Linksys by Cisco

24-Port 10/100/1000 Gigabit Switch with Webview and PoE User Guide

Model: SRW2024P

BUSINESS SERIES

cisco

Chapter 1: Getting Started 1
How to Use this Guide 1
Document Style Conventions 1
Finding Information in Your PDF Documents 2
Finding Text in a PDF 2
Finding Text in Multiple PDFs 2

Chapter 2: Introduction 3
Welcome 3

Chapter 3: Getting to Know the Switch 4
Front Panel 4
LEDs 4
Ports 4
The Back Panel 5
The Side Panel 5
LAN Ports 5
The Gigabit Expansion Ports 6
The Console Port 6

Chapter 4: Connecting the Switch 7
Overview 7
Before You Install the Switch... 7
Placement Options 8
Desktop Placement 8
Rack-Mount Placement 8
Connecting the Switch 9
Uplinking the Switch 10

Chapter 5: Using the Console Interface for Configuration 11
Overview 11
Configuring the HyperTerminal Application 11
Connecting to the Switch through a Telnet Session 13
Configuring the Switch through the Console Interface 13
Switch Main Menu 14
System Configuration Menu 14
File Management 21
Restore System Default Settings 21
Reboot System 22
Back to Main Menu 22
PoE Configuration 24

Chapter 6: Using the web-based Utility for Configuration 28
Overview 28
Accessing the web-based Utility 28
Setup Tab - Summary 30
Device Information 30
System Information 30
PoE Information 31
Setup Tab - Network Settings 31

Identification 32
IP Configuration 32
Setup Tab - Time 32
Set Time 33
Manual 33
Automatic 33
SNTP Servers 34
Port Management Tab - Port Settings 35
Port Setting 36
Port Broadcast Control 37
Port Management Tab - Link Aggregation 38
Port Management Tab - LACP 39
Port Management Tab - PoE Power Settings 41
VLAN Management Tab - Create VLAN 42
Single VLAN 42
VLAN Range 42
VLAN Table 42
VLAN Management Tab - Port Settings 43
VLAN Management Tab - Ports to VLAN 44
Switch Port Mode 44
Membership 45
VLAN Management Tab - VLAN to Ports 45
VLAN Management Tab—GVRP 46
Statistics Tab - RMON Statistics 48
Statistics Tab - RMON History 50
History Control Table 50
Statistics Tab - RMON Alarm 51
Statistics Tab - RMON Events 54
Event Setting 54
Statistics Tab - Port Utilization 55
Statistics Tab - 802.1x Statistics 56
ACL Tab - IP Based ACL 57
ACL Tab—IPv6 Based ACL 59
ACL Tab - MAC Based ACL 61
ACL Tab—TCAM Utilization 62
Security Tab - ACL Binding 63
Security Tab - Authentication Servers 64
RADIUS Server Setting 64
TACACS Server Setting 65
Security Tab - 802.1x Settings 65
Security Tab - Port Security 69
Security Tab - HTTPS Settings 70
Security Tab - Management ACL 71
Security Tab—Dynamic VLAN 71
Security Tab—Network Access MAC Address 72
Security Tab - SSH Settings 74
SSH Host-Key Settings 75
QoS Tab 76
QoS Tab - CoS Settings 77
CoS to Queue 78
Port to CoS 78

QoS Tab - Queue Settings 78
QoS Tab - DSCP Settings 79
QoS Tab - Diffserv Settings 80
Class Map 81
Policy Map 82
QoS Tab - Diffserv Port Binding 83
QoS Tab - Bandwidth 84
Spanning Tree Tab 85
Spanning Tree Tab - STP Status 85
Spanning Tree Tab - Global STP 86
Spanning Tree Tab - STP Port Settings 88
Spanning Tree Tab—RSTP Port Settings 90
Spanning Tree Tab—MSTP Properties 92
Spanning Tree Tab—MSTP Instance Settings 92
Spanning Tree Tab—MSTP Interface Settings 93
Multicast Tab - Global Settings 95
Multicast Tab - Static Member Ports 97
Multicast Tab - Static Router Ports 97
Multicast Tab - Member Ports Query 99
Multicast Tab - Router Ports Query 100
SNMP Tab 100
SNMP Tab—Global Parameters 101
SNMP Tab—Views 103
SNMP Tab—Group Profile 104
SNMP Tab—Group Membership 104
SNMP Tab—Communities 106
SNMP Tab—Notification Recipient 107
Admin Tab - User Authentication 109
Admin Tab - Forwarding Database 110
Address Aging 110
Static Address Setting 111
Dynamic Address Query 111
Admin Tab - Log 112
Syslog 114
SMTP Setting 114
Admin Tab - Port Mirroring 115
Admin Tab - Cable Test 116
Admin Tab - Ping 117
Admin Tab - Save Configuration 118
Admin Tab - Jumbo Frame 118
Admin Tab - Firmware Upgrade 119
Admin Tab - HTTP Upgrade 121
Admin Tab - Reboot 122
Admin Tab - Factory Default 123

Appendix A: About Gigabit Ethernet and Fiber Optic Cabling 124
Gigabit Ethernet 124
Fiber Optic Cabling 124

Appendix B: Windows Help 125
TCP/IP 125

Shared Resources 125
Network Neighborhood/My Network Places 125

Appendix C: Downloading with Xmodem 126
Startup Menu Procedures 126

Appendix D: Glossary 129

Appendix E: Warranty Information 136
LIMITED WARRANTY 136
Exclusions and Limitations 136
Obtaining Warranty Service 137
Technical Support 137

Appendix F: Regulatory Information 138
FCC Statement 138
FCC Caution 138
FCC Radiation Exposure Statement 138
Generic Discussion on RF Exposure 138
Explosive Environment, Medical and FAA Device Information 140
Safety Notices 140
Industry Canada (Canada) 140
User Information for Consumer Products Covered by EU Directive 2002/96/EC on Waste Electric and Electronic Equipment (WEEE) 141

Appendix G: Specifications 149

Getting Started

How to Use this Guide

This User Guide has been designed to make working with the switch easier than ever. Look for the following items when reading this guide:

WARNING: This graphic means there is a Warning and is something that could damage your self, property, or the camera.

NOTE: This checkmark means there is a Note of interest and is something you should pay special attention to while using the camera.

CAUTION: This exclamation point means that caution should be used when performing a step or a serious error may occur.

Document Style Conventions

The following style conventions are used in this document.

- **Menus, Tabs, and Buttons:** Bold type is used to indicate the name of a button, menu, or tab in an application.

  Example: Click **Submit All Changes** to save your entries.

- **Screens, Page Areas, and Fields:** Italic type is used to indicate the name of screens, page areas, and fields.

  Example: Scroll down to the *PBX Parameters* area of the screen.

- **Data Input:** The **`Courier`** font is used to indicate characters that you should type into a field exactly as printed in this guide.

  Example: In the *Mailbox Subscribe Expires* field, type **`30`**.

  In this example, you would type the number 30 in the field.

- **Parameters:** Angle brackets and italic type indicate parameters that you must replace with the appropriate data.

  Example: Type **`800@`**<*IP address of device*>**`:5090`**

  In this example, you would type the characters 800@, followed by the IP address of your device, followed by a colon and the number 5090.

Finding Information in Your PDF Documents

The PDF Find/Search tool lets you find information quickly and easily online. You can:

- Search an individual PDF
- Search multiple PDFs at once (for example, all PDFs in a specific folder or disk drive)
- Perform advanced searches

Finding Text in a PDF

By default, the Find toolbar is open. If it has been closed, choose **Edit > Find**.

Use Find to search for text in an open PDF:

1. Enter your search terms in the *Find* box on the toolbar.
2. Optionally click the arrow next to the Find text box to refine your search (such as Whole words only).
3. Press **Enter**. Acrobat jumps to the first instance of the search term. Pressing **Enter** again continues to more instances of the term.

Finding Text in Multiple PDFs

The *Search* window lets you search for terms in multiple PDFs. The PDFs do not need to be open. Either:

- Choose **Edit** > **Search**

  or

- Click the arrow next to the *Find* box and choose Open Full Acrobat Search. The *Search* window appears.

In the *Search* window:

1. Enter the text you want to find.
2. Choose **All PDF Documents in**.
3. From the drop-down box, choose **Browse for Location**.
4. Choose the location you want to search, either on your computer or on a network, then click **OK**.
5. If you want to specify additional search criteria, click **Advanced Search Options**, and choose the options you want.
6. Click **Search.**

For more information about the Find and Search functions, see the Adobe Acrobat online help.

Introduction

Welcome

The Linksys WebView Managed Switch allows you to expand your network securely. Configuration of the switch is secured using SSL for web access. User control is secured with 802.1x security using a RADIUS authentication mechanism or MAC-based filtering.

Extensive QoS features make the solution ideal for real-time applications like voice and video. The four priority queues together with the weighted round robin and strict priority scheduling techniques facilitate efficient co-existence of real-time traffic with data traffic allowing them each to meet their QoS needs. Individual users or applications can be prioritized above others using various Class of Service options: by port, layer 2 priority (802.1p), and Layer 3 priority (TOS or DSCP). Intelligent Broadcast, and Multicast storm control minimizes and contain the effect of these types of traffic on regular traffic. IGMP Snooping limits bandwidth-intensive video traffic to only the requestors, without flooding to all users. Incoming traffic can be policed, and outgoing traffic can be shaped, allowing you to control network access and traffic flow.

Several features allow you to expand and grow your network of switches. Link aggregation allows multiple high-bandwidth trunks between switches. This feature also provides a level of reliability so that the system continues to operate if one of the links breaks. Spanning Tree Protocol (STP), Fast Spanning Tree, and Rapid Spanning Tree (RSTP) allow you to build a mesh of switches, increasing the availability of the system.

The rich management functionality of the WebView switches includes SNMP, RMON, Telnet, and HTTP Management options, allowing you to flexibly integrate and manage these devices in your network.

Getting to Know the Switch

Front Panel

The switch's LEDs and ports are located on the front panel.

LEDs

System—The **System** LED lights green to indicate the power is being supplied to the switch. Lights orange to indicate that the switch's power-on-self-test (POST) is in progress. Flashes orange to indicate that the POST has failed.

Link/Act (1-24)—The **Link/Act** LED lights orange to indicate a functional 1000Mbps network link through the corresponding port (1 through 24) with an attached device.

Link/Act (1-24)—The **Link/Act** LED lights green to indicate a functional 10/100Mbps network link. Flashes to indicate that the switch is actively sending or receiving data over that port.

PoE—The **PoE** LED lights orange to indicate a powered device is connected to the corresponding port (1 through 24). Flashes to indicate that the switch is actively sending power over that port.

Ports

LAN (1-24)—The LAN (Local Area Network) ports connect to Ethernet network devices, such as other switches or routers.

