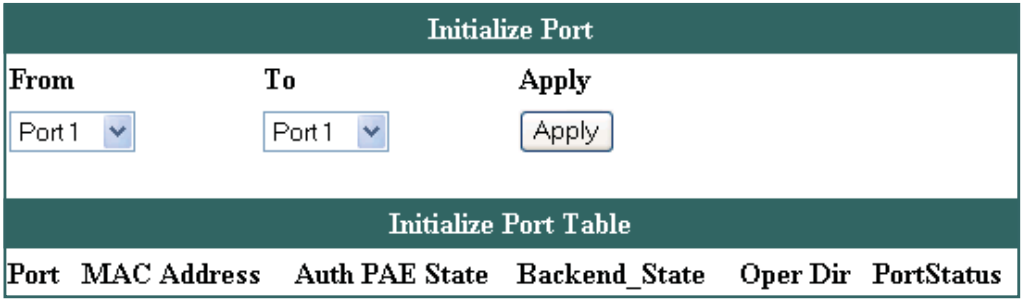
4 Click **Apply** to make the changes effective.

Initializing ports

This screen allows you to initialize a port or group of ports. The *Initialize Port Table* in the bottom half of the screen displays the current status of the port(s) once you have clicked **Apply**.

To initialize 802.1X ports:

1 In the left pane, click **Configuration**, **PAE Access Entity**, then click **Initialize Port(s)**. The *Initialize Port* screen opens.



2 Click the arrow button to open the **From** and **To** lists, then select the consecutively numbered group of ports on the switch to initialize.

3 Click **Apply** to make the changes effective. The following fields can be viewed in the *Initialize Port Table* after clicking **Apply**:

- **Port** - The port number.
- **MAC Address** - The MAC address of the switch where the port resides.
- **Auth PAE State** - The Authenticator PAE State displays one of the following: *Initialize*, *Disconnected*, *Connecting*, *Authenticating*, *Authenticated*, *Aborting*, *Held*, *ForceAuth*, *ForceUnauth*, or *N/A*.
- **Backend State** - The Backend Authentication State displays one of the following: *Request*, *Response*, *Success*, *Fail*, *Timeout*, *Idle*, *Initialize*, or *N/A*.

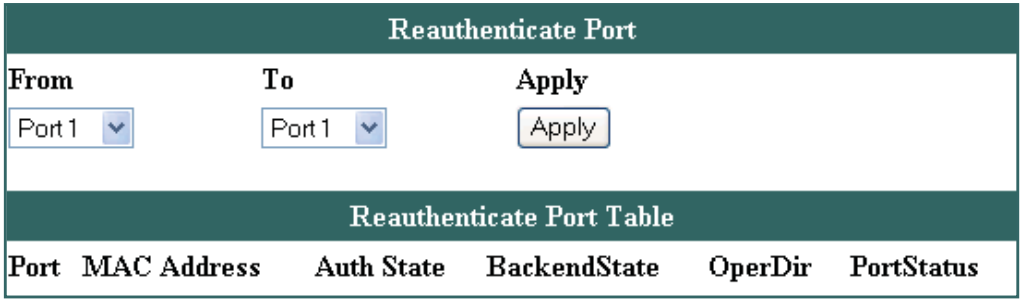
- **Oper Dir** - The Operational Controlled Directions are *both* and *in*.
- **PortStatus** - The status of the controlled port can be *authorized*, *unauthorized*, or *N/A*.

Reauthenticating port(s)

This screen allows you to reauthenticate a port or group of ports. The *Reauthenticate Port Table* displays the current status of the port(s) once you have clicked **Apply**.

To reauthenticate 802.1X ports:

1. In the left pane, click **Configuration**, **PAE Access Entity**, then click **Reauthenticate Port(s)**. The *Reauthenticate Port* screen opens.



2. Click the arrow button to open the **From** and **To** lists, then select the consecutively numbered group of ports on the switch to reauthenticate.
3. Click **Apply** to make the changes effective.

The following fields can be viewed in the *Reauthenticate Port Table* after clicking **Apply**:

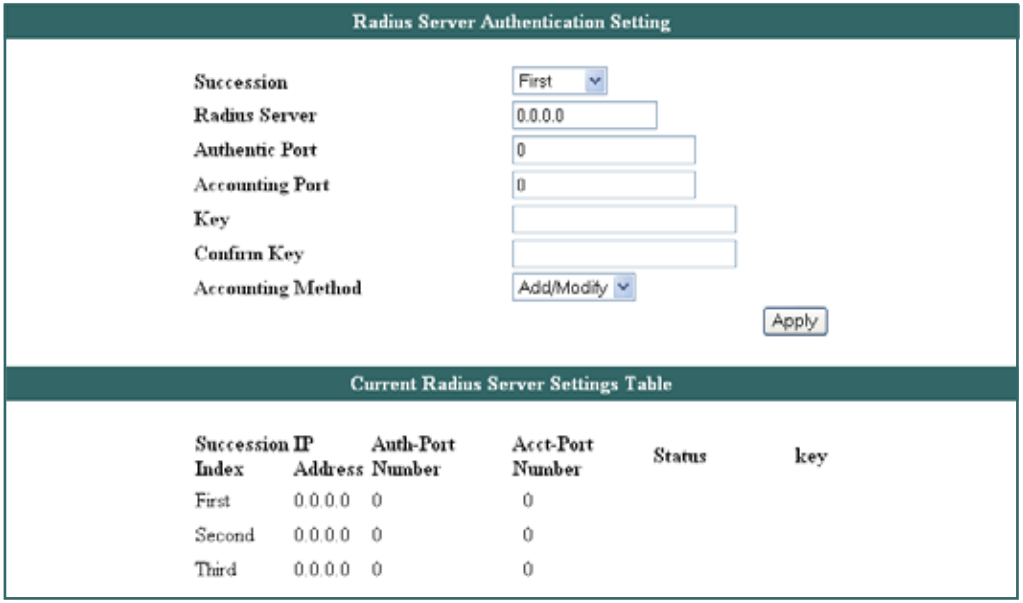
- **Port** - The port number.
- **MAC Address** - The MAC address of the switch where the port resides.
- **Auth State** - The Authenticator State will display one of the following: *Initialize*, *Disconnected*, *Connecting*, *Authenticating*, *Authenticated*, *Aborting*, *Held*, *ForceAuth*, *ForceUnauth*, or *N/A*.
- **BackendState** - The Backend State will display one of the following: *Request*, *Response*, *Success*, *Fail*, *Timeout*, *Idle*, *Initialize*, or *N/A*.
- **Oper Dir** - The Operational Controlled Directions are *both* and *in*.
- **PortStatus** - The status of the controlled port can be *authorized*, *unauthorized*, or *N/A*.

Using a RADIUS server

The RADIUS feature of the switch allows you to facilitate centralized user administration, as well as providing protection against a hacker.

To set up a RADIUS server:

1. In the left pane, click **Configuration**, **PAE Access Entity**, then click **Radius Server**. The *Radius Server Authentication Setting* screen opens.



2. Click the arrow button to open the **Succession** list, then select the desired RADIUS server to configure: **First**, **Second**, or **Third**.
3. Type the RADIUS server IP address in the **Radius Server** field.
4. Type the RADIUS authentic server(s) UDP port in the **Authentic Port** field. The default is 1812.
5. Type the RADIUS account server(s) UDP port in the **Accounting Port** field. The default is 1813.
6. Type the RADIUS server key in the **Key** field.
7. Type the RADIUS server shared key in the **Confirm Key** field.

8 Click the arrow button to open the **Accounting Method** list, then select to **Add/Modify** or **Delete** an entry on the table in the bottom-half of this screen.

9 Click **Apply** to make the changes effective.

Management

Use the screen and folders contained in the **Management** folder to manage the switch. The hyperlinked screens and folders contained in the **Management** folder include:

- *Security IP* - See "Setting up a switch for remote management" on page 110
- *User Accounts* - See "Managing user accounts" on page 45
- *SNMPV3* - See "Using SNMPV3" on page 111
  - *SNMP User Table* - See "Adding and deleting SNMP User Table entries" on page 119
  - *SNMP View Table* - See "Adding and deleting SNMP View Table entries" on page 111
  - *SNMP Group Table* - See "Adding and deleting SNMP Group Table entries" on page 113
  - *SNMP Community Table* - See "Adding and deleting SNMP Community Table entries" on page 115
  - *SNMP Host Table* - See "Adding and deleting SNMP Host Table entries" on page 118
  - *SNMP Engine ID* - See "Modifying the SNMP Engine ID" on page 117

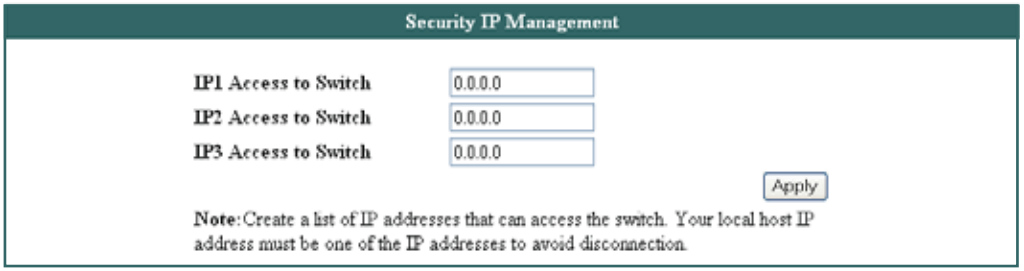
These menus are discussed in this section with the exception of the User Accounts (see "Managing user accounts" on page 45).

Setting up a switch for remote management

Some settings must be entered to allow the switch to be managed from an SNMP-based (Simple Network Management Protocol-based) Network Management System such as SNMP v1 or to be able to access the switch using the Telnet protocol or the Web manager.

To set up a switch for remote management:

1. In the left pane, click **Management**, then click **Security IP**. The *Security IP Management* screen opens.



2. Type the management station IP address in the **IP Access to Switch** field.

   Management stations are computers on the network that are used to manage the switch. You can limit the number of possible management stations by entering as many as three IP addresses. If the three IP address fields contain all zeros (0), then any station with any IP address can access the switch to manage and configure it. If there is one or more IP addresses entered in the IP address fields, then only stations with the IP addresses entered will be allowed to access the switch to manage or configure it.

3. Click **Apply** to make the changes effective.

Managing user accounts

For more information, see “Managing user accounts” on page 45.

Using SNMPV3

Your switch supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. The SNMP version used to monitor and control the switch can be specified by the administrator. The three versions of SNMP vary in the level of security provided between the management station and the network device.

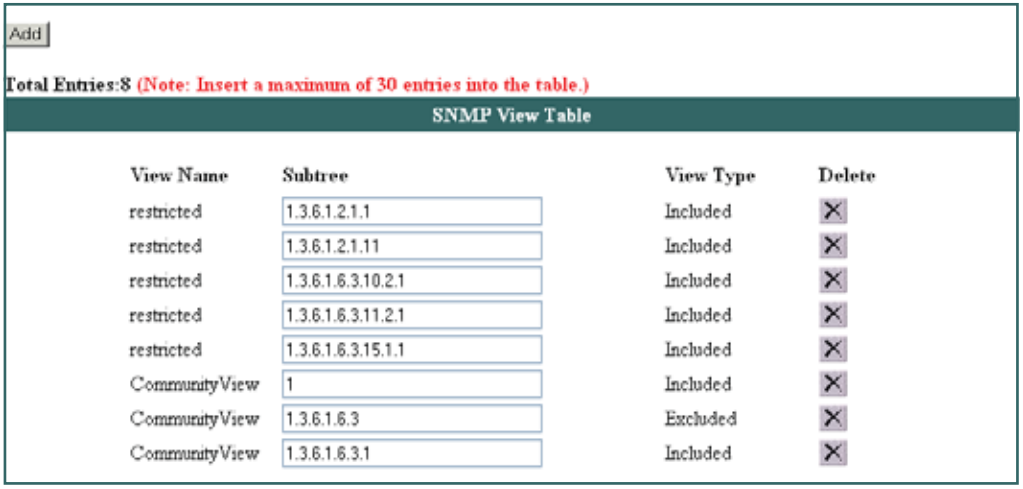
SNMP settings are configured using the menus located on the SNMP V3 folder of the Web manager. Workstations on the network that are allowed SNMP privileged access to the switch can be restricted with the Security IP Management screen. For more information, see "Setting up a switch for remote management" on page 110.

Adding and deleting SNMP View Table entries

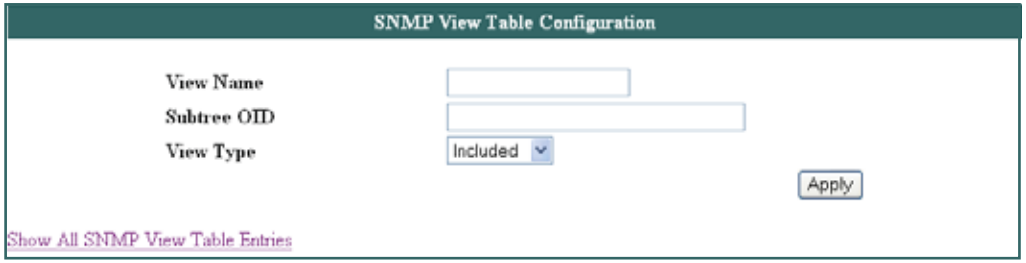
The *SNMP View Table* is used to assign views to community strings that define which MIB objects can be accessed by an SNMP manager.

To add an SNMP View Table entry:

1 In the left pane, click **Management**, **SNMPV3**, then click **SNMP View Table**. The *SNMP View Table* screen opens.



2 Click **Add**. The *SNMP View Table Configuration* screen opens.



3 Type the name of the new SNMP view being created in the **View Name** field. This is an alphanumeric string of as many as 32 characters.

4 Type the Object Identifier (OID) subtree for the view in the **Subtree OID** field. The OID identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager.

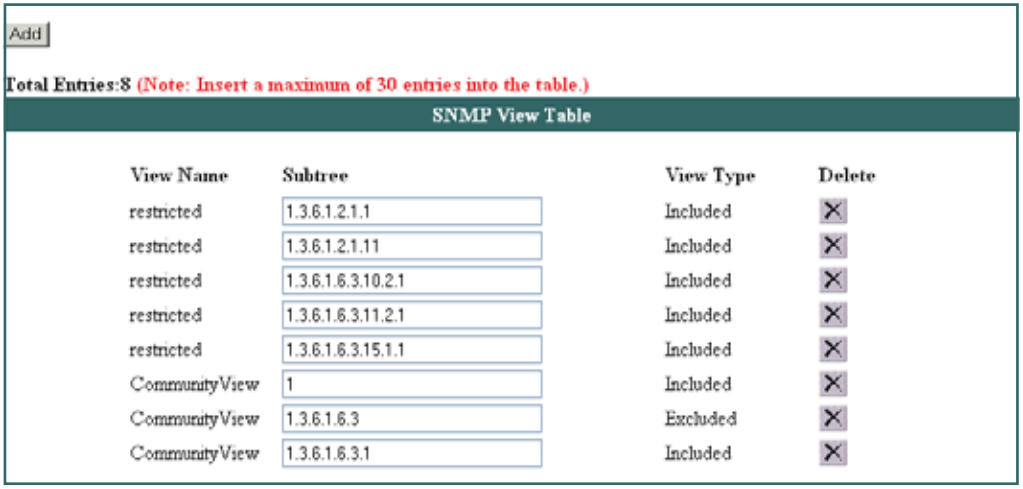
5 Click the arrow button to open the **View Type** list, then select one of the following:

- **Included** to include this object in the list of objects that an SNMP manager can access.
- **Excluded** to exclude this object from the list of objects that an SNMP manager can access.