MiniGBIC (12) /MiniGBIC (24)—The switch is equipped with two mini-GBIC ports. The miniGBIC (Gigabit Interface Converter) port is a connection point for a miniGBIC expansion module, so the switch can be uplinked via fiber to another switch. If a Gigabit mini-GBIC port is being used, the associated LAN port (12 and/or 24) cannot be used. These ports link to a high-speed network peripheral system or clients at speeds of 1000Mbps.

Use the Linksys MGBT1, MGBSX1, or MGBLH1 miniGBIC modules with the switch. The MGBSX1 and the MGBLH1 require fiber cabling with LC connectors, while the MGBT1 requires a Category 5e Ethernet cable with an RJ-45 connector.

Console—The Console port is where you can connect a serial cable to a PC's serial port for configuration using your PC's HyperTerminal program. See *Chapter 4: Using the Console Interface for Configuration* for more information.

The Back Panel

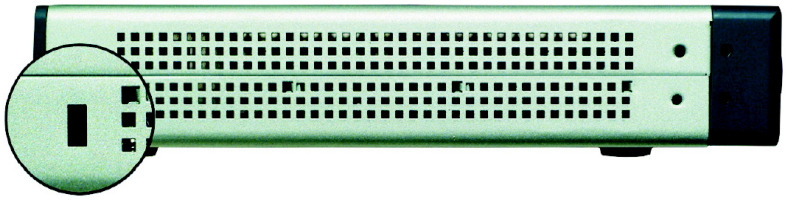
The power port is located on the back panel of the switch.

Power—The **Power** port is where you connect the power cord.

NOTE: If you need to reset the switch, disconnect the power cord from the back of the switch. Wait a few seconds and then reconnect it.

The Side Panel

The security slot is located on a side panel.



Security Slot—The security slot is where you can attach a lock to the switch to help prevent theft.

LAN Ports

The switch is equipped with 24 auto-sensing RJ-45 LAN ports. These RJ-45 ports support network speeds of 10Mbps, 100Mbps or 1000Mbps, and can operate in half and full-duplex modes. Auto-sensing technology enables each port to automatically detect the speed of the device connected to it (10Mbps, 100Mbps or 1000Mbps), and adjust its speed and duplex mode accordingly.

The switch's RJ-45 ports also support the IEEE 802.3af Power-over-Ethernet (PoE) standard that enables DC power to be supplied to attached devices using wires in the connecting twisted-pair cable. Any 802.3af-compliant device attached to a port can directly draw power from the switch over the twisted-pair cable without requiring its own separate power source. This capability gives network administrators centralized power control for devices such as IP phones and wireless access points, which translates into greater network availability. For each attached 802.3af-compliant device, the switch automatically senses the load and dynamically supplies the required power. The switch delivers power to a device using the two data wire pairs in the twisted-pair cable. Each port can provide up to 15.4 W of power at the standard -48 VDC

voltage. To connect a device to a port, you will need to use Category 5 (or better) network cable.

The Gigabit Expansion Ports

The switch is equipped with two miniGBIC ports that have shared Gigabit Ethernet ports (12 and 24) which provide for the installation of one expansion module. These ports provide links to high-speed network segments or individual workstations at speeds of up to 1000Mbps (Gigabit Ethernet). To establish a Gigabit Ethernet connection using a mini-GBIC port, you will need to install an MGBT1, MGBSX2, or MGBLH1 Gigabit expansion module and use Category 5e cabling or fiber optic cabling. For more information on fiber optic cabling, see Appendix A, "About Gigabit Ethernet and Fiber Optic Cabling".

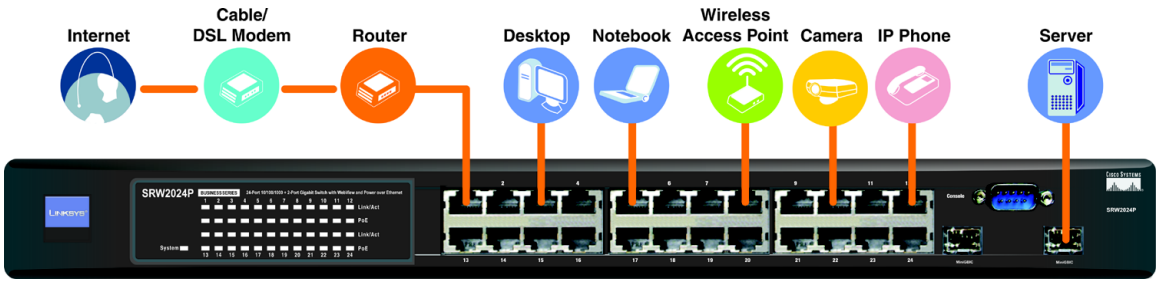
The Console Port

The switch has a console port on the front panel that allows you to connect to a computer's serial port (for configuration purposes) using the provided serial cable. You can use HyperTerminal to manage the switch through the console port. With this and many other Linksys products, your networking options are limitless. Go to the Linksys website at www.linksys.com for more information about products that work with the switch.

Connecting the Switch

Overview

This chapter will explain how to connect network devices to the switch. For an example of a typical network configuration, see the application diagram shown below.



When you connect your network devices, make sure you don't exceed the maximum cabling distances, which are listed in the following table:

From	To	Maximum Distance
Switch	Switch or Hub*	100 meters (328 feet)
Hub	Hub	5 meters (16.4 feet)
Switch or Hub	Computer	100 meters (328 feet)

*A hub refers to any type of 100Mbps hub, including regular hubs and stackable hubs. A 10Mbps hub connected to another 10Mbps hub can span up to 100 meters (328 feet).

Before You Install the Switch...

When you choose a location for the switch, observe the following guidelines:

- Make sure that the switch will be accessible and that the cables can be easily connected.
- Keep cabling away from sources of electrical noise, power lines, and fluorescent lighting fixtures.
- Position the switch away from water and moisture sources.
- To ensure adequate air flow around the switch, be sure to provide a minimum clearance of two inches (50 mm).
- Do not stack free-standing switches more than four units high.

Placement Options

Before connecting cables to the switch, first you will physically install the switch. Either set the switch on its four rubber feet for desktop placement or mount the switch in a standard-sized, 19-inch wide, 1U high rack for rack-mount placement.

Desktop Placement

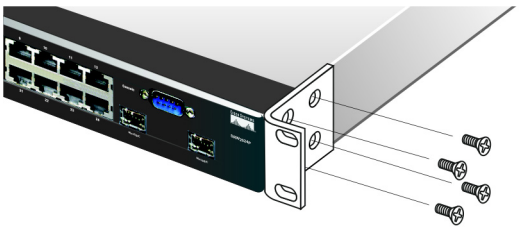
1. Attach the rubber feet to the recessed areas on the bottom of the switch.
2. Place the switch on a desktop near an AC power source.
3. Keep enough ventilation space for the switch and check the environmental restrictions mentioned in the specifications.
4. Proceed with connecting the switch.

Rack-Mount Placement

To mount the switch in any standard-sized, 19-inch wide, 1U high rack, follow these instructions:

CAUTION: Make sure you use the screws supplied with the mounting brackets. Using the wrong screws could damage the switch and would invalidate your warranty.

1. Place the switch on a hard flat surface with the front panel facing you.
2. Attach a rack–mount bracket to one side of the switch with the supplied screws. Then attach the other bracket to the other side.



3. Make sure the brackets are properly attached to the switch.

4. Use the appropriate screws (not included) to securely attach the brackets to your rack.

5. Proceed with connecting the switch.

Connecting the Switch

To connect network devices to the switch, follow these instructions:

1. Make sure all the devices you will connect to the switch are powered off.
2. For 10/100Mbps devices, connect a Category 5 Ethernet network cable to one of the numbered ports on the switch. For a 1000Mbps device, connect a Category 5e Ethernet network cable to one of the numbered ports on the switch.
3. Connect the other end to a PC or other network device.
4. Repeat steps 2 and 3 to connect additional devices. If pre-standard or 802.3af-compliant PoE devices are connected to the switch's 10/100/1000 ports, the switch automatically supplies the required power.
5. If you are using a miniGBIC port, then connect a miniGBIC module to a miniGBIC port. For detailed instructions, refer to the module's documentation.
6. If you will use the switch's console interface to configure the switch, then connect the supplied serial cable to the switch's Console port, and tighten the captive retaining screws. Connect the other end to your PC's serial port. (This PC must be running a VT100 terminal emulation software, such as HyperTerminal.)

CAUTION: Make sure you use the power cord that is supplied with the switch. Use of a different power cord could damage the switch.

7. Connect the supplied power cord to the switch's power port, and plug the other end into an electrical outlet.
8. Power on the network devices connected to the switch. Each active port's corresponding Link/Act LED will light up on the switch.

Uplinking the Switch

To uplink the switch, connect one end of a Category 5 (or better) Ethernet network cable into one of the 24 gigabit ports, and then connect the other end of the cable into the peripheral device's uplink port. MDI/MDIX will automatically detect the speed and cable type.

If you will use the switch's console interface to configure the switch, proceed to Chapter 5, "Using the Console Interface for Configuration" for directions.

If you will use the switch's web-based utility to configure the switch, proceed to Chapter 6, "Using the web-based Utility for Configuration" for directions.

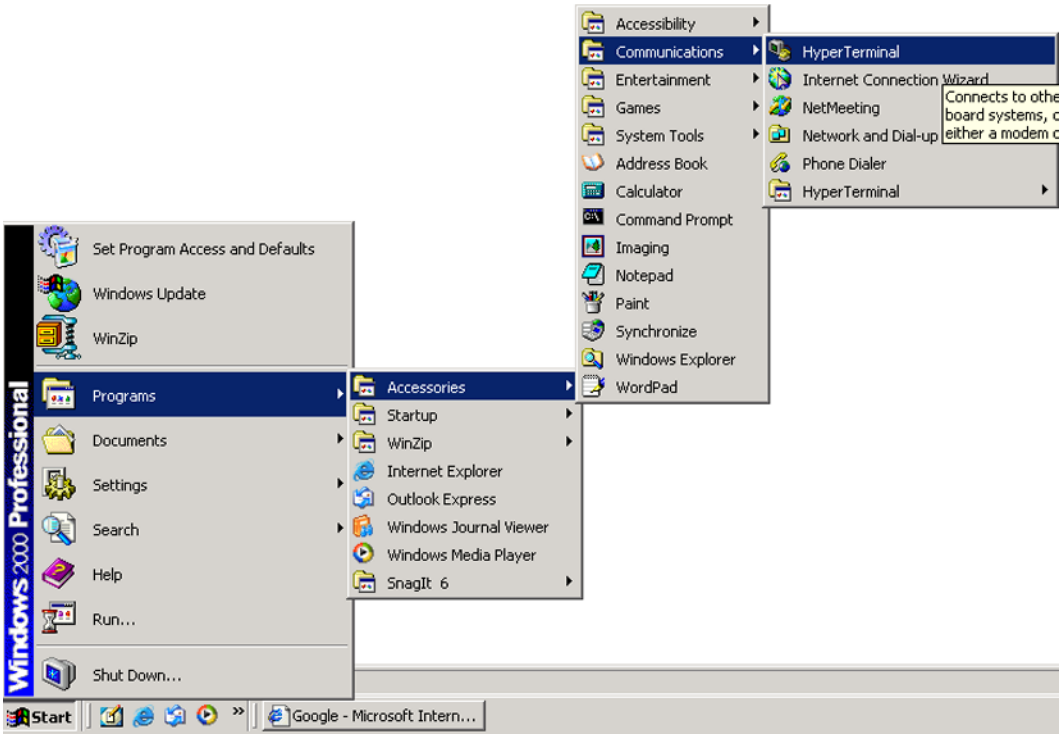
Using the Console Interface for Configuration

Overview

The switch features a menu-driven console interface for basic configuration of the switch and management of your network. The switch can be configured using CLI through the console interface or through a telnet connection. This chapter describes console interface configuration. Configuration can also be performed through the web utility, which is covered in the next chapter.

Configuring the HyperTerminal Application

Before you use the console interface, you will need to configure the HyperTerminal application on your PC.



1. Click the **Start** button. Select **Programs** and choose **Accessories**. Select **Communications**. Select **HyperTerminal** from the options listed in this menu.

2. On the *Connection Description* screen, enter a name for this connection. In the example, the name of connection is SRW2024P. Select an icon for the application. Then, click the **OK** button.

3. On the *Connect To* screen, select a port to communicate with the switch: **COM1**, **COM2**, or **TCP/IP**.

4. Set the serial port settings as follows:

   Bits per second: **38400**

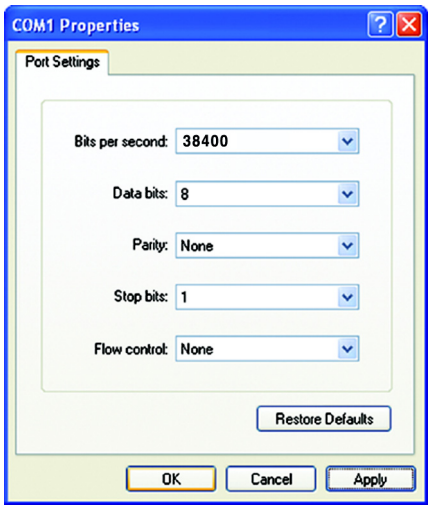
   Data bits: **8**

   Parity: **None**

   Stop bits: **1**

   Flow control: **None**

5. Then, click the **OK** button.



Connecting to the Switch through a Telnet Session

Open a command line editor and enter **telnet 192.168.1.254**. Then, press the **Enter** key.

The *Login* screen appears. The first time you open the CLI interface, select **Edit** and press **Enter**. Type **admin** in the *User Name* field. Leave the *Password* field blank.

Press the **Esc** key and you will return to the login screen. Press the **Right Arrow** key to navigate to **Execute** and press the **Enter** key to enter the CLI interface.

Configuring the Switch through the Console Interface

The console screens consist of a series of menus. Each menu has several options, which are listed vertically. You select a menu option when you highlight it; pressing the **Enter** key activates the highlighted option.

To navigate through the menus and actions of the console interface, use the **Up** or **Down Arrow** keys to move up or down, and use the **Left** or **Right Arrow** keys to move left or right. Use the **Enter** key to select a menu option, and use the **Esc** key to return to the previous selection. Menu options and any values entered or present will be highlighted. The bottom of the screen lists the actions available.

Switch Main Menu

The *System Main Menu* screen displays these choices:

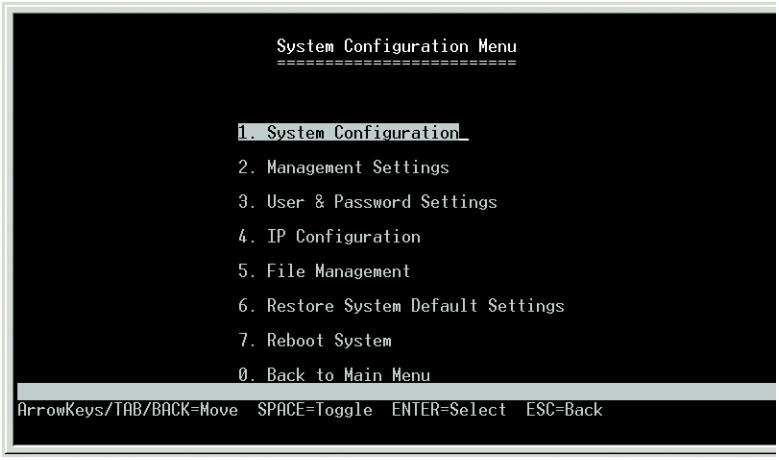
1. System Configuration Information Menu
2. Port Status
3. Port Configuration
4. PoE Configuration
5. Help
6. Logout

System Configuration Menu

On the *System Configuration Menu* screen, you have these choices:

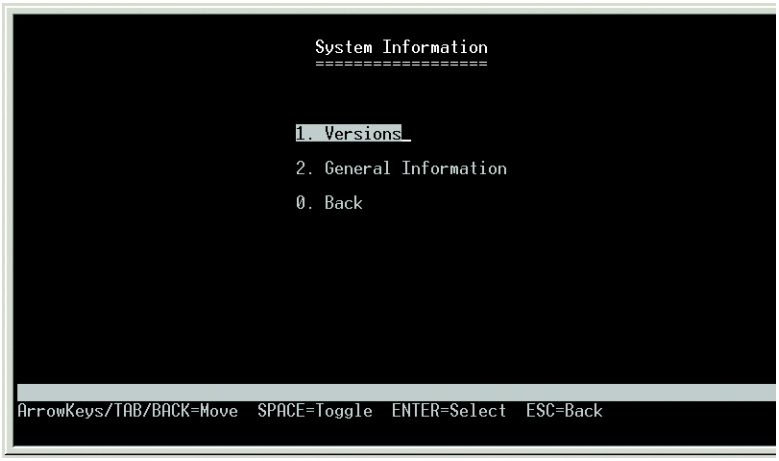
1. System Information
2. Management Settings
3. User & Password Settings
4. IP Configuration
5. File Management
6. Restore System Default Settings
7. Reboot System

8. Back to Main Menu



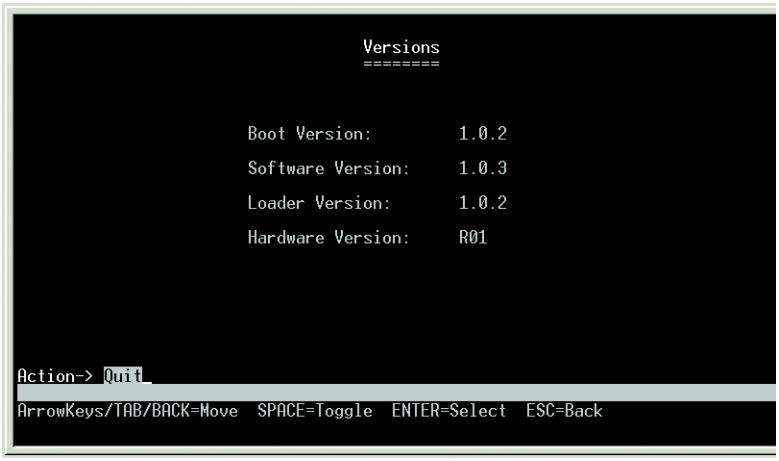
System Information

Using this screen, you can check the switch's firmware versions and general system information.



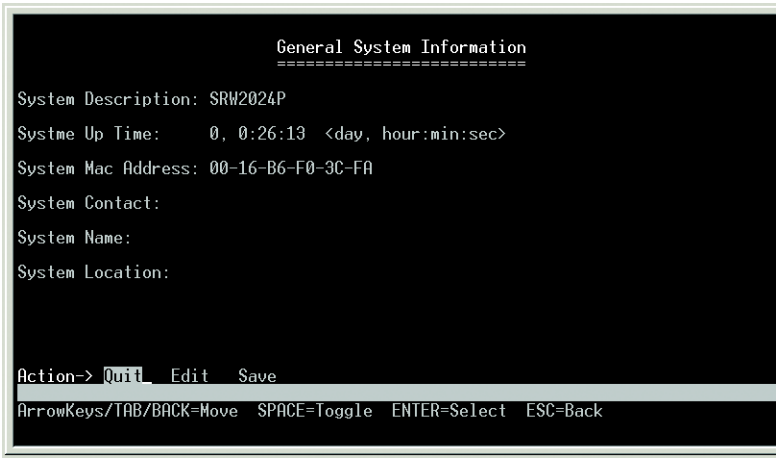
Versions

The *Versions* screen displays the switch's boot, software, loader, and hardware firmware versions.



General Information

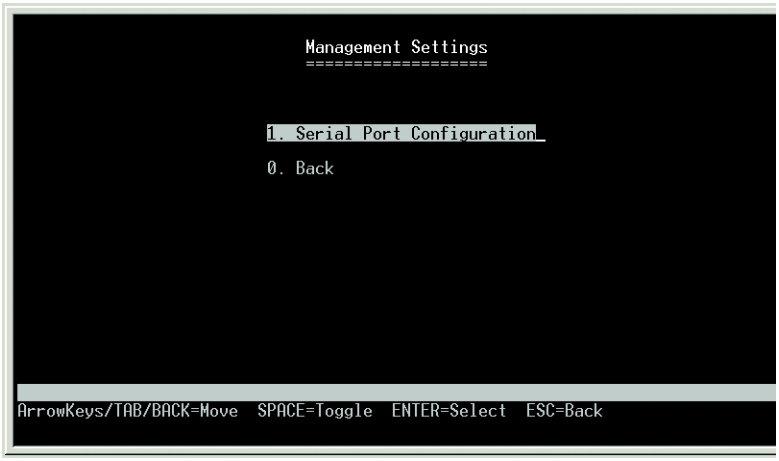
The *General System Information* screen displays the switch's description, System Up Time, System MAC Address, System Contact, System Name, and System Location.



Select **Edit** and press the **Enter** key to make changes. When your changes are complete, press the **Esc** key to return to the *Action* menu. Select **Save** and press the **Enter** key to save your changes. To exit, select **Quit** and press the **Enter** key.

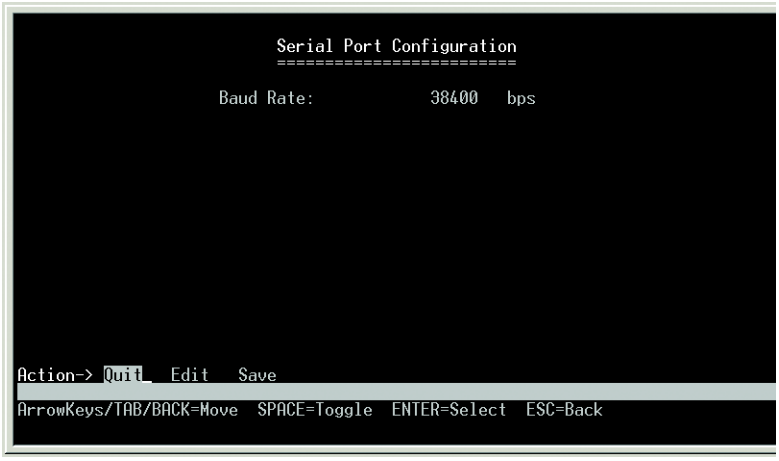
Management Settings

From the *Management Settings* screen, you can set Serial Port Session Configuration.