6 Click **Apply** to make the changes effective.

To delete an SNMP View Table entry:

1 In the left pane, click **Management**, **SNMPV3**, then click **SNMP View Table**. The *SNMP View Table* screen opens.



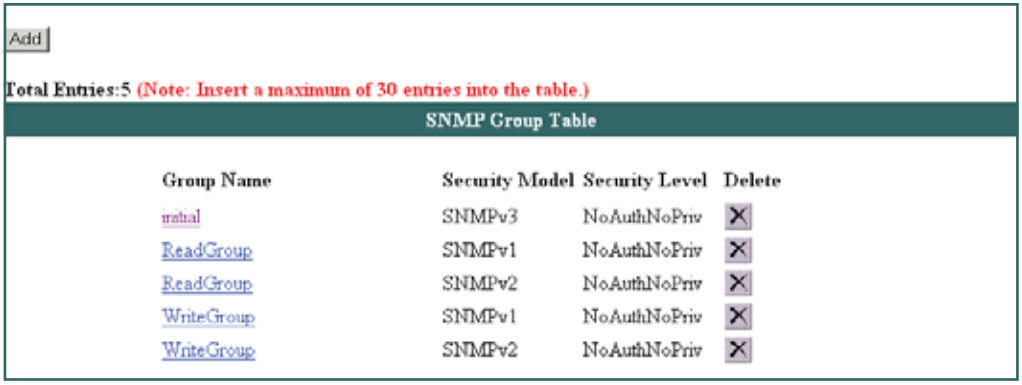
2 Click the button in the **Delete** column next the table entry you want to delete.

Adding and deleting SNMP Group Table entries

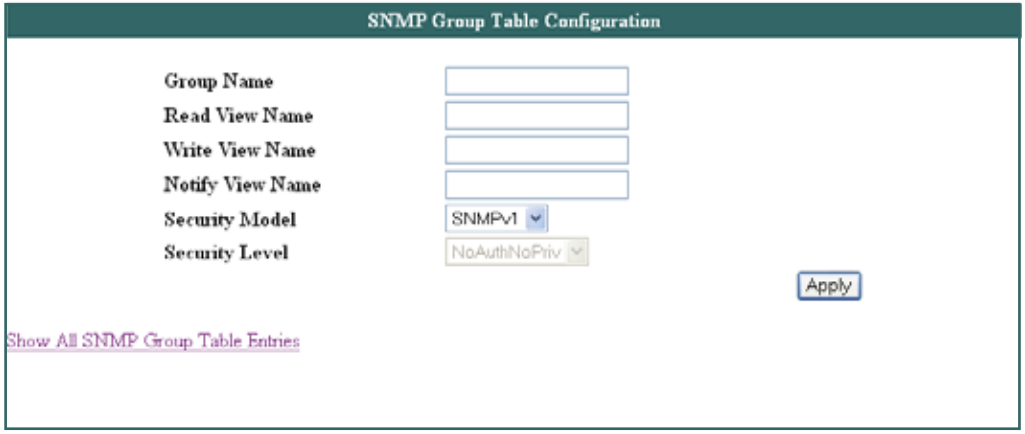
The SNMP Group created with this table maps SNMP users (identified in the SNMP User Table) to the views created in the previous menu.

To add an SNMP Group Table entry:

1 In the left pane, click **Management**, **SNMPV3**, then click **SNMP Group Table**. The *SNMP Group Table* screen opens.



2 Click **Add**. The *SNMP Group Table Configuration* screen opens.



3 Type the name of the new SNMP group of SNMP users being created in the **Group Name** field. This is an alphanumeric string of as many as 32 characters.

4 Type the name used to specify which SNMP group of users can request SNMP messages in the **Read View Name** field.

5 Type the name used to specify which SNMP group of users are allowed SNMP write privileges to the switch's SNMP agent in the **Write View Name** field.

6 Type the name used to specify which SNMP group of users can receive SNMP trap messages generated by the switch's SNMP agent in the **Notify View Name** field.

7 Click the arrow button to open the **Security Model** list, then select one of the following:

- **SNMPv1** - Specifies that SNMP version 1 will be used.
- **SNMPv2** - Specifies that SNMP version 2c will be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features.
- **USM** - Specifies that the SNMP version 3 will be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network.

8 Click the arrow button to open the **Security Level** list, then select one of the following:

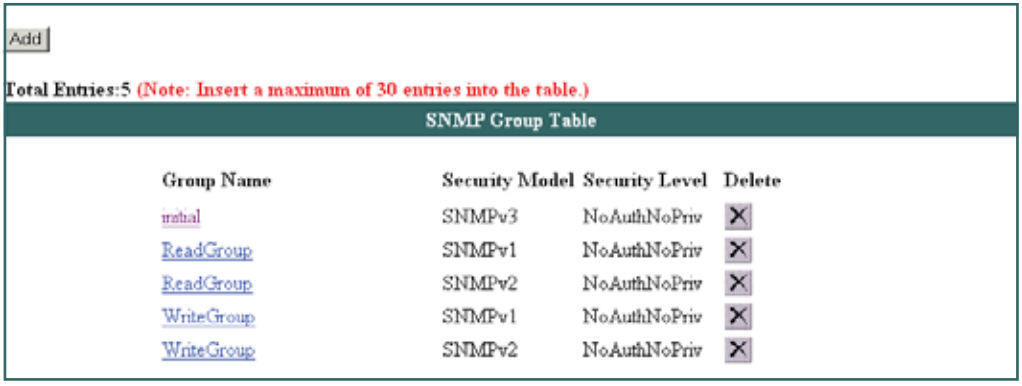
- **NoAuthNoPriv** - Specifies that there will be no authorization and no encryption of packets sent between the switch and a remote SNMP manager.

- **AuthNoPriv** - Specifies that authorization will be required, but there will be no encryption of packets sent between the switch and a remote SNMP manager.
- **AuthPriv** - Specifies that authorization will be required, and that packets sent between the switch and a remote SNMP manger will be encrypted.

9 Click **Apply** to make the changes effective.

To delete an SNMP Group Table entry:

1 In the left pane, click **Management**, **SNMPV3**, then click **SNMP Group Table**. The *SNMP Group Table* screen opens.



2 Click the button in the **Delete** column next the table entry you want to delete.

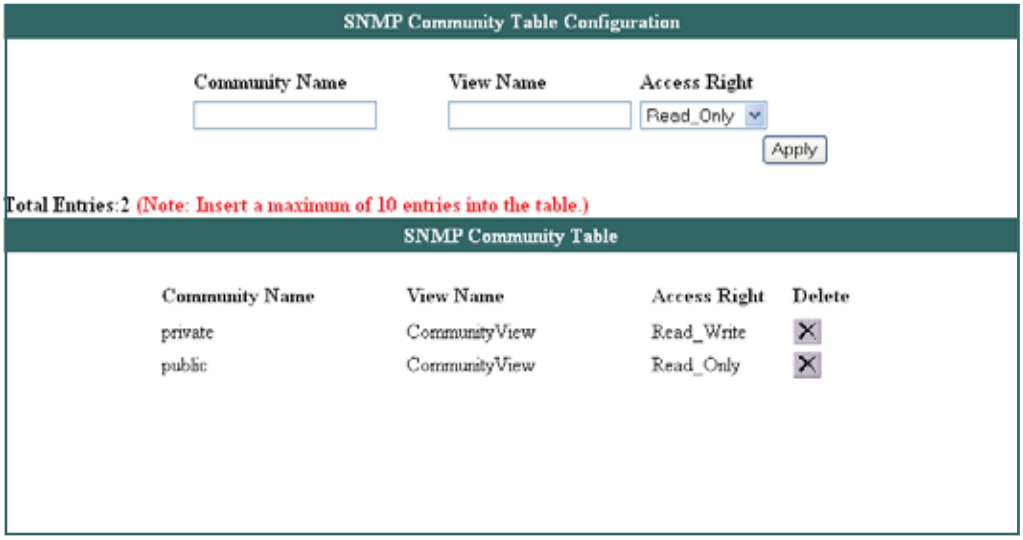
Adding and deleting SNMP Community Table entries

Use this table to create an SNMP community string to define the relationship between the SNMP manager and an agent. The community string acts like a password to permit access to the agent on the switch. One or more of the following characteristics can be associated with the community string:

- An Access List of IP addresses of SNMP managers that are permitted to use the community string to gain access to the switch's SNMP agent.
- An MIB view that defines the subset of all MIB objects that will be accessible to the SNMP community.
- Read/write or read-only level permission for the MIB objects accessible to the SNMP community.

To add an SNMP Community Table entry:

1 In the left pane, click **Management**, **SNMPV3**, then click **SNMP Community Table**. The *SNMP Community Table Configuration* screen opens.



2 Type the community name in the **Community Name** field. This is an alphanumeric string of as many as 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB (Management Information Base) objects in the switch's SNMP agent.

3 Type the view name in the **View Name** field. This is an alphanumeric string of as many as 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the switch. The view name must exist in the SNMP View Table.

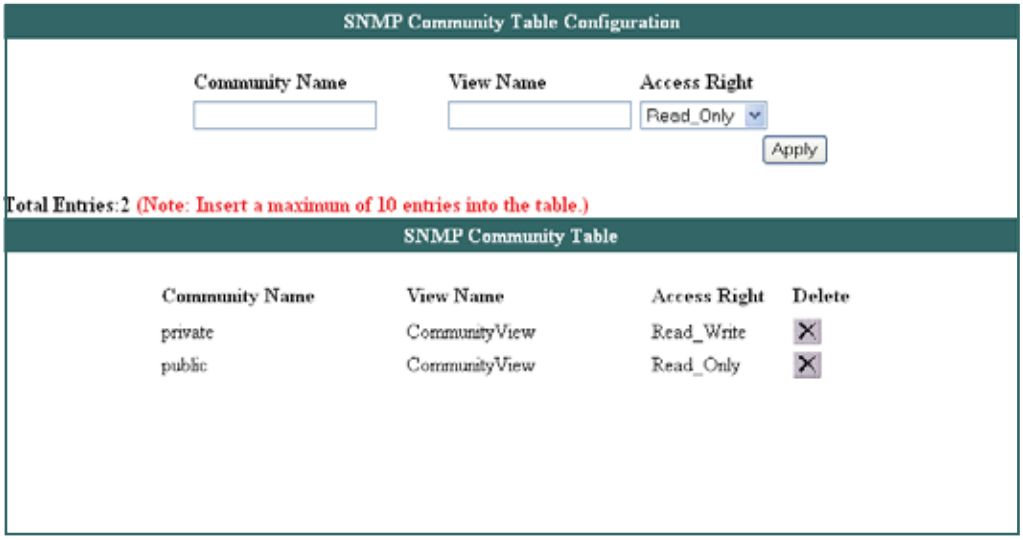
4 Click the arrow button to open the **Access Right** list, then select one of the following:

- **Read_Only** Specifies that SNMP community members using the community string created with this command can only read the contents of the MIBs on the switch.
- **Read_Write** Specifies that SNMP community members using the community string created with this command can read from and write to the contents of the MIBs on the switch.

5 Click **Apply** to make the changes effective.

To delete an SNMP Community Table entry:

1 In the left pane, click **Management**, **SNMPV3**, then click **SNMP Community Table**. The *SNMP Community Table Configuration* screen opens.



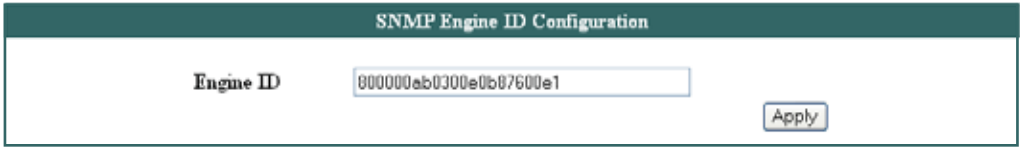
2 Click the button in the **Delete** column next the table entry you want to delete.

Modifying the SNMP Engine ID

The Engine ID is a unique identifier used for SNMP V3 implementations. This is an alphanumeric string used to identify the SNMP engine on the switch.

To modify the SNMP Engine ID:

1 In the left pane, click **Management**, **SNMPV3**, then click **SNMP Engine ID**. The *SNMP Engine ID Configuration* screen opens.



2 Type the new Engine ID in the **Engine ID** field.

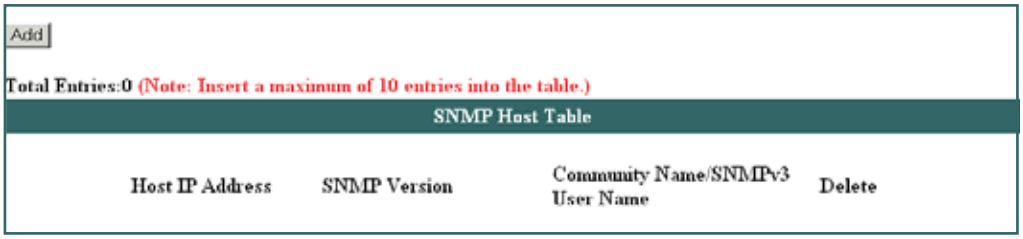
3 Click **Apply** to make the changes effective.

Adding and deleting SNMP Host Table entries

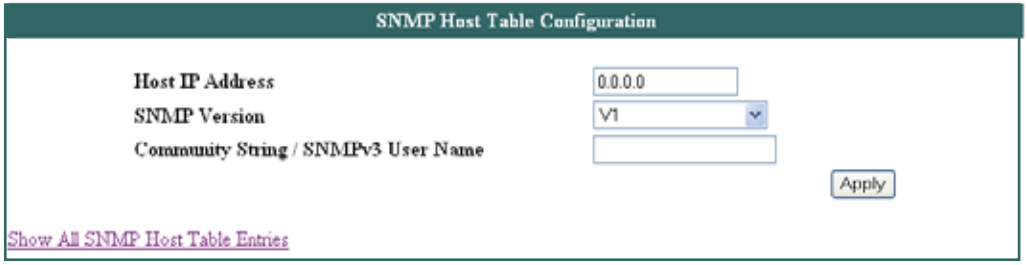
Use the SNMP Host Table to set up trap recipients.

To add an SNMP Host Table entry:

1. In the left pane, click **Management**, **SNMPV3**, then click **SNMP Host Table**. The *SNMP Host Table* screen opens.



2. Click **Add**. The *SNMP Host Table Configuration* screen opens.



3. Type the IP address of the remote management station that will serve as the SNMP host for the switch in the **Host IP Address** field.
4. Click the arrow button to open the **SNMP Version** list, then select one of the following:
   - **V1** - To specifies that SNMP version 1 will be used.
   - **V2** - To specify that SNMP version 2 will be used.
   - **V3** - To specify that the SNMP version 3 will be used.
5. Type the community string or SNMP V3 user name in the **Community String/SNMPv3 User Name** field.
6. Click **Apply** to make the changes effective.

To delete an SNMP Host Table entry:

1 In the left pane, click **Management**, **SNMPV3**, then click **SNMP Host Table**. The *SNMP Host Table* screen opens.

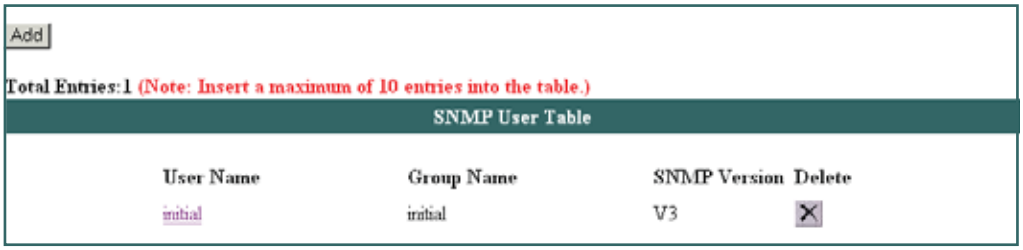
2 Click the button in the **Delete** column next the table entry you want to delete.