Serial Port Configuration

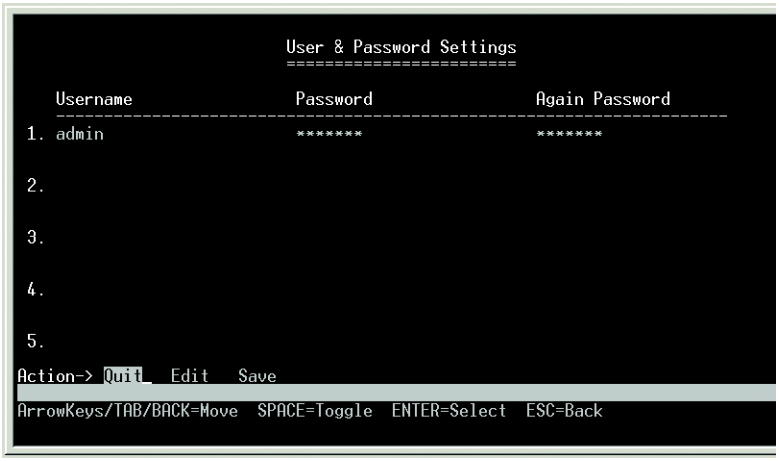
On the *Serial Port Configuration* screen, the switch's baud rate is displayed.



Select **Edit** and press the **Enter** key to make changes. Toggle to the desired speed and when your changes are complete, press the **Esc** key to return to the *Action* menu. Select **Save** and press the **Enter** key to save your changes. To exit, select **Quit** and press the **Enter** key.

User & Password Settings

From this screen, you can administer the user names and passwords of those accessing the switch.

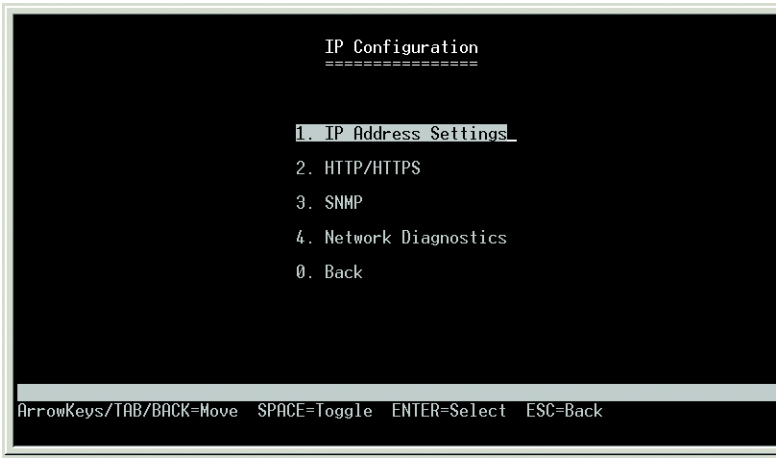


Select **Edit** and press the **Enter** key to make changes. When your changes are complete, press the **Esc** key to return to the *Action* menu. Select **Save** and press the **Enter** key to save your changes. To exit, select **Quit** and press the **Enter** key.

NOTE: The *Username & Password Settings* screen can also be used to set passwords for other users.

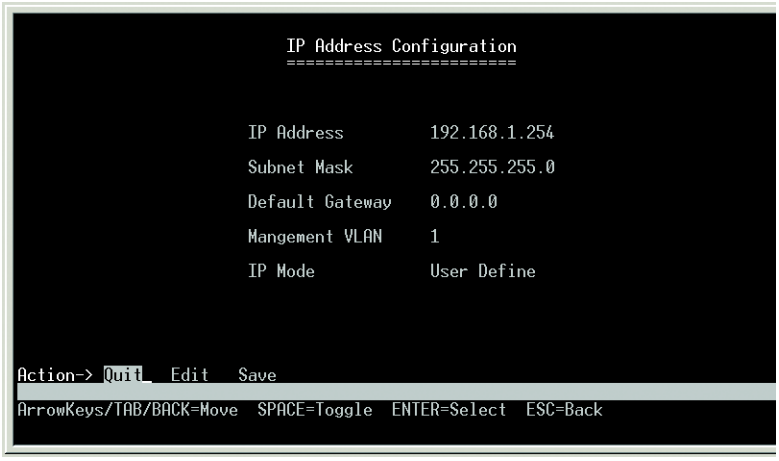
IP Configuration

The *IP Configuration* screen displays these choices: the switch's IP Address Settings, HTTP/HTTPS, SNMP, and Network Diagnostics.



IP Address Settings

The switch's IP information is displayed here.



IP Address. The IP Address of the switch is displayed. (The default IP address is **192.168.1.254**.) Verify that the address you enter is correct and does not conflict with another device on the network.

Subnet Mask. The subnet mask of the switch is displayed.

Default Gateway. The IP address of your network's default gateway is displayed.

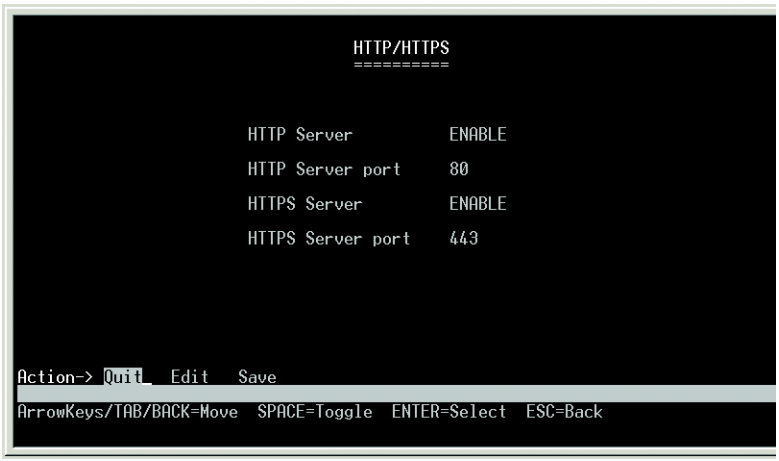
Management VLAN. The VLAN ID number is displayed. Set the ID number of the Management VLAN. This is the only VLAN through which you can gain management access to the switch. By default, all ports on the switch are members of VLAN 1, so a management station can be connected to any port on the switch. If other VLANs are configured and you change the Management VLAN, you may lose management access to the switch. In this case, you should reconnect the management station to a port that is a member of the Management VLAN.

IP Mode. Choose to have either a user-defined IP address or to have it assigned by DHCP or BOOTP.

Select **Edit** to make changes. When your changes are complete, press the **Esc** key to return to the *Action* menu, and select **Save** to save your changes.

HTTP/HTTPS

The *HTTP/HTTPS* screen allows you to set the Hyper Text Transfer Protocol server (web server) information for the switch.



HTTP Server. Enable or disable the switch's HTTP server function.

HTTP Server port. Set the TCP port that HTTP packets are sent and received from.

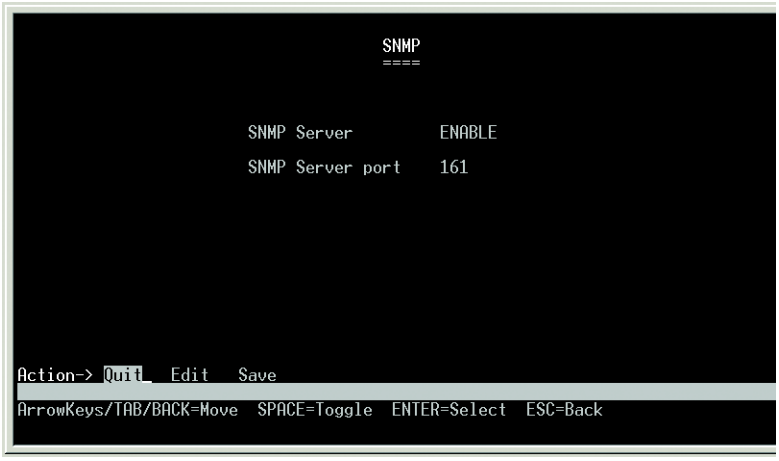
HTTPS Server. Enable or disable the Secure HTTP server function of the switch.

HTTPS Server port. Set the TCP port that the HTTPS packets are sent and received from.

Select **Edit** and press the **Enter** key to make changes. When your changes are complete, press the **Esc** key to return to the *Action* menu. Select **Save** and press the **Enter** key to save your changes. To exit, select **Quit** and press the **Enter** key.

SNMP

The *SNMP* screen allows you to set the switch's SNMP settings.



SNMP Server. Enable or Disable the SNMP function for the switch.

SNMP Server Port. Set the TCP port that will be used for sending and receiving SNMP packets.

Network Diagnostics

The *Network Configuration* screen allows you to use ping to test network connectivity. The *Ping* screen displays the IP address of the location you want to contact.

Select **Edit** to change the IP address, and select **Execute** to begin the ping test.

After the ping test is complete, the *Ping* screen displays the IP address, status, and statistics of the ping test.

Select **Edit** and press the **Enter** key to make changes. When your changes are complete, press the **Esc** key to return to the *Action* menu. Select **Save** and press the **Enter** key to save your changes. To exit, select **Quit** and press the **Enter** key.

File Management

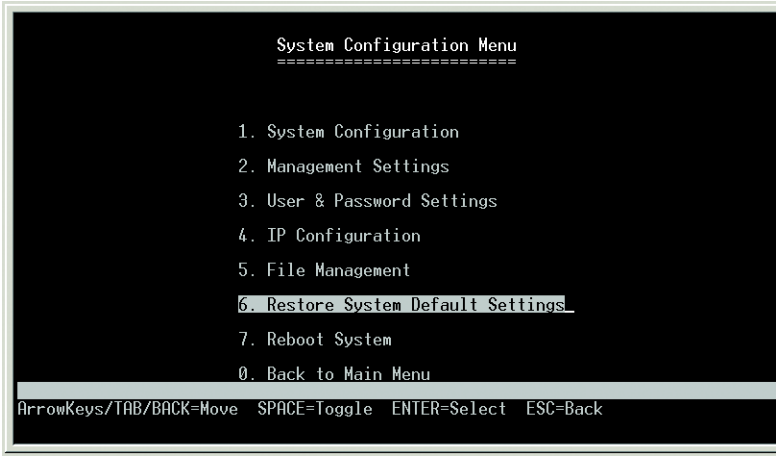
The *File Management* screen allows you to upload or download files, such as the startup configuration, boot, or image file, using a TFTP server.