Adding and deleting SNMP User Table entries

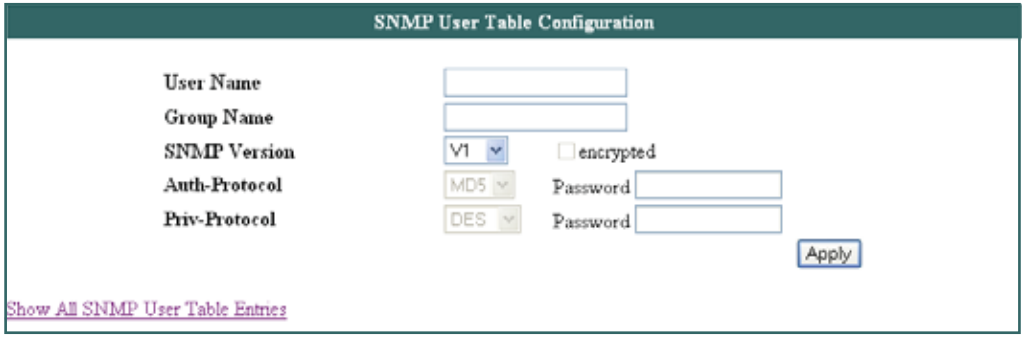
Use the SNMP User Table to create a new SNMP user and add the user to an existing SNMP group or to a newly created group.

To add an SNMP User Table entry:

1 In the left pane, click **Management**, **SNMPV3**, then click **SNMP User Table**. The *SNMP User Table* screen opens.



2 Click **Add**. The *SNMP User Table Configuration* screen opens.



3 Type in the new SNMP V3 user name or community string for V1 or V2 in the **User Name** field. This can be any alphanumeric name of as many as 32 characters that will identify the new SNMP user.

4 Type in the new SNMP V3 group name in the **Group Name** field. This can be any alphanumeric name of as many as 32 characters that will identify the SNMP group the new SNMP user will be associated with.

5 Click the arrow button to open the **SNMP Version** list, then select one of the following:

- **V1** - To specifies that SNMP version 1 will be used.
- **V2** - To specify that SNMP version 2 will be used.
- **V3** - To specify that the SNMP version 3 will be used.

6 If you selected **V3** in Step 5, you can check **encrypted**.

-OR-

Go to Step 9.

7 If you checked encrypted in Step 6, click the arrow button to open the **Auth-Protocol** list, then select one of the following:

- **MD5** - To specify that the HMAC-MD5-96 authentication level will be used.
- **SHA** - To specify that the HMAC-SHA-96 authentication level will be used.

Type the authentication protocol password in the **Password** field. This is an alphanumeric sting of between 8 and 20 characters that will be used to authorize the agent to receive packets for the host.

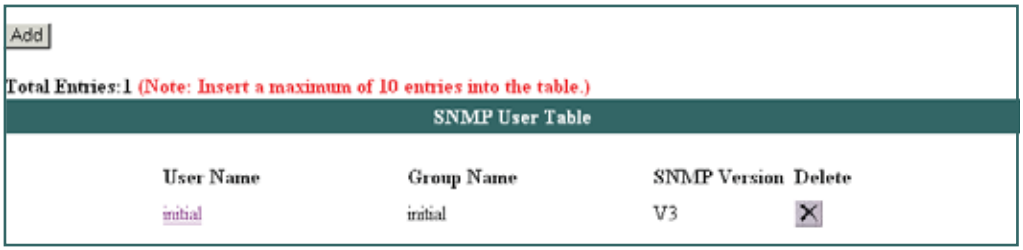
8 If you checked encrypted in Step 6, click the arrow button to open the **Priv-Protocol** list, then select **DES** or **None**.

Type the private protocol in the **Password** field. This is an alphanumeric string of between 8 and 16 characters that will be used to encrypt the contents of messages the host sends to the agent.

9 Click **Apply** to make the changes effective.

To delete an SNMP User Table entry:

1 In the left pane, click **Management**, **SNMPV3**, then click **SNMP User Table**. The *SNMP User Table* screen opens.



2 Click the button in the **Delete** column next the table entry you want to delete.

Monitoring

Your switch provides extensive network monitoring capabilities that can be viewed under the Monitoring menu. Use the screen and folders contained in the **Monitoring** folder to monitor the switch. The hyperlinked screens and folders contained in the **Monitoring** folder include:

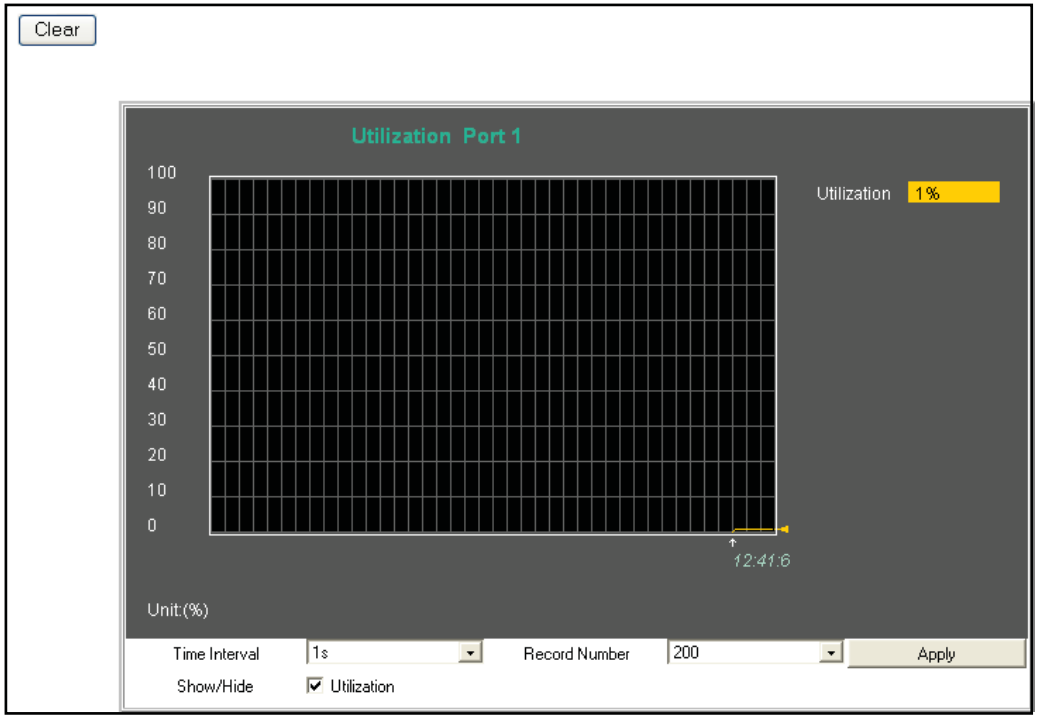
- *Port Utilization* - See "Viewing Port Utilization" on page 123
- *Packets* - See "Viewing packet statistics" on page 124
  - *Received (RX)* - See "Viewing Received (RX) packet statistics" on page 124
  - *UMB Cast (RX)* - See "Viewing UMB-cast (RX) packet statistics" on page 126
  - *Transmitted (TX)* - See "Viewing Transmitted (TX) packet statistics" on page 128
- *Errors* - See "Viewing errors" on page 130
  - *Received (RX)* - See "Viewing errors Received (RX)" on page 130
  - *Transmitted (TX)* - See "Viewing errors Transmitted (TX)" on page 132
- *Size* - See "Viewing packet size" on page 134
  - *Packet Size* - See "To view packet size in graph form:" on page 134
- *MAC Address* - See "Viewing the MAC address forwarding table" on page 137
- *IGMP Snooping Group* - See "Viewing the IGMP Snooping Group" on page 138
- *IGMP Snooping Forward* - See "Viewing IGMP Snooping forwarding table" on page 139
- *VLAN Status* - See "Viewing VLAN status" on page 140
- *Router Port* - See "Viewing router port" on page 140
- *Power Status* - See "Viewing port access control information" on page 142
- *Port Access Control* - See "Viewing port access control information" on page 142
  - *Authenticator State* - See "Viewing authenticator state" on page 142

Viewing Port Utilization

The *Utilization* screen shows the percentage of the total available bandwidth being used on the port.

To view port utilization:

1. In the left pane, click **Monitoring**, then click **Port Utilization**. The *Utilization* screen opens.



2. Click the port on the front panel display that you want to display the port utilization for.
3. Click the arrow button to open the **Time Interval** list, then select the desired setting between 1s and 60s, where **s** stands for seconds. The default value is one second.
4. Click the arrow button to open the **Record Number** list, then select number of times the Switch will be polled between 20 and 200. The default value is 20.
5. Click the **Utilization** checkbox to see utilization statistics.

6 Click the **Clear** button to clear all statistics counters on this screen.

7 Click **Apply**.

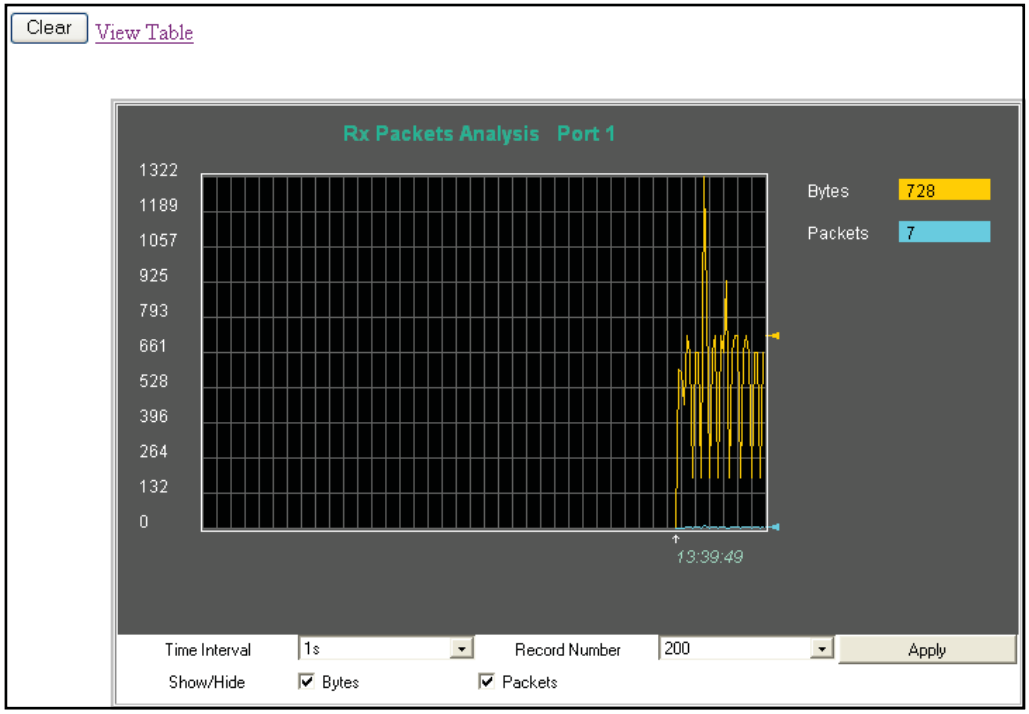
Viewing packet statistics

You can view various packet statistics either a line graph or a table.

Viewing Received (RX) packet statistics

To view packets received statistics in graph form:

1 In the left pane, click **Monitoring**, **Packets**, then click **Received (RX)**. The *Rx Packets Analysis* screen opens.



2 Click the **Clear** button to clear all statistics counters on this screen.

3 Click the arrow button to open the **Time Interval** list, then select the desired setting between 1s and 60s, where **s** stands for seconds. The default value is one second.

4 Click the arrow button to open the **Record Number** list, then select number of times the Switch will be polled between 20 and 200. The default value is 20.

5 Click the **Bytes** checkbox to see the number of bytes received on the port.

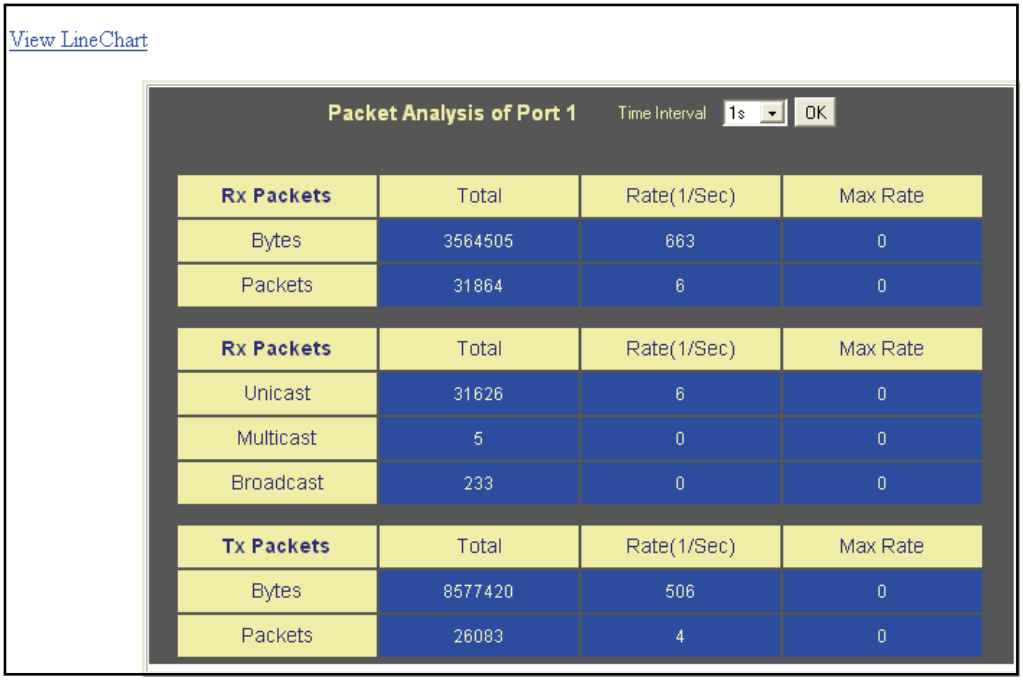
6 Click the **Packets** checkbox to see the number of packets received on the port.

7 Click **Apply**.

To view packets received statistics in table form:

1 In the left pane, click **Monitoring**, **Packets**, then click **Received (RX)**. The *Rx Packets Analysis* screen opens.