Select **Edit** to change the settings. When your changes are complete, press the **Esc** key to return to the *Action* menu, and select **Execute** to upload or download the designated file.

If you are downloading a new boot image, please follow these steps:

1. Download the new boot code. DO NOT RESET THE DEVICE!
2. Download the new software image.
3. Reset the device now.

Restore System Default Settings



To restore the switch back to the factory default settings, select **Restore System Default Settings** and press the **Enter** key. You will be asked if you want to continue. Press the **y** key to restore the switch's default settings, or press the **n** key to cancel.

Reboot System

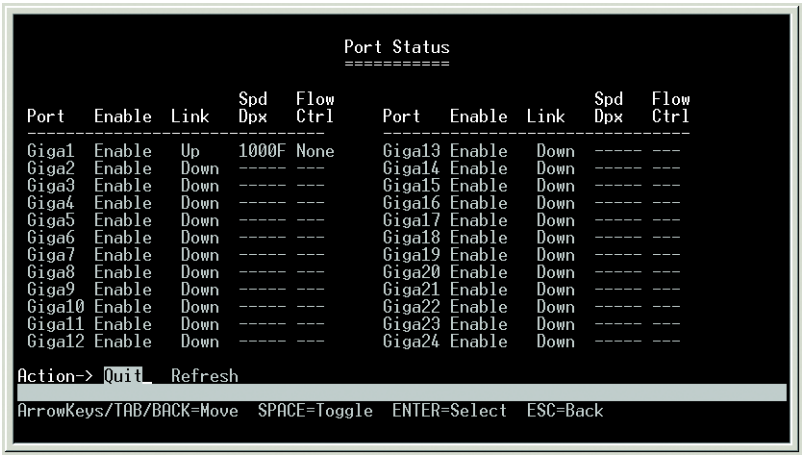
Select **Reboot System** and press the **Enter** key if you want to restart the switch. You will be asked if you want to continue. Press the **y** key to reboot the switch, or press the **n** key to cancel. After the switch has rebooted, the *Switch Main Menu* screen appears.

Back to Main Menu

Select **Back to Main Menu** and press the **Enter** key if you want to return to the *Switch Main Menu* screen.

Port Status

On the *Switch Main Menu* screen, select **Port Status** and press the **Enter** key if you want to view the status information for the switch's ports.

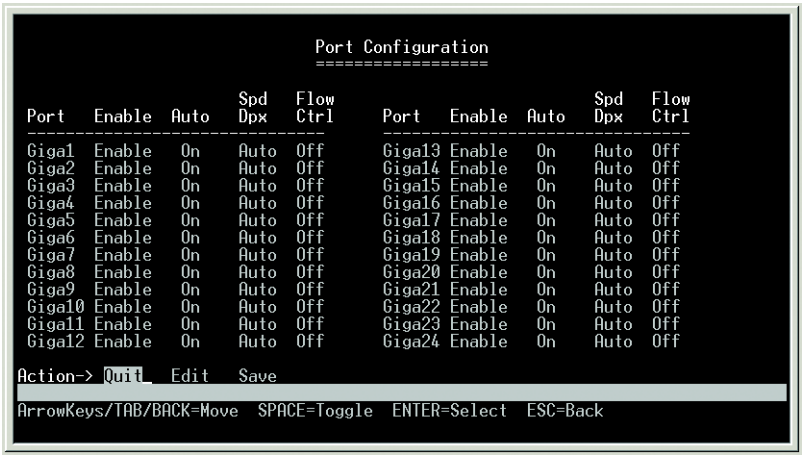


The *Port Status* screen displays the port numbers, their status, Link status, speed and duplex mode, and status of flow control, which is the flow of packet transmissions.

If you want to change any settings for a port, you must use the *Port Configuration* screen.

Port Configuration

On the *Switch Main Menu* screen, select **Port Configuration** and press the **Enter** key if you want to configure the switch's ports.



The *Port Configuration* screen displays the port numbers, their status, auto-negotiation status, speed and duplex mode, and status of flow control, which is the flow of packet transmissions.

NOTE: When downloading a configuration file, be sure that it is a valid configuration file. If you have edited the file, ensure that only valid entries have been configured.

Select **Edit** and press the **Enter** key to make changes. When your changes are complete, press the **Esc** key to return to the *Action* menu. Select **Save** and press the **Enter** key to save your changes. To exit, select **Quit** and press the **Enter** key.

You can use the *Port Configuration* screen to enable or disable an interface, set auto-negotiation and the interface capabilities to advertise or manually fix the speed, duplex mode, and flow control.

Enable—Allows you to manually enable or disable an interface. You can disable an interface due to abnormal behavior (for example, excessive collisions), and then enable it again, once the problem has been resolved. You may also disable an interface for security reasons.

Auto-negotiation (Port Capabilities)—Allows auto-negotiation to be enabled/disabled. When auto-negotiation is enabled, you need to specify the capabilities to be advertised. When auto-negotiation is disabled, you can force the settings for speed, mode, and flow control. The following capabilities are supported:

- 10half – Supports 10 Mbps half-duplex operation
- 10full – Supports 10 Mbps full-duplex operation
- 100half – Supports 100 Mbps half-duplex operation
- 100full – Supports 100 Mbps full-duplex operation
- 1000full – Supports 1000 Mbps full-duplex operation
  (Default: Auto-negotiation enabled; Advertised capabilities for 100Base-TX – 10half, 10full, 100half, 100full; 1000Base-T – 10half, 10full, 100half, 100full, 1000full; 1000Base-SX/LX/LH (SFP) – 1000full; 100Base-FX (SFP) – 100full

Speed/Duplex—Allows manual selection of port speed and duplex mode (that is, with auto-negotiation disabled).

Flow Control—Allows automatic or manual selection of flow control.

PoE Configuration

On the *Switch Main Menu* screen, select **PoE Configuration** and press the **Enter** key if you want to configure the switch's ports.

PoE Main Menu

The *PoE Main Menu* screen displays three menu choices: System PoE Configuration, Port PoE Status, and Port PoE Configuration.

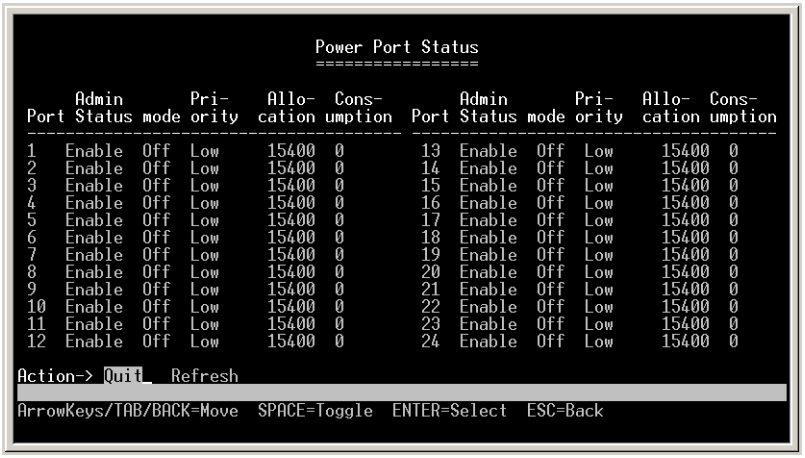
System PoE Configuration

The *Power Configuration* screen allows you to set the PoE power allocation from the switch to connected devices.

The switch's power management enables total switch power and individual port power to be controlled within a configured power budget. Port power can be automatically turned on and off for connected devices, and a per-port power priority can be set so that the switch never exceeds its allocated power budget. When a device is connected to a port, its power requirements are detected by the switch before power is supplied. If the power required by a device exceeds the power budget of the port or the whole switch, power is not supplied

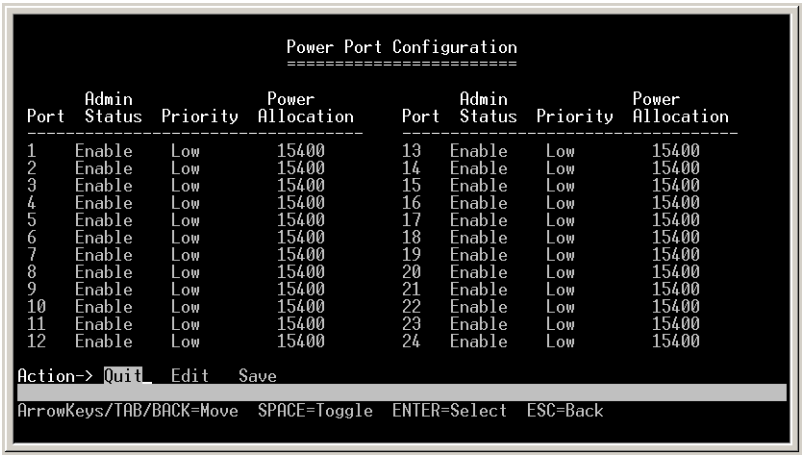
Port PoE Status

The *Power Port Status* screen allows you to view the current PoE settings for each port on the switch.



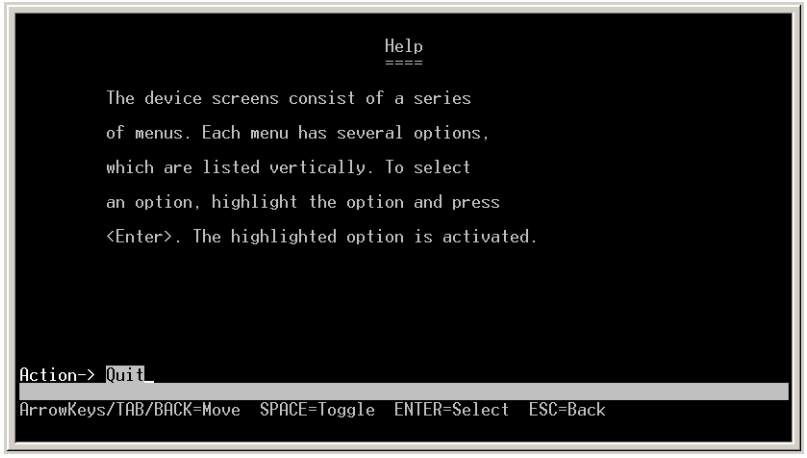
Ports can be set to one of three power priority levels: critical, high, or low. To control the power supply within the switch's budget, ports set at critical or high priority have power enabled in preference to those ports set at low priority. For example, when a device is connected to a port set to critical priority, the switch supplies the required power, if necessary by dropping power to ports set for a lower priority. If power is dropped to some low-priority ports and later the power demands on the switch fall back within its budget, the dropped power is automatically restored.

Port PoE Configuration



The *Power Port Configuration* screen allows you to set the PoE settings for each port. Select the **Edit** action and use the **Left**, **Right**, **Up**, and **Down** arrows to select the attribute you would like to set. You can set the Admin Status, the Priority, and the Power Allocation for each port. Use the **Save** action to save the new settings.