2 Click **View Table**.



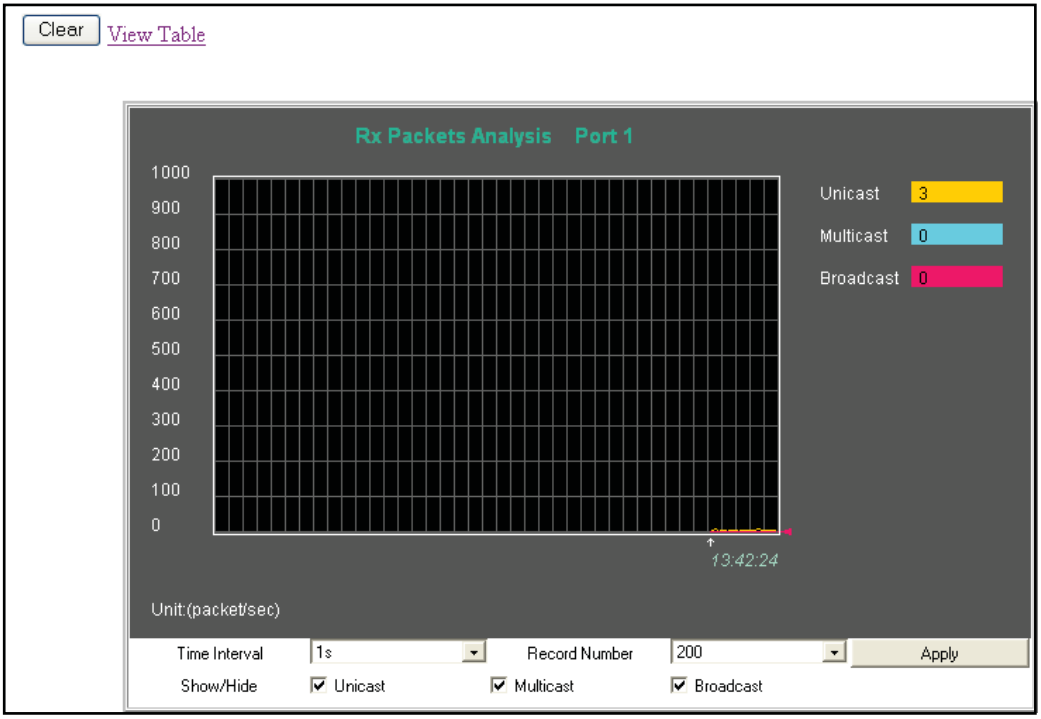
3 Click the arrow button to open the **Time Interval** list, then select the desired setting between 1s and 60s, where **s** stands for seconds. The default value is one second.

4 Click **OK**.

Viewing UMB-cast (RX) packet statistics

To view Unicast, Multicast, and Broadcast packets received statistics in graph form:

1. In the left pane, click **Monitoring**, **Packets**, then click **UMB cast (RX)**. The *Rx Packets Analysis* screen opens.



2. Click the **Clear** button to clear all statistics counters on this screen.
3. Click the arrow button to open the **Time Interval** list, then select the desired setting between 1s and 60s, where **s** stands for seconds. The default value is one second.
4. Click the arrow button to open the **Record Number** list, then select number of times the Switch will be polled between 20 and 200. The default value is 20.
5. Click the **Unicast** checkbox to see the total number of good packets that were received by a unicast address.
6. Click the **Multicast** checkbox to see the total number of good packets that were received by a multicast address.

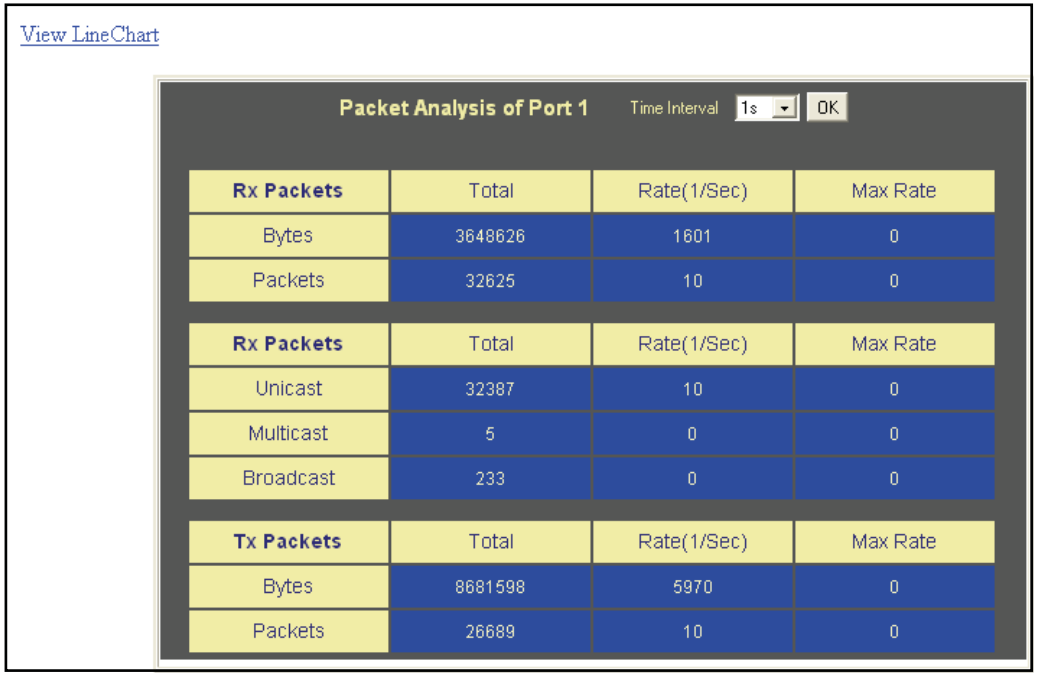
7 Click the **Broadcast** checkbox to see the total number of good packets that were received by a broadcast address.

8 Click **Apply**.

To view Unicast, Multicast, and Broadcast packets received statistics in table form:

1 In the left pane, click **Monitoring**, **Packets**, then click **UMB cast (RX)**. The *Rx Packets Analysis* screen opens.

2 Click **View Table**.



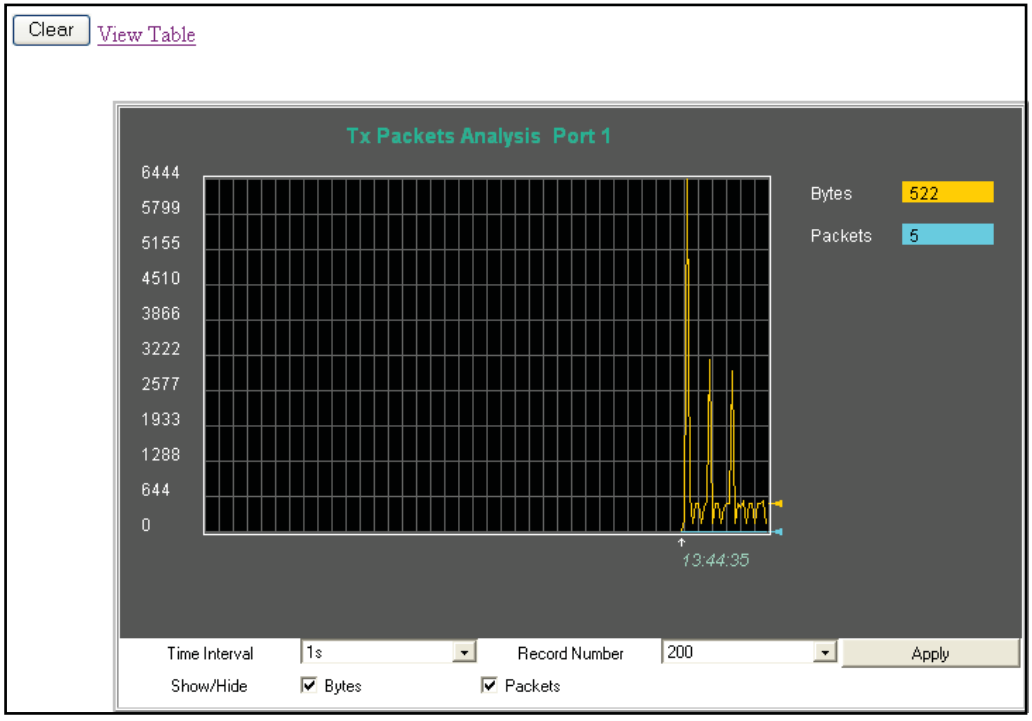
3 Click the arrow button to open the **Time Interval** list, then select the desired setting between 1s and 60s, where **s** stands for seconds. The default value is one second.

4 Click **OK**.

Viewing Transmitted (TX) packet statistics

To view packets transmitted statistics in graph form:

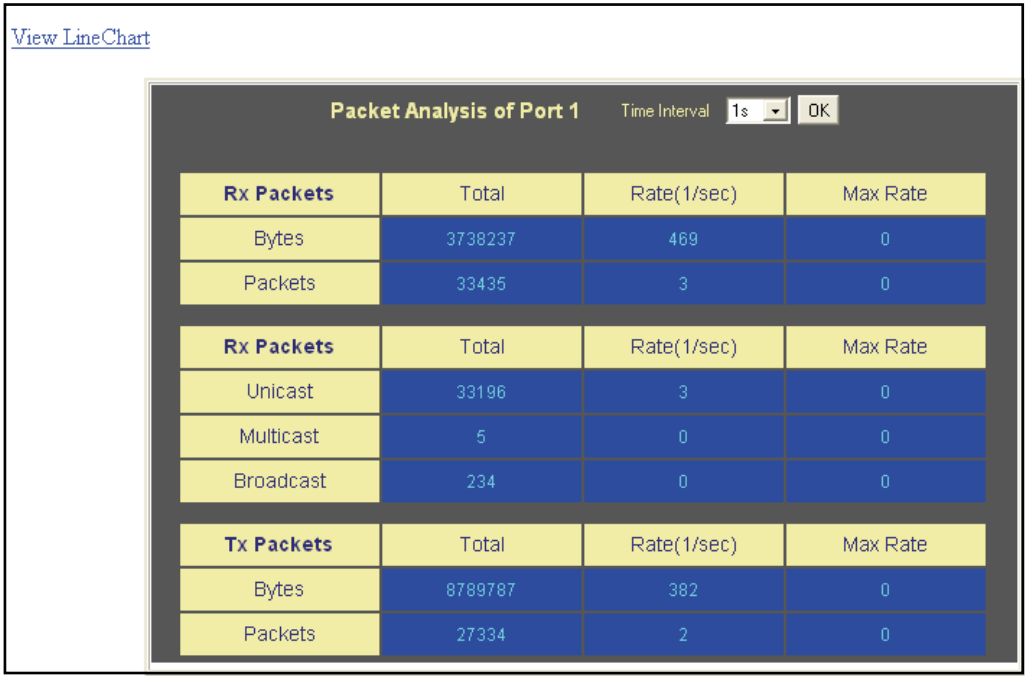
1. In the left pane, click **Monitoring**, **Packets**, then click **Transmitted (TX)**. The *Tx Packets Analysis* screen opens.



2. Click the **Clear** button to clear all statistics counters on this screen.
3. Click the arrow button to open the **Time Interval** list, then select the desired setting between 1s and 60s, where **s** stands for seconds. The default value is one second.
4. Click the arrow button to open the **Record Number** list, then select number of times the Switch will be polled between 20 and 200. The default value is 20.
5. Click the **Bytes** checkbox to see the number of bytes successfully sent on the port.
6. Click the **Packets** checkbox to see the number of packets successfully sent on the port.
7. Click **Apply**.

To view packets transmitted statistics in table form:

1. In the left pane, click **Monitoring**, **Packets**, then click **Transmitted (TX)**. The *Tx Packets Analysis* screen opens.
2. Click **View Table**.



3. Click the arrow button to open the **Time Interval** list, then select the desired setting between 1s and 60s, where **s** stands for seconds. The default value is one second.
4. Click **OK**.

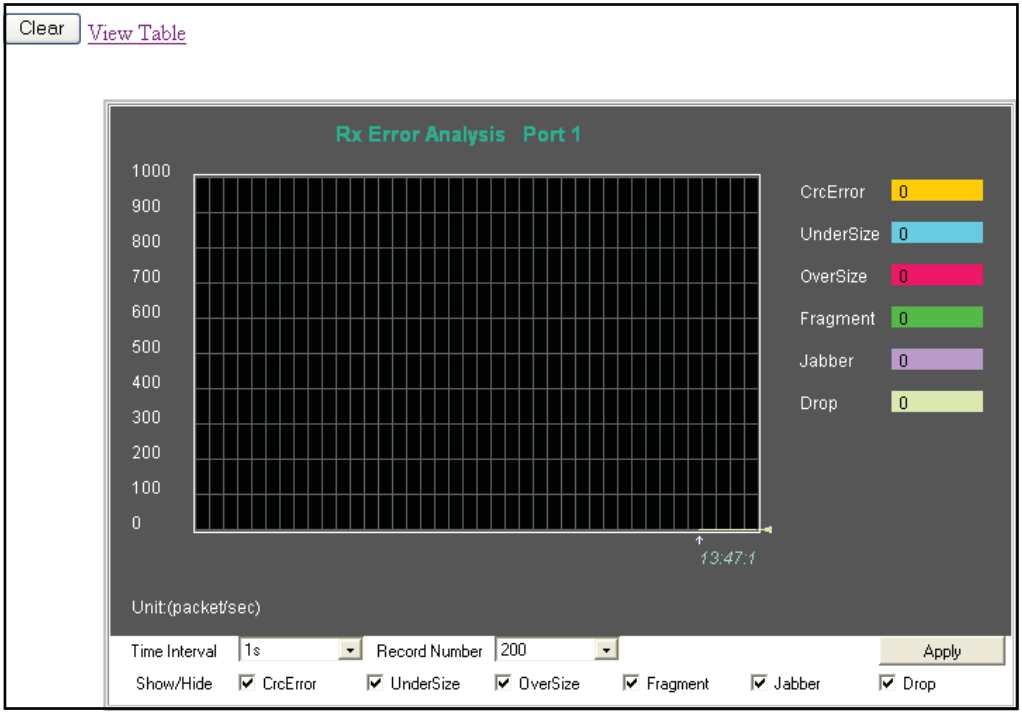
Viewing errors

You can view port error statistics compiled by the switch's management agent to be viewed as either a line graph or a table.

Viewing errors Received (RX)

To view errors received in graph form:

1. In the left pane, click **Monitoring**, **Errors**, then click **Received (RX)**. The *Rx Error Analysis* screen opens.



2. Click the **Clear** button to clear all statistics counters on this screen.
3. Click the arrow button to open the **Time Interval** list, then select the desired setting between 1s and 60s, where **s** stands for seconds. The default value is one second.
4. Click the arrow button to open the **Record Number** list, then select number of times the Switch will be polled between 20 and 200. The default value is 20.
5. Click the **CrcError** checkbox to count otherwise valid frames that did not end on a byte (octet) boundary.

6 Click the **UnderSize** checkbox to see the number of frames detected that are less than the minimum permitted frame size of 64 bytes and have a good CRC. Undersize frames usually indicate collision fragments, a normal network occurrence.

7 Click the **OverSize** checkbox to count packets received that were longer than 1518 octets, or if a VLAN frame 1522 octets, and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1522.

8 Click the **Fragment** checkbox to see the number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions.

9 Click the **Jabber** checkbox to see the number of frames with lengths more than the MAX_PKT_LEN bytes. Internally, MAX_PKT_LEN is equal to 1522.

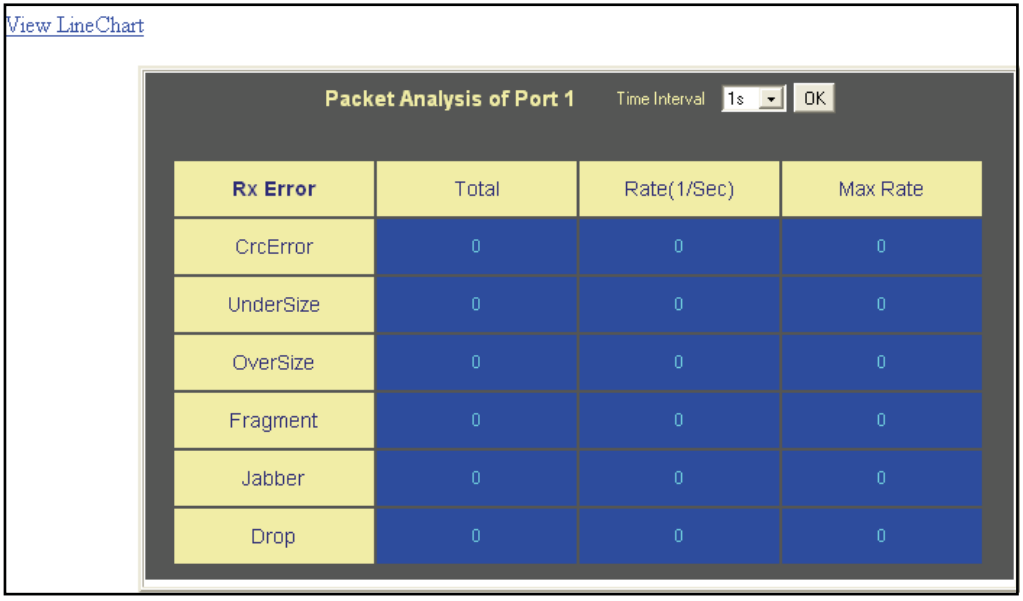
10 Click the **Drop** checkbox to see the number of frames that are dropped by this port since the last switch reboot.

11 Click **Apply**.

To view errors received in table form:

1 In the left pane, click **Monitoring**, **Errors**, then click **Received (RX)**. The *Rx Error Analysis* screen opens.

2 Click **View Table**.



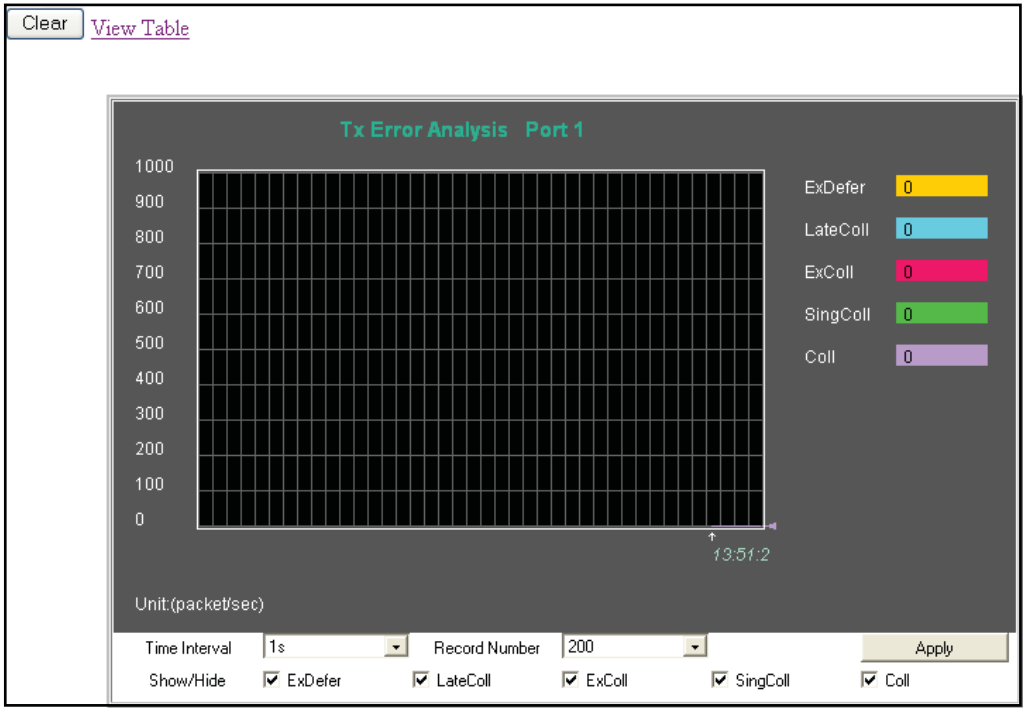
3 Click the arrow button to open the **Time Interval** list, then select the desired setting between 1s and 60s, where **s** stands for seconds. The default value is one second.

4 Click **OK**.

Viewing errors Transmitted (TX)

To view errors transmitted in graph form:

1 In the left pane, click **Monitoring**, **Errors**, then click **Transmitted (TX)**. The *Tx Error Analysis* screen opens.



2 Click the **Clear** button to clear all statistics counters on this screen.

3 Click the arrow button to open the **Time Interval** list, then select the desired setting between 1s and 60s, where **s** stands for seconds. The default value is one second.

4 Click the arrow button to open the **Record Number** list, then select number of times the Switch will be polled between 20 and 200. The default value is 20.

5 Click the **ExDefer** checkbox to count the number of frames for which the first transaction attempt on a particular interface was delayed because the medium was busy.

6 Click the **LateColl** checkbox to count the number of times that a collision is detected later than 512 bit-times into the transmission of a packet.

7 Click the **ExColl** checkbox to count the number of frames for which transmission failed due to excessive collisions.

8 Click the **SingColl** checkbox to count the number of successfully transmitted frames for which transmission is inhibited by more than one collision.

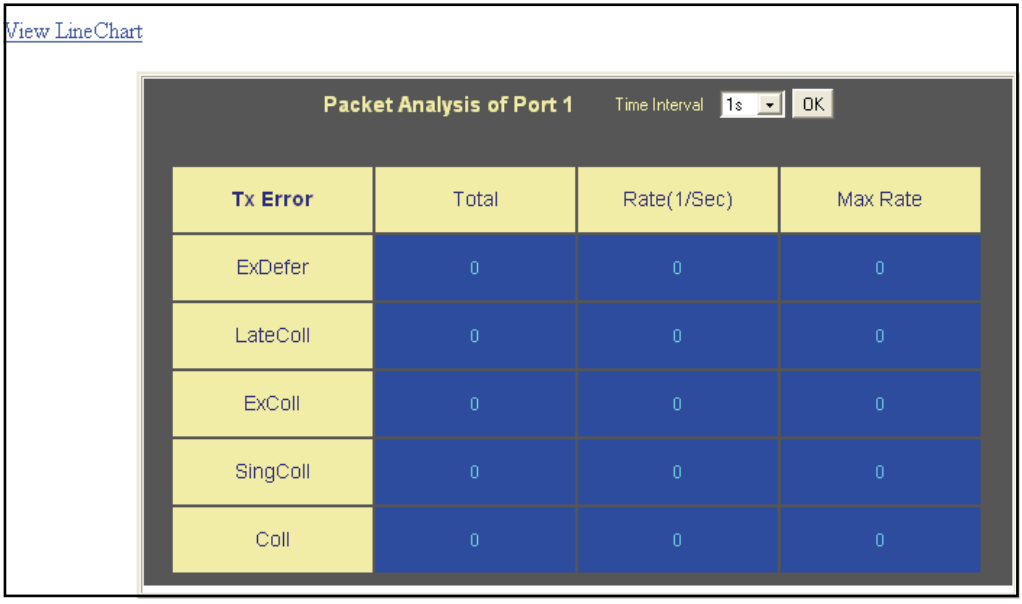
9 Click the **Coll** checkbox to see an estimate of the total number of collisions on this network.

10 Click **Apply**.

To view errors transmitted in table form:

1 In the left pane, click **Monitoring**, **Errors**, then click **Transmitted (TX)**. The *Tx Error Analysis* screen opens.

2 Click **View Table**.



3 Click the arrow button to open the **Time Interval** list, then select the desired setting between 1s and 60s, where **s** stands for seconds. The default value is one second.

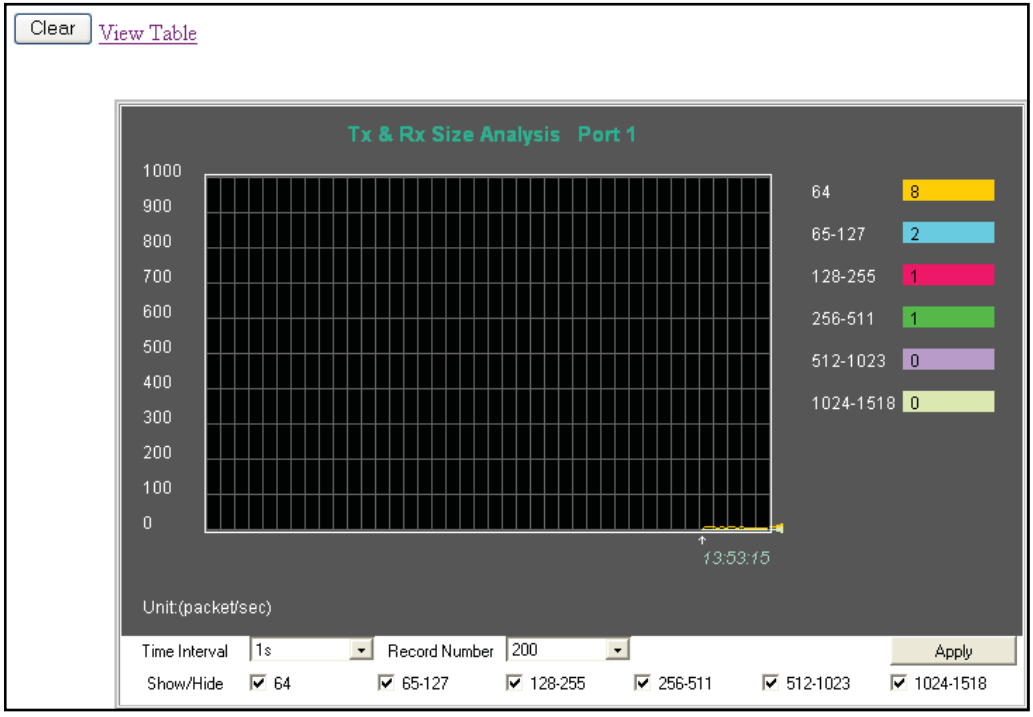
4 Click **OK**.

Viewing packet size

You can view the size of packets received by the switch, arranged in six groups, to be viewed as either a line graph or a table.

To view packet size in graph form:

1 In the left pane, click **Monitoring**, **Size**, then click **Packet Size**. The *Rx Size Analysis* screen opens.



2 Click the **Clear** button to clear all statistics counters on this screen.

3 Click the arrow button to open the **Time Interval** list, then select the desired setting between 1s and 60s, where **s** stands for seconds. The default value is one second.

4. Click the arrow button to open the **Record Number** list, then select number of times the Switch will be polled between 20 and 200. The default value is 20.

5. Click the **64** checkbox to count the total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).

6. Click the **65-127** checkbox to count the total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).

7. Click the **128-255** checkbox to count the total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).

8. Click the **256-511** checkbox to count the total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).

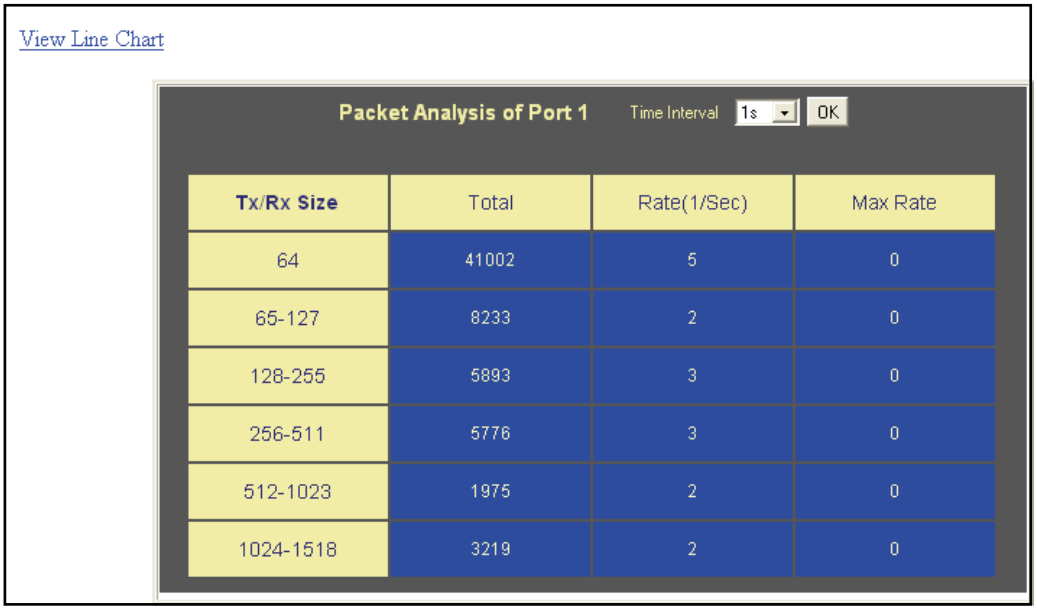
9. Click the **512-1023** checkbox to count the total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).

10. Click the **1024-1518** checkbox to count the total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

11. Click **Apply**.

To view packet size in table form:

1. In the left pane, click **Monitoring**, **Size**, then click **Packet Size**. The *Rx Size Analysis* screen opens.
2. Click **View Table**.



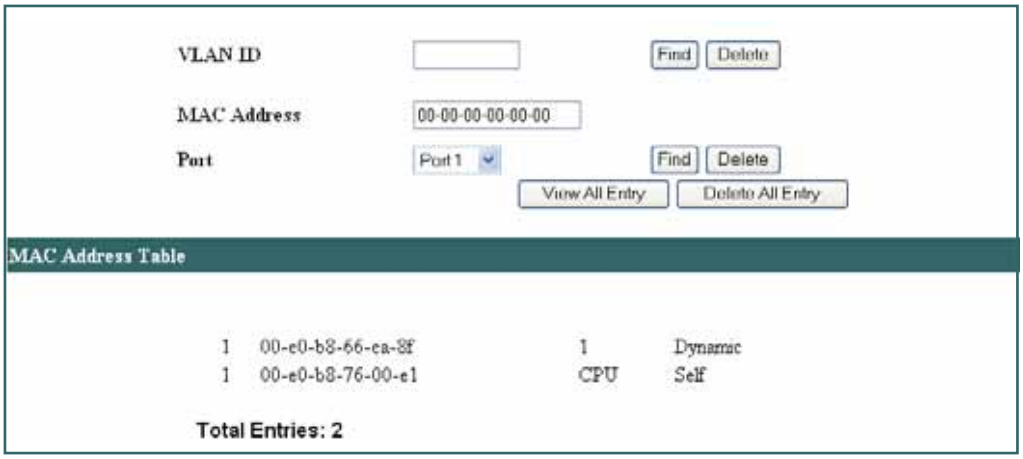
3. Click the arrow button to open the **Time Interval** list, then select the desired setting between 1s and 60s, where **s** stands for seconds. The default value is one second.
4. Click **OK**.

Viewing the MAC address forwarding table

This screen allows the switch's dynamic MAC address forwarding table to be viewed. When the switch learns an association between a MAC address and a port number, it makes an entry into its forwarding table. These entries are then used to forward packets through the switch.

To view the MAC address forwarding table:

1 In the left pane, click **Monitoring**, then click **MAC Address**. The *MAC Address Table* screen opens.



2 Type a VLAN ID in the **VLAN ID** field for the forwarding table to be browsed by, then click **Find**.

-OR-

Type a MAC Address in the **MAC Address** field for the forwarding table to be browsed by, then click **Find**.

-OR-

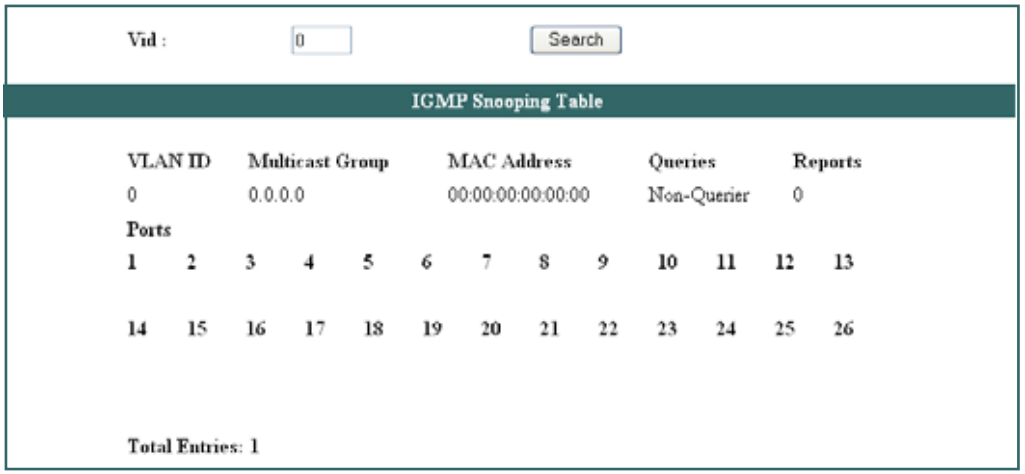
Click the arrow button to open the **Port** list, select the desired port to be browsed by, then click **Find**.