Help



Select **Help** and press the **Enter** key if you want to view the help information. This screen explains how to navigate the various screens of the console interface.

Log Out

Select **Log Out** to log out of the Console Configuration Utility.

Using the web-based Utility for Configuration

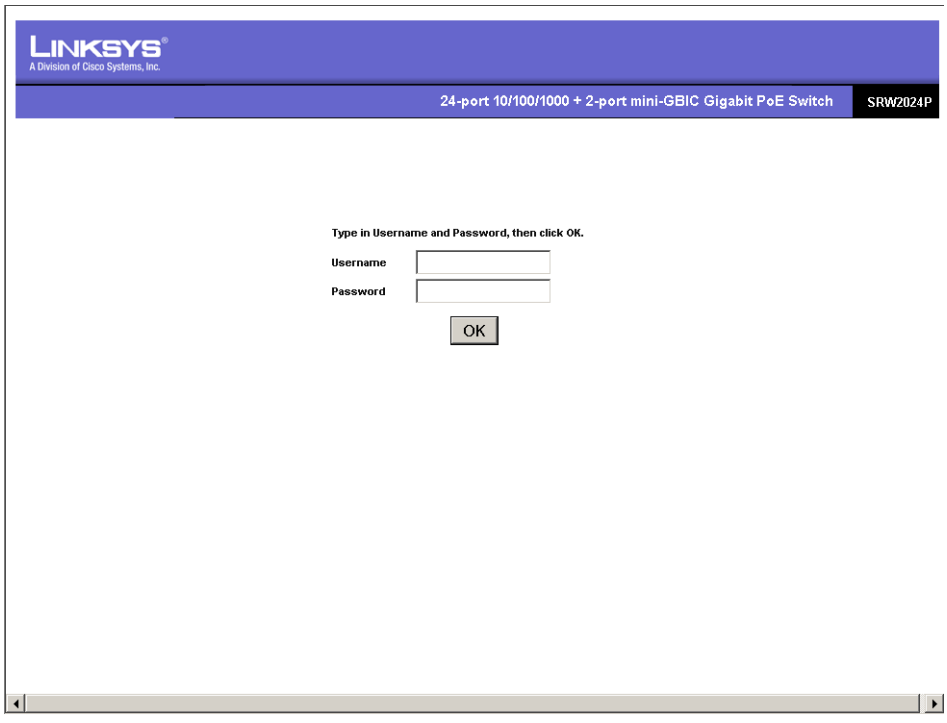
Overview

This chapter describes the features included in the web-based Utility. All of the features shown in this chapter, unless specifically identified, are included in the all of Fast Ethernet switches. Additional features for specific switches are noted.

Accessing the web-based Utility

NOTE: The web-based Utility is optimized for viewing with a screen resolution of 1024 x 768. Internet Explorer version 5.5 or above is recommended.

Open your web browser and enter **192.168.1.254** into the *Address* field. Press the **Enter** key and the *login* screen appears.



NOTE: The default IP address of the device is 192.168.1.254. If you have modified this address, enter the correct IP address. The device should be on the same subnet as the PC that is used for configuration.

The first time you open the web-based Utility, enter **admin** in the *User Name* field, and leave the *Password* field blank. Click the **OK** button. For security purposes, it is recommended that later you set a password from the *System Password* screen.

The first screen that appears is the *Setup Summary* screen. 13 main tabs are accessible from the web-based Utility: Setup, Port Management, VLAN Management, Statistics, ACL, Security, QoS (Quality of Service), Spanning Tree, Multicast, SNMP, Admin, and Logout. Click one of the main tabs to view additional tabs.

NOTE: After configuring values using the web-based Utility, you may be required to refresh the page to see the updated configuration.

The LEDs on the *Setup Summary* screen display status information about their corresponding ports.

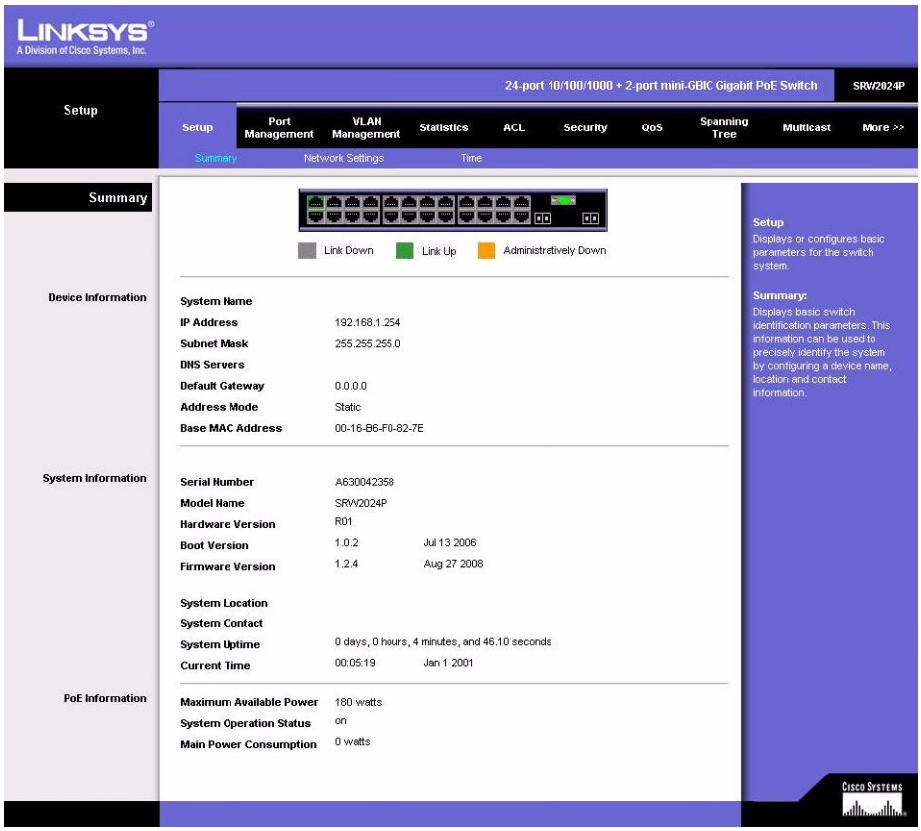
- A green LED indicates a connection
- A grey LED indicates no connection
- An orange LED indicates the port has been closed down by the administrator

When you click a port's LED, the statistics for that port are displayed.

NOTE: The LEDs displayed in the web-based Utility are not the same as the LEDs on the front panel of the switch.

Setup Tab - Summary

The *Summary* screen provides device and system information about the switch.



Device Information

System Name—Displays the name for the switch.

IP Address—The IP address of the switch.

Subnet Mask—The Subnet Mask of the switch.

DNS Servers—The DNS Servers are displayed here.

Default Gateway—The Default Gateway is displayed here.

Address Mode—Indicates whether the switch is configured with a Static or Dynamic IP address.

Base MAC Address—This is the MAC address of the switch.

System Information

Serial Number—The product's Serial Number is displayed here.

Model Name—This is the model number and name of the switch.

Hardware Version—The version number of the switch's hardware is displayed here.

Boot Version—This indicates the system boot version currently running on the device.

Firmware Version—The Firmware (software) version number is displayed here.

System Location—The system name is displayed here.

System Contact—The contact person for this switch is displayed here.

System Up Time—This field displays the amount of time that has elapsed since the switch was last reset.

Current Time—The system time is displayed here.

PoE Information

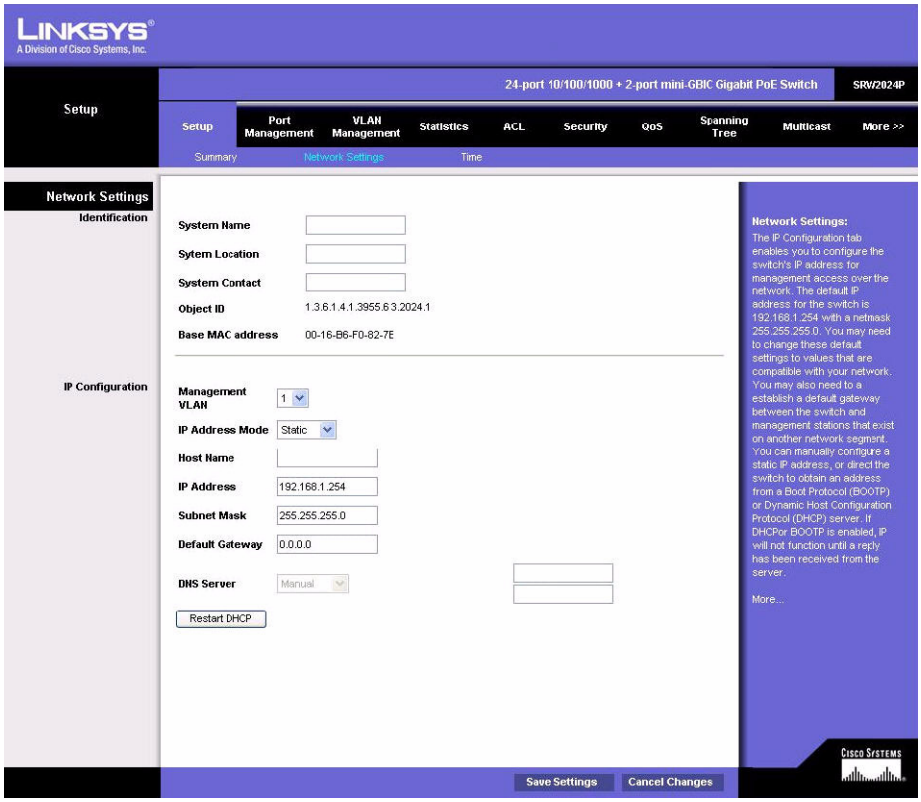
Maximum Available Power—This shows the maximum power that can be supplied to a connected PoE device.

System Operation Status—This shows whether the switch can provide PoE power or not.

Main Power Consumption—This shows the current number of watts that the switch is providing to PoE devices.

Setup Tab - Network Settings

The *Network Settings* screen allows you to assign DHCP or static IP settings to interfaces and assign default gateways.



Identification

System Name—This field allows you to assign a system name.

System Location—This field is used to enter a description of where the switch is located, such as 3rd floor.

System Contact—Enter the administrative contact person in this field.

System Object ID—The system object identifier is displayed here.

Base MAC Address—This is the MAC address of the switch.

IP Configuration

Management VLAN—This drop-down list allows you to select the Management VLAN.

IP Address Mode—This drop-down list allows you to select Static or Dynamic IP address configuration.

Host Name—Enter the DHCP Host Name here.

IP Address—If using a static IP address, enter the IP address here.

Subnet Mask—Enter the subnet mask of the currently configured IP address.

Default Gateway—Enter the IP address of the Default Gateway.

DNS Server—Enter the primary DNS Server information.