Viewing the IGMP Snooping Group

This screen allows the switch's IGMP Snooping table to be viewed. IGMP Snooping allows the switch to read the Multicast Group IP address and the corresponding MAC address from IGMP packets that pass through the switch. The number of IGMP reports that were snooped is displayed in the **Reports** field.

To view the IGMP Snooping table:

1. In the left pane, click **Monitoring**, then click **IGMP Snooping Group**. The *IGMP Snooping Table* screen opens.

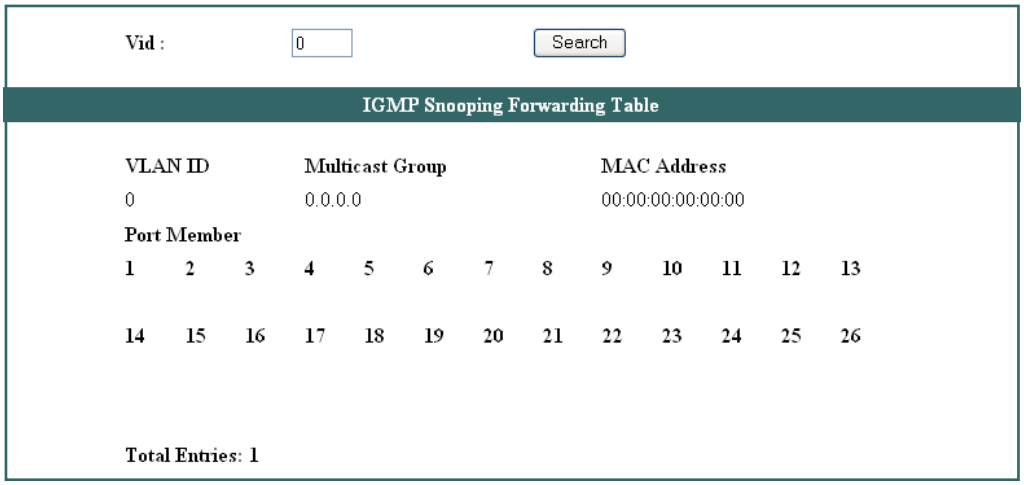


2. Type the VLAN ID for the desired IGMP Snooping Group Table in the **Vid** field, then click **Search**.

Viewing IGMP Snooping forwarding table

To view the IGMP Snooping forwarding table:

1 In the left pane, click **Monitoring**, then click **IGMP Snooping Forwarding**. The *IGMP Snooping Forwarding Table* screen opens.

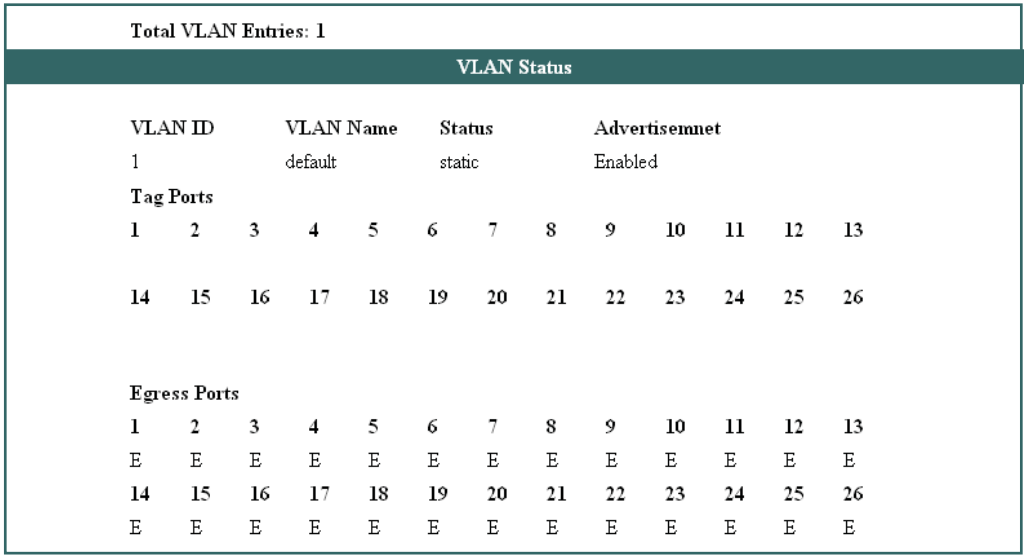


2 Type the VLAN ID for the desired IGMP Snooping Forwarding Table in the **Vid** field, then click **Search**.

Viewing VLAN status

To view the current VLAN configuration:

- In the left pane, click **Monitoring**, then click **VLAN Status**. The *VLAN Status* screen opens.

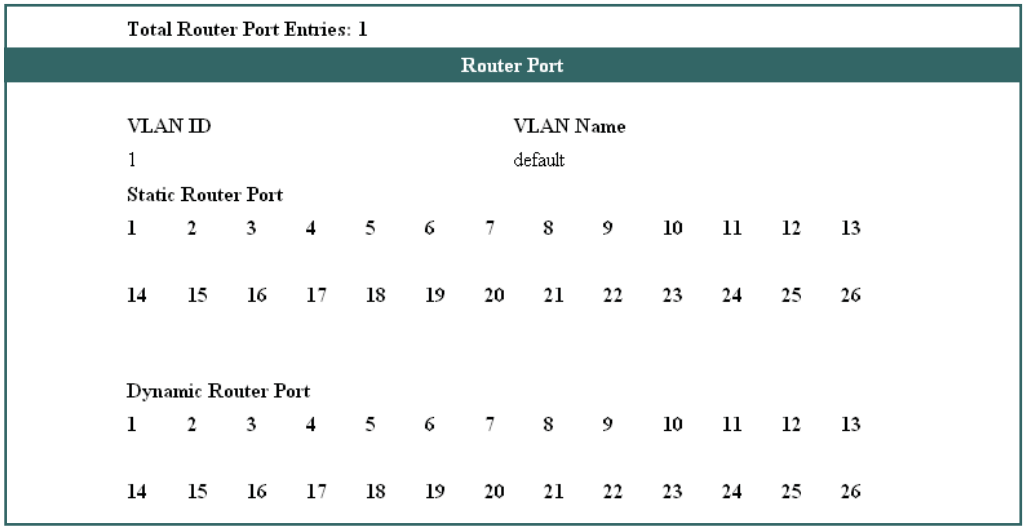


Viewing router port

This screen displays which of the switch's ports are currently configured as router ports. A router port configured by a user (using the console or Web-based management interfaces) is displayed as a static router port in the first two rows of the *Router Port* screen. A router port that is dynamically configured by the switch is located in the third and fourth rows. Static router ports are configured by the user and dynamically assigned router ports are configured by the switch.

To view the Router Port table:

- In the left pane, click **Monitoring**, then click **Router Port**. The *Router Port* screen opens.



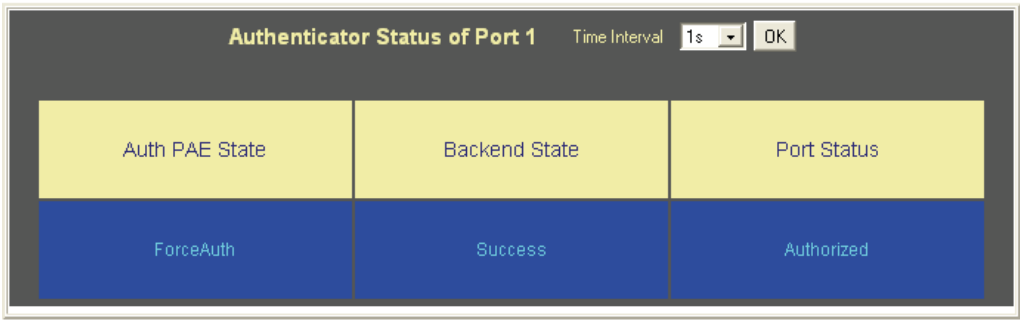
Viewing port access control information

Viewing authenticator state

This screen displays port access control information.

To view port access control information:

1. In the left pane, click **Monitoring**, **Port Access Control**, then click **Authenticator State**. The *Authenticator Status* screen opens.



2. Click the arrow button to open the **Time Interval** list, then select the desired setting between 1s and 60s, where **s** stands for seconds. The default value is one second.
3. Click **OK**.

Maintenance

Use the screen and folders contained in the **Maintenance** folder to maintain the switch. The hyperlinked screens and folders contained in the **Maintenance** folder include:

- TFTP Services - See “Using TFTP services” on page 143
  - Download Firmware from TFTP Server - See “Downloading firmware from a TFTP server” on page 144
  - Download Settings from TFTP Server - See “Downloading settings from a TFTP server” on page 144
  - Upload Settings to TFTP Server - See “Uploading settings to a TFTP server” on page 145
  - Upload Log to TFTP Server - See “Uploading a log to a TFTP server” on page 145
- Switch History - See “Viewing switch history” on page 146
- Ping Test - See “Performing a Ping test” on page 147
- Save Changes - See “Saving changes” on page 147
- Reboot Services - See “Rebooting the switch” on page 147
  - Reboot - See “Restarting the switch” on page 49
  - Reset - See “Resetting the switch” on page 48
  - Reset System - See “Resetting the switch” on page 48
  - Reset Configuration - See “Resetting the switch” on page 48
- Logout - See “Logging out” on page 148

Using TFTP services

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

Important

The TFTP server must be running TFTP server software to perform the file transfer. TFTP server software is a part of many network management software packages (such as NetSight) or can be obtained as a separate program.

Downloading firmware from a TFTP server

To update the switch's firmware:

1 In the left pane, click **Maintenance**, **TFTP Services**, then click **Download Firmware from TFTP Server**. The *Download Firmware from TFTP Server* screen opens.

2 Type the IP address of the TFTP server in the **Server IP Address** field. The TFTP server must be on the same IP subnet as the switch.

3 Type the path and the filename to the firmware file on the TFTP server in the **File Name** field.

Tips & Tricks

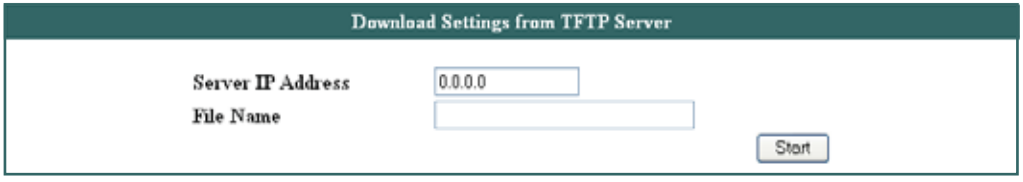
Use **Save Changes** from the **Maintenance** folder to enter the address into NV-RAM.

4 Click **Start**.

Downloading settings from a TFTP server

To download a configuration file for the switch:

1 In the left pane, click **Maintenance**, **TFTP Services**, then click **Download Settings from TFTP Server**. The *Download Firmware from TFTP Server* screen opens.



2 Type the IP address of the TFTP server in the **Server IP Address** field. The TFTP server must be on the same IP subnet as the switch.

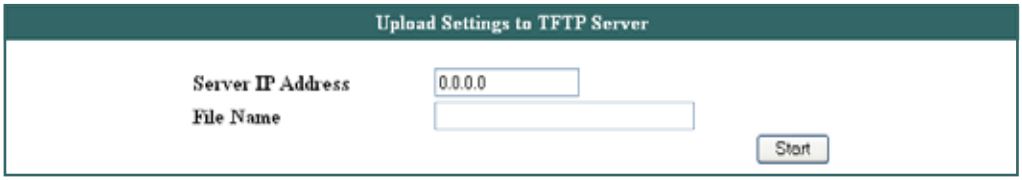
3 Type the path and the filename to the switch configuration file on the TFTP server in the **File Name** field.

4 Click **Start**.

Uploading settings to a TFTP server

To upload a configuration file for the switch:

1 In the left pane, click **Maintenance**, **TFTP Services**, then click **Upload Settings to TFTP Server**. The *Upload Firmware to TFTP Server* screen opens.



2 Type the IP address of the TFTP server in the **Server IP Address** field. The TFTP server must be on the same IP subnet as the switch.

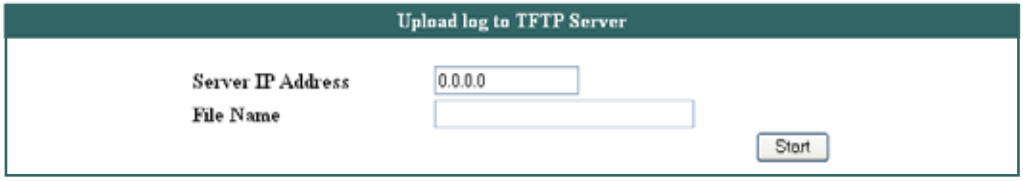
3 Type the path and the filename to the settings file on the TFTP server in the **File Name** field.

4 Click **Start**.

Uploading a log to a TFTP server

To upload the history log for the switch:

1 In the left pane, click **Maintenance**, **TFTP Services**, then click **Upload Log to TFTP Server**. The *Upload Log to TFTP Server* screen opens.



2 Type the IP address of the TFTP server in the **Server IP Address** field. The TFTP server must be on the same IP subnet as the switch.

3 Type the path and the filename to the history file on the TFTP server in the **File Name** field.

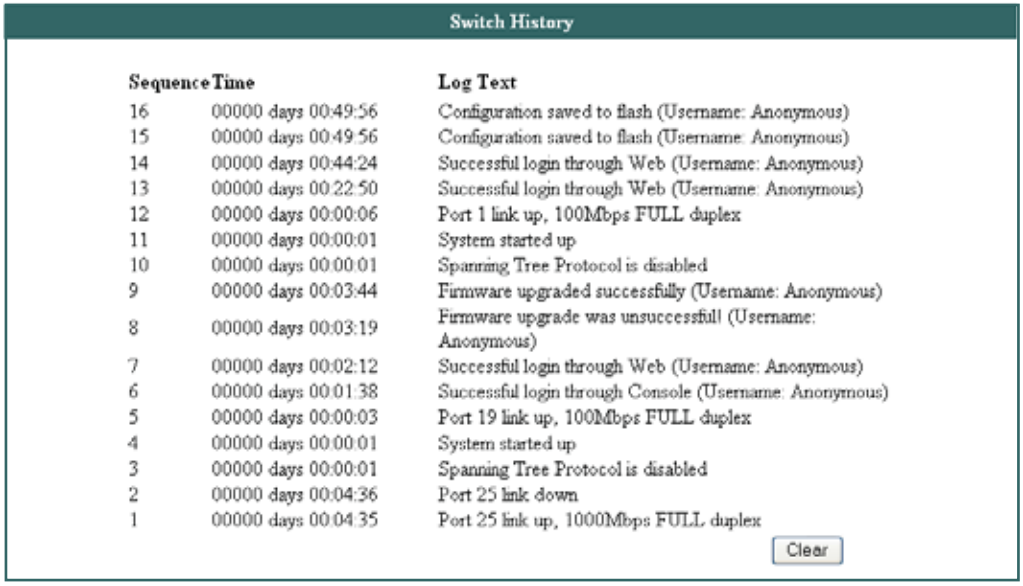
4 Click **Start**.

Viewing switch history

This screen allows the *Switch History* log to be viewed. The switch records all traps, in sequence, that identify events on the switch. The time since the last cold start of the switch is also recorded.

To view the history log for the switch:

- In the left pane, click **Maintenance**, then click **Switch History**. The *Switch History* screen opens.

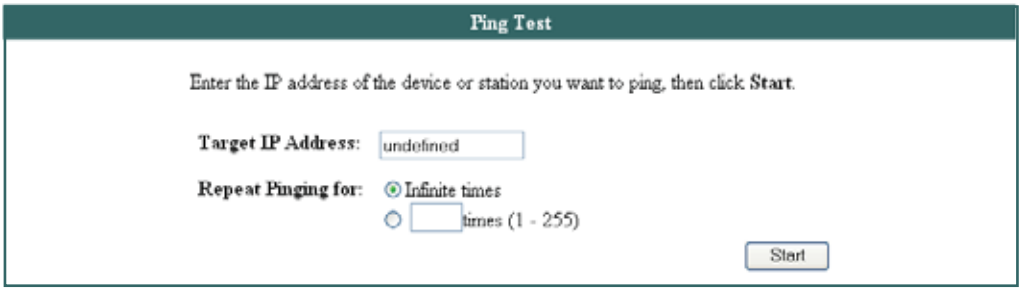


Performing a Ping test

PING is a small program that sends data packets to the IP address you specify. The destination node then returns the packets to the switch. This is very useful to verify connectivity between the switch and other nodes on the network.

To perform a Ping test:

1. In the left pane, click **Maintenance**, then click **Ping Test**. The *Ping Test* screen opens.



The following fields can be set on this screen:

2. Type the IP Address of the network node in the **Target IP Address** field.
3. Click to repeat the Pinging for **Infinte times** or a specified number of times. If you clicked to specify the number of times, type a number between 1 and 255 in the field provided.
4. Click **Start**.

Saving changes

For more information, see “Saving changes” on page 47.

Rebooting the switch

For more information, see “Resetting the switch” on page 48 and “Restarting the switch” on page 49.

Logging out

To logout of the Web configuration program:

1. In the left pane, click **Maintenance**, then click **Logout**. The *Logout Web Setup* screen opens.

2. Click the **Apply** button.

Chapter 5

Technical Support

Telephone numbers

Gateway offers a wide range of customer service, technical support, and information services. You can access the following services through your telephone to get answers to your questions:

Resource	Service description	How to reach
Fax on demand support	Order a catalog of documents on common problems, then order documents by document numbers. The documents will be faxed to you.	800-846-4526 (US) 877-709-2951 (Canada)
Gateway's fee-based software tutorial service	Get tutorial assistance for software issues billed by the minute.	800-229-1103 (charged to your credit card) 900-555-4695 (charged to your telephone bill)
Gateway Technical Support	Talk to a Gateway Technical Support representative about a non-tutorial technical support question.) TDD Technical Support (for hearing impaired) is available: Weekdays 6:00 a.m. - 8:00 p.m. Central Time Weekends 6:00 a.m. - 5:00 p.m. Central Time	877-485-1464 (US) 800-846-3609 (Canada and Puerto Rico 605-232-2191 (all other countries) 800-846-1778 (TDD)
Sales, accounting, and warranty	Get information about available systems, pricing, orders, billing statements, warranty service, or other non-technical issues.	800-846-2000 (US) 888-888-2037 (Canada)

Appendix A

Safety, Regulatory, and Legal Information

- Important safety information
- Regulatory compliance statements
- Notices

Important safety information

Your Gateway switch is designed and tested to meet the latest standards for safety of information technology equipment. However, to ensure safe use of this product, it is important that the safety instructions marked on the product and in the documentation are followed.

Warning

Always follow these instructions to help guard against personal injury and damage to your Gateway switch.

Setting up your switch

- Read and follow all instructions marked on the product and in the documentation before you operate your switch. Retain all safety and operating instructions for future use.
- Do not use this product near water or a heat source such as a radiator.
- Set up the switch on a stable work surface.
- The product should be operated only from the type of power source indicated on the rating label.
- Openings in the case are provided for ventilation. Do not block or cover these openings. Make sure you provide adequate space, at least 6 inches (15 cm), around the system for ventilation when you set up your work area. Never insert objects of any kind into the ventilation openings.
- Some products are equipped with a three-wire power cord to make sure that the product is correctly grounded when in use. The plug on this cord will fit only into a grounding-type outlet. This is a safety feature. If you are unable to insert the plug into an outlet, contact an electrician to install the appropriate outlet.
- If you use an extension cord with this switch, make sure that the total ampere rating on the products plugged into the extension cord does not exceed the extension cord ampere rating.

General precautions for rack-mountable products

Observe the following precautions for rack stability and safety. Also refer to the rack installation documentation accompanying the system and the rack for specific caution statements and procedures.

Systems are considered to be components in a rack. Thus, “component” refers to any system as well as to various peripherals or supporting hardware.

Warning

High voltages can enter your computer through both the power cord and the modem connection. Protect your computer by using a surge protector. If you have a telephone modem, use a surge protector that has a modem jack. If you have a cable modem, use a surge protector that has an antenna/cable jack. During an electrical storm, unplug both the surge protector and the modem.

Before working on the rack, make sure that the stabilizers are secured to the rack, extended to the floor, and that the full weight of the rack rests on the floor. Install front and side stabilizers on a single rack or front stabilizers for joined multiple racks before working on the rack.

Always load the rack from the bottom up, and load the heaviest item in the rack first.

Make sure that the rack is level and stable before extending a component from the rack.

Use caution when pressing the component rail release latches and sliding a component into or out of a rack; the slide rails can pinch your fingers.

After a component is inserted into the rack, carefully extend the rail into a locking position, and then slide the component into the rack.

Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.

Ensure that correct airflow is provided to components in the rack.

Do not step on or stand on any component when servicing other components in a rack.

Important

A qualified electrician must perform all connections to DC power and to safety grounds. All electrical wiring must comply with applicable local or national codes and practices.

Warning

Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

Warning

The switch chassis must be positively grounded to the rack cabinet frame. Do not attempt to connect power to the switch until grounding cables are connected. Completed power and safety ground wiring must be inspected by a qualified electrical inspector. An electrical hazard will exist if the safety ground cable is omitted or disconnected.

Preventing static electricity discharge

The components inside your computer are extremely sensitive to static electricity, also known as *electrostatic discharge* (ESD).

Warning

ESD can permanently damage electrostatic discharge-sensitive components in your computer. Prevent ESD damage by following ESD guidelines every time you open the computer case.

Warning

To avoid exposure to dangerous electrical voltages and moving parts, turn off your computer and unplug the power cord and modem and network cables before opening the case.

Before opening the computer case, follow these guidelines:

- Turn off your computer.
- Wear a grounding wrist strap (available at most electronics stores) and attach it to a bare metal part of your computer.

Warning

To prevent risk of electric shock, do not insert any object into the vent holes of the power supply.

- Touch a bare metal surface on the back of the computer.
- Unplug the power cord and the modem and network cables.

Before working with computer components, follow these guidelines:

- Avoid static-causing surfaces such as carpeted floors, plastic, and packing foam.

- Remove components from their antistatic bags only when you are ready to use them. Do not lay components on the outside of antistatic bags because only the inside of the bags provide electrostatic protection.
- Always hold expansion cards by their edges or their metal mounting brackets. Avoid touching the edge connectors and components on the cards. Never slide expansion cards or components over any surface.

Care during use

- Do not walk on the power cord or allow anything to rest on it.
- Do not spill anything on the switch. The best way to avoid spills is to avoid eating and drinking near your switch.
- When a computer is turned off, a small amount of electrical current still flows through it. To avoid electrical shock, always unplug all power cables and modem cables from the wall outlets before cleaning the switch.
- Unplug the switch from the wall outlet and refer servicing to qualified personnel if:
- The power cord or plug is damaged.
- Liquid has been spilled into the switch
- The switch does not operate correctly when the operating instructions are followed.
- The switch was dropped or the case is damaged.
- The switch performance changes.

Replacement parts and accessories

Use only replacement parts and accessories recommended by Gateway.

Important

Do not use Gateway products in areas classified as hazardous locations. Such areas include patient care areas of medical and dental facilities, oxygen-laden environments, or industrial facilities.

Warning

To reduce the risk of fire, use only No. 26 AWG or larger telecommunications line cord.

Regulatory compliance statements

United States of America

Federal Communications Commission (FCC)
Unintentional emitter per FCC Part 15

This device has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio or television reception. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause interference to radio and television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment to an outlet on a different circuit from that to which the receiver is connected

- Consult the dealer or an experienced radio/TV technician for help.

Compliance Accessories: The accessories associated with this equipment are: shielded video cable when an external monitor is connected. These accessories are required to be used in order to ensure compliance with FCC rules.

FCC declaration of conformity

Responsible party:

Gateway Companies, Inc.
610 Gateway Drive, North Sioux City, SD 57049
(605) 232-2000 Fax: (605) 232-2023

Products:

- Gateway 7601-24.2
- Gateway 7601-48.2
- Gateway 7801-24.4
- Gateway 7801-48.4

For unique identification of the product configuration, please submit the 10-digit serial number found on the product to the responsible party.

This device complies with Part 15 of the FCC Rules. Operation of this product is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Caution

Changes or modifications not expressly approved by Gateway could void the FCC compliance and negate your authority to operate the product.

Canada

Industry Canada (IC)
Unintentional emitter per ICES-003

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus as set out in the radio interference regulations of Industry Canada.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de Classe B prescrites dans le règlement sur le brouillage radioélectrique édicté par Industrie Canada.

Warning

To avoid electrical shock or equipment malfunction do not attempt to make electrical ground connections by yourself. Contact the appropriate inspection authority or an electrician, as appropriate.

California Proposition 65 Warning

Warning

This product contains chemicals, including lead, known to the State of California to cause cancer, birth defects or reproductive harm.

Notices

Copyright © 2004 Gateway, Inc.
All Rights Reserved
14303 Gateway Place
Poway, CA 92064 USA

All Rights Reserved

This publication is protected by copyright and all rights are reserved. No part of it may be reproduced or transmitted by any means or in any form, without prior consent in writing from Gateway.

The information in this manual has been carefully checked and is believed to be accurate. However, changes are made periodically. These changes are incorporated in newer publication editions. Gateway may improve and/or change products described in this publication at any time. Due to continuing system improvements, Gateway is not responsible for inaccurate information which may appear in this manual. For the latest product updates, consult the Gateway Web site at www.gateway.com. In no event will Gateway be liable for direct, indirect, special, exemplary, incidental, or consequential damages resulting from any defect or omission in this manual, even if advised of the possibility of such damages.

In the interest of continued product development, Gateway reserves the right to make improvements in this manual and the products it describes at any time, without notices or obligation.

Trademark Acknowledgments

Gateway and the Black-and-White Spot Design are trademarks or registered trademarks of Gateway, Inc. in the U.S. and other countries. SpotShop, Spotshop.com, and Your:)Ware are trademarks of Gateway, Inc. Intel, Intel Inside logo, and Pentium are registered trademarks and MMX is a trademark of Intel Corporation. Microsoft, MS, MS-DOS, and Windows are trademarks or registered trademarks of Microsoft Corporation. All other product names mentioned herein are used for identification purposes only, and may be the trademarks or registered trademarks of their respective companies.

Index

A

Acceptable Frame Type
  field 75
Access ID
  field 98
access profile
  adding rule 97
  masking 28
  using 92
Access Profile Configuration
  screen 93, 95
Access Profile Table
  screen 93, 94, 97, 99
Access Right
  field 45, 116
Access Rule Configuration
  screen 98
Access Rule Table
  screen 97, 99, 100
accessories
  safety precautions 154
Accounting Method
  field 109
Accounting Port
  field 108
Act
  LED indicator 9
active group
  port group configuration 31
adding
  access profile rule 97
  Ethernet access profile mask 93
  Internet access profile mask 94
  multicast forwarding 68
  SNMP Community Table entries 115
  SNMP Group Table entries 113
  SNMP Host Table entries 118
  SNMP User Table entries 119
  SNMP View Table entries 111
  switch to stack 21
  unicast forwarding 66
  user 45
AdmDir
  field 104
Admin privileges 45
Admin State
  field 53, 81
advanced switch information
  setting 55
Advertisement
  field 72
agent 25
aging time
  MAC address 28
Allowed to Go Port
  field 67
assigning
  default priority 83
  user priority 84
Asymmetric VLAN
  field 56
  support 2, 36
attaching rubber feet 5
Auth PAE State
  field 106
Auth State
  field 107
Authentic Port
  field 108
authentication level
  HMAC-MDA-96 26
  HMAC-SHA-96 26
authenticator state
  viewing 142
Authenticator Status
  screen 142
Auth-Protocol
  field 120
Automated troubleshooting system 150
Auto-MDIX 2

B

Backend State
  field 106, 107
Bandwidth Settings
  screen 75

basic switch information
setting 53
viewing 53
baud rate
console port 16
Boot PROM 53
Boot PROM Version
field 54
BOOTP 23, 51, 52
BPDU packets 29
Bridge Forward Delay (4-30 sec)
field 64
Bridge Hello Time (1-10 Sec)
field 64
Bridge Max Age (6-40 Sec)
field 64
Bridge Priority (0- 65535 Sec)
field 64
Broadcast
checkbox 127
Broadcast Storm
field 85
Bytes
checkbox 125, 128

C

Capability
field 106
CFI (Canonical Format Identifier) 33
changes
saving 47
changing
switch stack 19
See also modifying
Class of Service 82, 84
Class of Traffic 84
CLI command
config ipif System ipaddress 24
config stacking mode 13, 17, 18, 19, 20
download configuration 23
show stacking 18
Coll
checkbox 133
Community Name
field 116
Community String/SNMPv3 User Name
field 118
community strings 25
components
identifying 7
configuration
console port 16
configuration mode
auto 17
disabled 18
enabled 17
master 18
slave 18
configuring
IEEE 802.1x port settings 103
IGMP snooping 59
individual switch ports 56
port capability settings 105
Spanning Tree Protocol 63, 65
static router port settings 61
switch 42
Confirm Key
field 108
Confirm New Password
field 45
connecting
switch 11
switch to end node 12
switch to hub or switch 13
connection
in-band 16
out-of-band 16
console
LED indicators 9
console port
baud rate 16
configuration 16
data width 16
flow control 16
parity 16
stop bits 16
converting
standalone to switch stack 20
Cost
field 66
CRC (Cyclic Redundancy Check) 34
CrcError

checkbox 130
creating VLANs 71
Current IGMP Snooping Group Entries
screen 59, 60
Current Static Router Ports Entries
screen 62
Current Time
screen 77

D

data width
console port 16
Day
field 77
Daylight Saving Time
setting 78
Daylight Saving Time Offset in Minutes
field 78
Daylight Saving Time State
field 78
Default Gateway
field 53
default priority
assigning 83
deleting
multicast forwarding 69
SNMP Community Table entries 115
SNMP Group Table entries 113
SNMP Host Table entries 118
SNMP User Table entries 119
SNMP View Table entries 111
unicast forwarding 67
VLANs 71
desktop
installation 5
Destination IP Mask
field 95
Destination Lookup Fail
field 85
Destination MAC Mask
field 94
Device Type
field 54
DHCP 51, 52
diagnostic port 16
Download Firmware from TFTP Server
screen 144
downloading
firmware from a TFTP server 144
settings from a TFTP server 144
Drop
checkbox 131
Dscp
field 95
D-View 16, 25