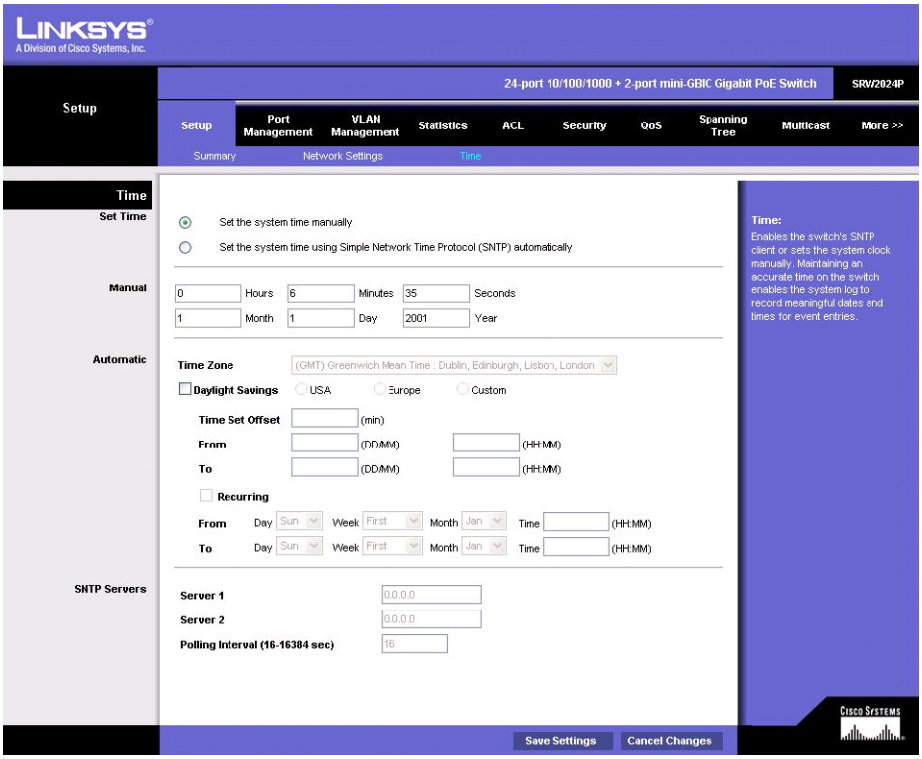
You can click **Restart DHCP** to assign a new IP address using DHCP.

Click the **Save Settings** button to save your changes or click **Cancel Changes** to discard the information.

Setup Tab - Time

The *Time* screen allows you to configure the time settings for the switch. Simple Network Time Protocol (SNTP) allows the switch to set its internal clock based on periodic updates from a time server (SNTP or NTP). Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. If the clock is not set, the switch records the time from the factory default set at the last bootup. When the SNTP client is enabled, the switch periodically sends a request for a time update to a configured time server. You can

configure up to two time server IP addresses. The switch attempts to poll each server in the sequence.



Set Time

Set the system time manually—When this option is selected, the local hardware clock is utilized.

Set the system time using Simple Network Time Protocol (SNTP) automatically. When this option is selected, the time is synchronized to an SNTP server.

Manual

Hours—The hour can be entered here.

Minutes—The minutes can be entered here.

Seconds—The seconds can be entered here.

Month—The month can be entered here.

Day—The day can be entered here.

Year—The year can be entered here.

Automatic

Time Zone—Select your time zone from the drop-down list.

Daylight Savings—Select **Daylight Savings** to enable it on the switch. If the switch should use US daylight savings, then select **USA**. If the switch should use EU daylight savings, then select **European**. If it should use another kind of daylight savings, then select **Custom** and complete the *From* and *To* fields.

Time Set Offset— For European or Custom daylight savings, specify the time change in minutes. The default is **60** minutes. You may enter **1-1440 minutes.**

From—If you selected Custom for the *Daylight Saving* setting, then enter the date and time when daylight savings begins.

To—If you selected Custom for the *Daylight Saving* setting, then enter the date and time when daylight savings ends.

Recurring—If you selected Custom for the *Daylight Saving* setting and daylight savings has the same start and end dates and times every year, then select **Recurring**.

From—If you selected Recurring, then enter the date and time when daylight savings begins.

To—If you selected Recurring, then enter the date and time when daylight savings ends.

SNTP Servers

Server1—Enter the the IP address of the primary SNTP server here.

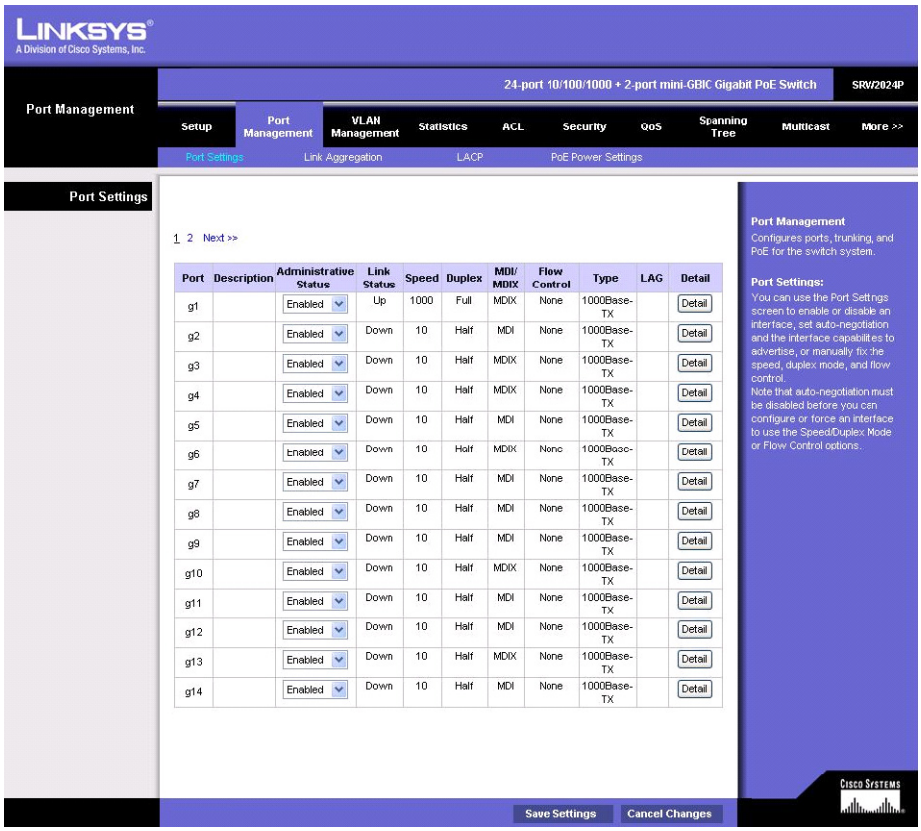
Server2—Enter the IP address of a secondary SNTP server here.

SNTP Polling Interval—The maximum number of seconds that the switch waits before polling the SNTP server. The default interval is every 1024 seconds (approximately 17 minutes). You may enter **60-86400 seconds.**

Click the **Save Settings** button to save your changes or click **Cancel Changes** to discard the information.

Port Management Tab - Port Settings

The *Port Management - Port Settings* screen shows you the settings for each of the switch's ports.



Port—The number of the port. To use an SFP module, click on the **Detail** button of the appropriate port (g1, g2).

Description—Displays a brief description of the port (can be entered by clicking on the **Detail** button).

Administrative Status—The port can be taken offline by selecting the Disabled option. When Enabled is selected, the port can be accessed normally.

Link Status—Up indicates a port has an active connection, Down indicates there is no active connection or the port has been taken offline by an Administrator.

Speed—The connection speed of the port is displayed here. The speed can be configured only when auto-negotiation is disabled on that port.

Duplex—This is the port duplex mode, Full (transmission occurs in both directions simultaneously) or Half (transmission occurs in only one direction at a time). This mode can be configured only when auto-negotiation is disabled and port speed is set to 10Mbps or 100Mbps. It cannot be configured on Link Aggregation Groups (LAGs).

MDI/MIDX—This is the MDI/MDIX status of the port. The MDI setting is used if the port is connected to an end station. The MDIX setting is used if the port is connected to a hub or another switch.

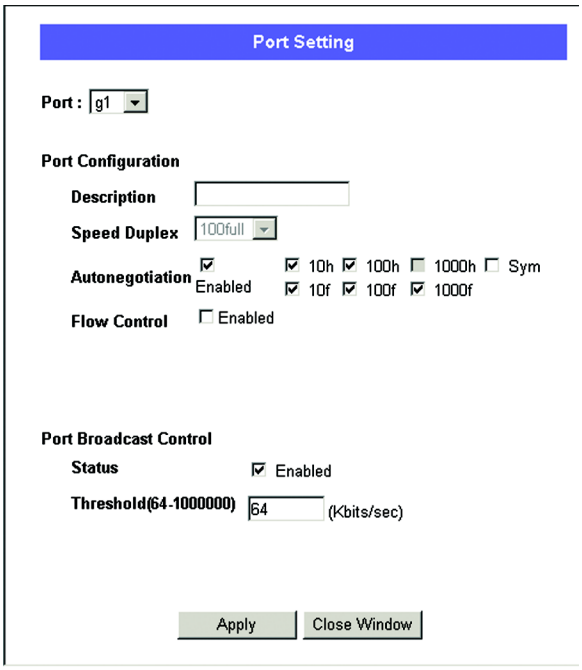
Flow Control—This is the flow control status of the port. It is active when the port uses Full Duplex Mode.

Type—Displays the port type.

LAG—This indicates if the port is part of a LAG.

Detail—The Detail button will open the Port Setting screen.

Port Setting



Port—Select the number of the port from the drop-down list.

Description—Allows you to describe an interface. (Range: 1-64 characters)

Port Type—This is the port type.

Speed Duplex—Allows you to manually set the port speed and duplex mode. (i.e., with auto-negotiation disabled)

Auto-negotiation (Port Capabilities)—Allows auto-negotiation to be enabled/disabled. When auto-negotiation is enabled, you need to specify the capabilities to be advertised. When auto-negotiation is disabled, you can force the settings for speed, mode, and flow control. The following capabilities are supported.

- **10half**—Supports 10 Mbps half-duplex operation
- **10full**—Supports 10 Mbps full-duplex operation
- **100half**—Supports 100 Mbps half-duplex operation
- **100full**—Supports 100 Mbps full-duplex operation

- **1000half**—Supports 1000 Mbps half-duplex operation
- **1000full**—Supports 1000 Mbps full-duplex operation
- **Sym** (Gigabit only)—Check this box to transmit and receive pause frames, or uncheck the box to auto-negotiate the sender and receiver for asymmetric pause frames. (The current switch chip supports only symmetric pause frames.)

Flow Control—Enables flow control. Flow control can eliminate frame loss by "blocking" traffic from end stations or segments connected directly to the switch when its buffers fill. When this feature is enabled, back pressure is used for half-duplex operation and IEEE 802.3x for full-duplex operation. Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise, back pressure jamming signals may degrade overall performance for the segment attached to the hub.