E

Edge
field 66
edge port 30
egress port
defined 32
egress rules 33
electrostatic discharge (ESD) 153
enabling
LACP 89
Engine ID
field 117
errors
viewing 130
errors Received (RX)
viewing 130
errors Transmitted (TX)
viewing 132
Ethernet access profile mask
adding 93
modifying 93
Ethernet type
field 94
EtherType 34
ExColl
checkbox 133
ExDefer
checkbox 133
External Ports
field 54

F

Facility
field 101
fans
system 8

features 2
File Name
field 144, 145, 146
filtering 28
ingress 36
MAC address 28
routine packet 28
using 27, 66
firmware
downloading from a TFTP server 144
Firmware Version
field 54
number 53
flow control
console port 16
FlowCtrl
field 58
Forward Portlist
checkboxes 86
forwarding
rules 33
using 27, 66
Forwarding BPDU
field 64
Fragment
checkbox 131
From Day
field 79
From Day of Week
field 79
From Month
field 79
From Time in HH:MM
field 79
From Which Day
field 79
front panel
identifying components 7

G

GBIC port 20
Get IP From
field 52
Group
field 85
group ID
multicast 37
Group ID (1-6)
field 91
Group Name
field 114, 120
groups
multicast 37
GVRP (GARP VLAN Registration Protocol)
field 74
switches 73
turning on 55
GVRP Status
field 55

H

Hardware Version
field 54
Hello Time 64
HMAC-MDA-96 authentication level 26
HMAC-SHA-96 authentication level 26
Host IP Address
field 118
Host Timeout
field 61
HP OpenView 16
HyperTerminal 16

I

ID
multicast group 37
identifying components
front panel 7
rear panel 8
side panels 8
IEEE 802.1ad
link aggregation 31
IEEE 802.1d
compatibility 30
legacy equipment 29
IEEE 802.1p
Default Priority Settings screen 83
field 94
priority queues 2
using priority queuing (QoS) 81
IEEE 802.1Q
Port Settings screen 74

Static VLANs screen 71, 73
VLAN 2, 32
VLAN packet forwarding 33
VLAN tags 33
IEEE 802.1w
compatibility 30
Rapid Spanning Tree 3, 29
IEEE 802.1x
Authenticator Settings screen 103, 104
Capability Settings screen 105
configuring port settings 103
Port-based Network Access Control 102
support 3
IEEE 802.1x Authentication Protocol
field 56
IEEE 802.1x Status
field 56
IEEE 802.3ad
LACP 89
IEEE 802.3x
compliance 2
IEEE 802.3z
compliance 2
IGMP (Internet Group Management Protocol)
queries 61
report 39
report packets 61
snooping 2, 59
type codes 39
using 38, 59
versions 38
IGMP Snooping
field 55
IGMP Snooping Forwarding Table
screen 139
viewing 139
IGMP Snooping Group
viewing 138
IGMP Snooping Settings
screen 60
IGMP Snooping Table
screen 138
in-band connection 16
Index
field 101
indicators
LED 9
individual switch ports
configuring 56
Ingress
field 74
ingress
filtering 36
port 32
rules 33
Initialize Port
screen 106
Initialize Port Table 106
initializing ports 106
installing
in rack 5
on desktop 5
on shelf 5
Internet access profile mask
adding 94
modifying 94
Internet Control Message Protocol (ICMP)
field 95
Internet Group Management Protocol (IGMP)
field 96
IP Access to Switch
field 110
IP Address
default switch address 23
field 52
Multicast Group 55
setting 24, 51
switch 23, 27
IP Address Settings
screen 51, 52

J

Jabber
checkbox 131

K

Key
field 108

L

LACP (Link Aggregation Control Protocol)
enabling 89

link aggregation 31
using 89
LACP Port Settings
screen 89
Last Member Query Interval
field 60
LateColl
checkbox 133
leave message 39
leave report 39
Leave Timer
field 61
LED indicators 6, 7, 9, 12
Act 9
console 9
Link 9
power 9
RPS 9
Speed 9
Link
LED indicator 9
link aggregation
LACP 31
static 31
using 90
Link Aggregation Algorithm
field 56
Link Aggregation Settings
screen 91
local console management 16
Lock Address Mode
field 81
log
uploading to a TFTP server 145
logging out 148
Logout Web Setup
screen 148

M

MAC Address
aging time 28
field 54, 67, 106, 107, 137
filtering 28
finding 24
setting port security 80
MAC Address Aging Time
field 55
MAC Address Forwarding table
forwarding filtering 66
viewing 137
MAC Address Table
screen 137
MAC Notification Global Settings
screen 87, 88
management 3
concepts 15
local console 16
Web-based 16
Management Information Base (MIB)
using 26, 27
Management Station IP Addresses table 53
managing
switch stacks 19
traffic control 85
traffic segmentation 86
user accounts 45
Master Port
defined 90
field 91
master switch
swapping 23
Max Learning Address.(0-10)
field 81
Max Response Time
field 60
Max. Latency (0-255)
field 82
Max. Packets (O-255)
field 82
MaxReq
field 104
Member Port
checkboxes 91
field 62
Migration
field 66
Mode
field 70, 90, 94, 96
modifying
Ethernet access profile mask 93
Internet access profile mask 94
multicast forwarding 68

Multicast Port Filtering Mode 70
Port VLAN ID (PVID) settings 73
SNMP Engine ID 117
unicast forwarding 66
VLANs 71
Month
field 77
mounting brackets
installing 5
mounting kit
unpacking 4
Multicast
checkbox 126
multicast forwarding
adding 68
deleting 69
modifying 68
Multicast Group
ID 37
IP address 55
using 37
Multicast MAC Address
field 69
Multicast Port Filtering Mode Setup
screen 70
Multicast Storm
field 85
multicasting 37
Multi-layer ACL 2

N

NetSight 143
Network Time Protocol (NPT) 76
New Password
field 45
No Limit
field 76
Notify View Name
field 114
NV-RAM 47, 144
NWay Ethernet ports 2, 7

O

Object Identifier (OID) 26, 27
Oper Dir
field 107
OSI model
layer 7 protocol 25
out-of-band connection 16
OverSize
checkbox 131

P

P2P
field 66
port 30
packet size
viewing 134
Packets
checkbox 125, 128, 135
viewing 124
PAE Access Entity 102
parity
console port 16
passive group
port group configuration 31
Password
field 120, 121
performance 2
performing
Ping test 147
Ping Test
performing 147
screen 147
Port
access control information 142
bandwidth 75
capability settings 105
checkboxes 86
configuring individual switch ports 56
console 16
diagnostic 16
edge 30
egress 32
features 2
field 106, 107, 137
GBIC 20
ingress 32
initializing 106
mirroring 2, 58
P2P 30
reauthenticating 107

RS-232 16
security 80
status 27
transition states 29
utilization 123
Port Configuration
screen 56, 57
Port Link Aggregation Group
screen 90, 92
Port number
field 69, 72
Port Security Settings
screen 80
Port VLAN ID (PVID) settings
modifying 73
PortControl
field 104
PortStatus
field 107
POST (Power On Self-Test) 26
power
failure 7
indicator 9
turning on 6
viewing status 142
Priority
field 66, 83, 84, 98
privileges
Admin 45
user 45
Priv-Protocol
field 121
Profile ID
field 93, 95, 98
Protocol
field 95
Protocol ID
field 96
PVID
field 74

Q

QoS Class of Traffic
screen 84
QoS control
features 2
QoS Output Scheduling
screen 82
Querier State
field 61
Query Interval
field 60
QuietPeriod
field 104

R

rack installation 5
RADIUS Server
field 108
using 108
RADIUS Server Authentication Setting
screen 108
Rapid Spanning Tree Protocol (RSTP) 29
Rate
field 76
Read View Name
field 114
rear panel
identifying components 8
ReAuth
field 105
Reauthenticate Port
screen 107
Reauthenticate Port Table 107
reauthenticating port 107
ReAuthPeriod
field 104
Reboot
screen 49
received (RX) packets
viewing 124
Record Number
field 123, 125, 126, 128, 130, 132, 135
Redundant Power Supply 9
remote management
setting up 110
Replace Dscp
field 98
replace priority
field 98
Reports
field 138

reset config option 49
reset option 48
reset system option 48
resetting switch 48
restarting switch 49
RMON Status
  field 56
Robustness Value
  field 60
root bridge 29
Router Port
  screen 141
router port
  viewing 140
Router Timeout
  field 61
routine packet filtering 28
RPS indicator 9
RS-232 port 16
rubber feet
  attaching 5
  unpacking 4
rules
  egress 33
  forwarding 33
  ingress 33
Rx Error Analysis
  screen 130, 131
Rx Packets Analysis
  screen 124, 125, 126, 127
Rx Size Analysis
  screen 134, 136

S

safety
  static electricity 153
Save Configuration
  button 47
  screen 47
saving changes 47, 144
Security IP Management
  screen 110, 111
Security IP Management table 53
Security Level
  field 114
Security Model
  field 114
Serial Port Auto Logout Time
  field 55
Server IP
  field 101
Server IP Address
  field 144, 145
ServerTimeout
  field 104
setting
  advanced switch information 55
  basic switch information 53
  Daylight Savings Time 78
  IP address 24, 51
  port bandwidth 75
  port security 80
  time zone 78
setting up
  port mirroring 58
  remote management 110
  safety precautions 152
settings
  downloading from a TFTP server 144
  Simple Network Time Protocol (SNTP) 76
  uploading to a TFTP server 145
Setup Port Mirroring
  screen 58
Setup Static Multicast Forwarding Table
  screen 68
Setup Static Unicast Forwarding Table
  screen 67
Severity
  field 101
shelf
  installation 5
side panels
  identifying components 8
Simple Network Time Protocol (SNTP)
  settings 76
SingColl
  checkbox 133
SNMP
  network management 25
  network manager 23
  versions 25
SNMP Community Table

adding entries 115
deleting entries 115
SNMP Community Table Configuration
screen 116, 117
SNMP Engine ID
modifying 117
SNMP Engine ID Configuration
screen 117
SNMP Group Table
adding entries 113
deleting entries 113
screen 115
SNMP Group Table Configuration
screen 114
SNMP Host Table
adding entries 118
deleting entries 118
screen 118, 119
SNMP Host Table Configuration
screen 118
SNMP User Table
adding entries 119
deleting entries 119
screen 119, 121
SNMP User Table Configuration
screen 120
SNMP Version
field 118, 120
SNMP View Table
adding entries 111
deleting entries 111
entry 116
screen 111, 113
SNMP View Table Configuration
screen 112
SNMPV3
using 111
SNTP (Simple Network Time Protocol)
support 2
SNTP Poll Interval in Seconds
field 77
SNTP Primary Server
field 77
SNTP Secondary Server
field 77
SNTP State
field 77
Source IP Mask
field 95
Source MAC Mask
field 93
Source Port
field 59
Spanning Tree Algorithm parameters 27
Spanning Tree Protocol
field 64
Spanning Tree Protocol (STP)
configuring 63, 65
using 63, 90
Speed
LED indicators 9
Speed/Duplex
field 57
stacking
connections 13
operation 17
standalone
converting switch to stacked switch 20
operation 17
State
field 57, 61, 66, 87, 88, 91
static
electricity 153
link aggregation 31
Static Multicast Forwarding Table
screen 68, 69
Static Router Ports Settings
configuring 61
screen 62
Status
field 59, 101
stop bits
console port 16
STP Version
field 64
Subnet Mask
field 52
Subtree OID
field 112
Succession
field 108
SuppTimeout

field 104
switch
configuring 42
connecting 11
connecting to end node 12
connecting to hub or switch 13
default IP address 23
IP address 23, 27
management concepts 15
resetting 48
restarting 49
setting up 4
Spanning Tree Algorithm parameters 27
stack connections 13
stacking 3
unpacking 4
Switch History
screen 146
viewing 146
Switch Information
screen 53
Switch Information (Advanced Settings)
screen 55, 102
Switch Information (Basic Settings)
screen 54
Switch Spanning Tree Settings
screen 63, 65
switch stack 3
adding switch 21
changing 19
converting 20
managing 19
swapping master switch 23
Syslog Global State
field 56
System Contact
field 54
system fans 8
System Location
field 54
System Log Server
screen 101
System Log Servers
screen 100, 102
using 100
System Name
field 54

T

tagging
defined 32
ports 35
tags
IEEE 802.1Q 33
Target IP Address
field 147
Target Port
field 59
TCP port number 96
TCP/IP 23
technical support 149
telephone numbers 150
Telnet Status
field 56
TFTP
server 20
using 23
TFTP services
using 143
Threshold
field 85
Time in HH:MM
field 78
Time Interval
field 123, 124, 125, 126, 127, 128, 129, 130, 132, 134, 136, 142
time zone
setting 78
Time Zone and DST
screen 78
Time Zone Offset from GMT in +/- HH:MM
field 79
To Day
field 79
To Day of Week
field 79
To Month
field 79
To Time in HH:MM
field 79, 80
To Which Day
field 79

traffic control
managing 85
Traffic Control Setting
screen 85
traffic segmentation
managing 86
Traffic Segmentation Setting
screen 86
transition states
port 29
Transmitted (TX) packets
viewing 128
traps
Authentication Failure type 26
Broadcast Multicast Storm type 27
Cold Start type 26
Link Change Event type 27
Port Partition type 27
Topology Change type 26
using 26
Warm Start type 26
Trivial File Transfer Protocol (TFTP) 143
turning on
switch 6
Tx Error Analysis
screen 132, 133
TX Hold Count(1-10)
field 64
Tx Packets Analysis
screen 128, 129
TxPeriod
field 104
Type
field 75, 91, 93, 95, 98

U

UDP multicast packets 61
UDP Port
field 101
port number 96
UDP/IP protocol 25
UDP/TIME protocol 76
UMB-cast (RX) packets
viewing 126
UnderSize
checkbox 131
Unicast
checkbox 126
unicast forwarding
adding 66
deleting 67
modifying 66
untagging
defined 32
ports 35
Upload Firmware to TFTP Server
screen 145
Upload Log to TFTP Server
screen 145
uploading
log to a TFTP server 145
settings to a TFTP server 145
user
adding 45
privileges 45
User Account Management
screen 45
User Account Modify Table
screen 45
user accounts
managing 45
user interface
Web-based manager 43
User Name
field 45, 120
user priority
assigning 84
using
access profiles 92
filtering 66
forwarding 66
IEEE 802.1p priority queuing (QoS) 81
IGMP 59
LACP 89
link aggregation 90
MIBs 27
RADIUS server 108
SNMPV3 111
Spanning Tree Protocol (STP) 63
system log servers 100
TFTP services 143
traps 26

Utilization
checkbox 123
screen 123

V

VID
field 68, 138, 139
VID (VLAN ID)
using 33
View Name
field 112, 116
View Type
field 112
viewing
authenticator state 142
basic switch information 53
errors 130
errors Received (RX) 130
errors Transmitted (TX) 132
IGMP Snooping forwarding table 139
IGMP Snooping Group 138
MAC address forwarding table 137
packet size 134
packets 124
port access control information 142
Port Utilization 123
power status 142
received (RX) packets 124
router port 140
switch history 146
Transmitted (TX) packets 128
UMB-cast (RX) packets 126
VLAN status 140
VLAN
asymmetric 36
field 93, 95
implementation 32
using 32
VLAN ID
field 60, 62, 67, 72, 137
VLAN Name
field 53, 60, 62, 72
VLAN Status
screen 140
viewing 140
VLANs
creating 71
deleting 71
modifying 71
VT-100
emulation 17
terminal 16

W

Web Status
field 56
Web-based management 16
Web-based manager
user interface 43
Write View Name
field 114

Y

Year
field 77

MAN MANAGED ETH SWITCH GDE R0 3/04

8509825