Default—**Autonegotiation enabled**— Advertised capabilities for 100Base-TX – 10half, 10full, 100half, 100full; 1000Base-T – 10half, 10full, 100half, 100full, 1000full; 1000Base-SX/LX/LH – 1000full)

Port Broadcast Control

You can protect your network from broadcast storms by setting a threshold for broadcast traffic for all ports. Any broadcast packets exceeding the specified threshold will then be dropped.

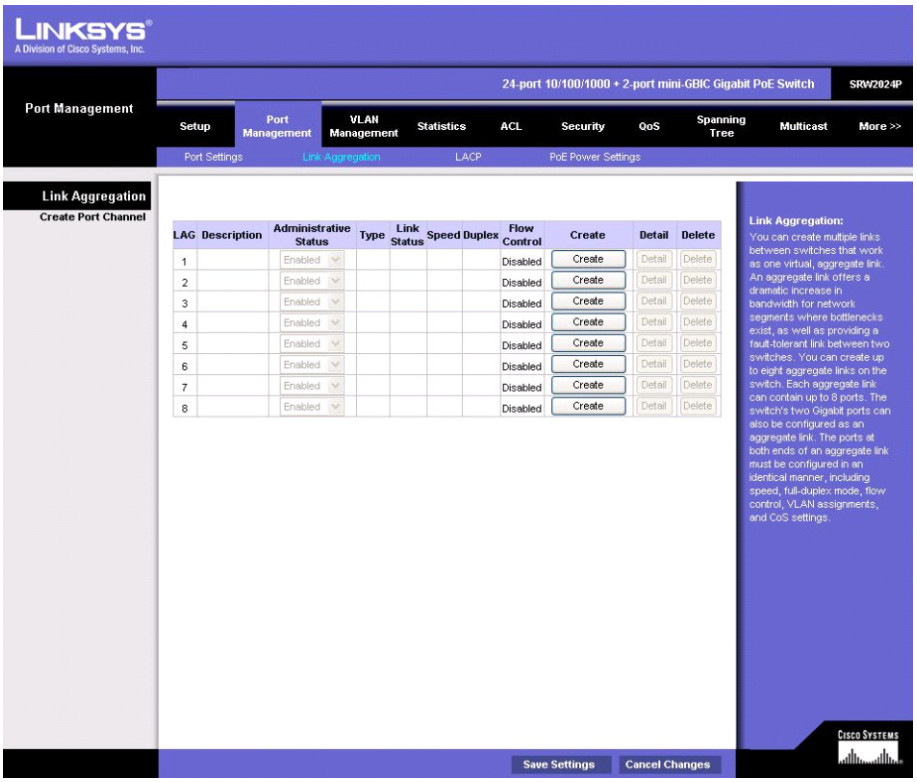
Status—To enable broadcast control on a specified port, select **Enabled** for that port.

Threshold—Set the threshold using the *Threshold* field. You may enter 64-1000000 K/bits/sec.

After you modify the required port settings, click **Apply**, or click **Close** to close the screen without saving any changes.

Click the **Save Settings** button to save your changes or click **Cancel** Changes

Port Management Tab - Link Aggregation

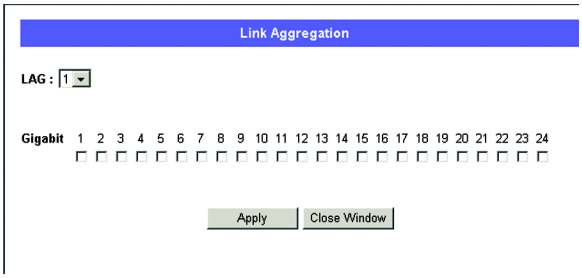


LAG—This indicates if the port is part of a LAG.

Description—Description for this LAG.

Administrative Status—The admin status of the LAG. Up indicates that the LAG is available. Down indicates that administrator has taken the port offline. When modifying the option, be sure to click the **Save Settings** option.

Type—The type of LAG is displayed here.



Link Status—The link status is displayed here.

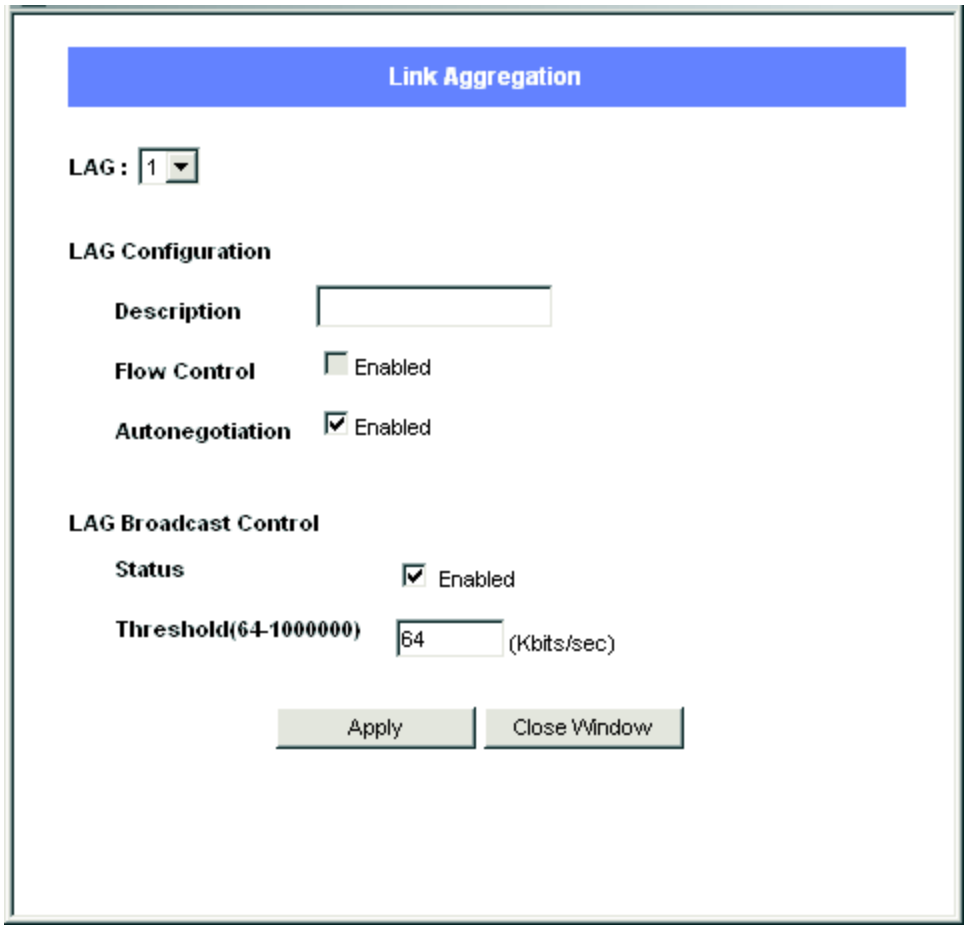
Speed—The connection speed is displayed here.

Duplex—The connection duplex is displayed here.

Flow Control—This is the flow control status of the LAG. It is active when the port uses Full Duplex Mode.

Create—To create a new LAG, click the **Create** button in the Create column, then add members to the LAG by clicking on the Select Member button. The *Select Member* screen for the Link Aggregation opens.

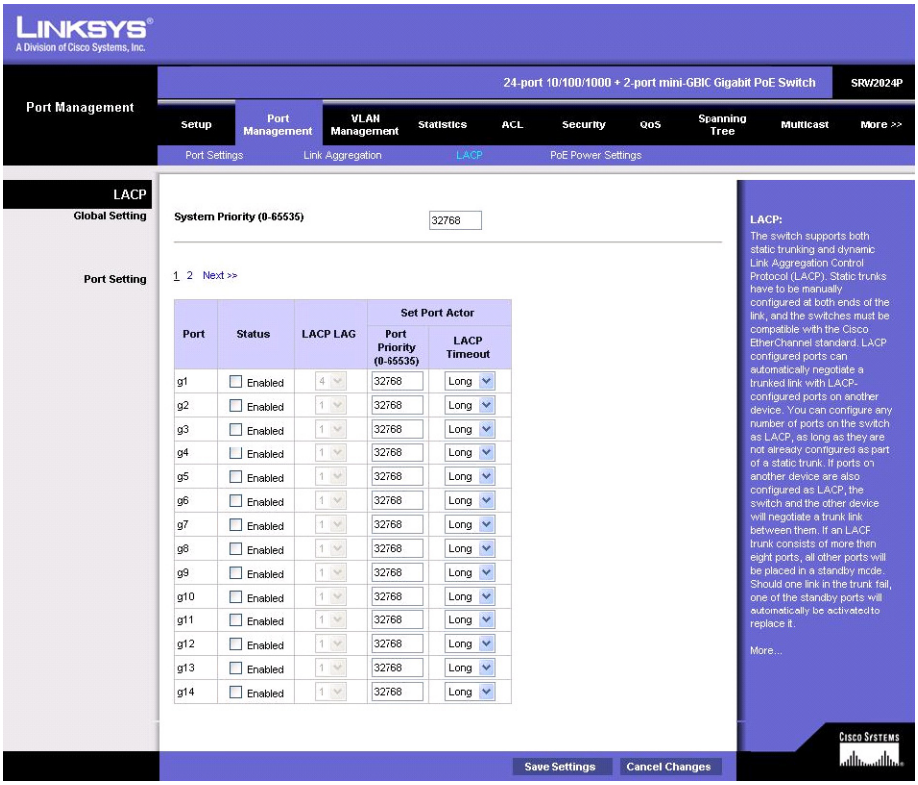
Detail—To configure the LAG and the LAG broadcast control, click the **Detail** button. The *detail* screen for the LAG opens. Assign up to 8 ports to the LAG by selecting the ports, then click **Apply**.



Port Management Tab - LACP

Ports can be statically grouped into an aggregate link (that is, LAG) to increase the bandwidth of a network connection or to ensure fault recovery. Or you can use the Link Aggregation Control Protocol (LACP) to automatically negotiate a LAG link between the switch and another network device. For static LAGs, the switches have to comply with the Cisco EtherChannel standard. For dynamic LAGs, the switches have to comply with LACP. This switch supports up to

eight LAGs. For example, a LAG consisting of two 1000 Mbps ports can support an aggregate bandwidth of 4 Gbps when operating at full duplex.



To avoid creating a loop in the network, be sure you enable LACP before connecting the ports, and also disconnect the ports before disabling LACP.

Global Setting

System Priority—Indicates the global LACP priority value. The possible range is 1- 65535. The default value is 1.

Port Setting

Set the System Priority and Port Priority for the Port Actor. After you have completed setting the port LACP parameters, click **Save Settings**.

Port—Defines the port number to which timeout and priority values are assigned.

Status—Select **Enabled** to enable the port.

Set Port Actor—This menu sets the local side of an aggregate link; that is, the ports on this switch.

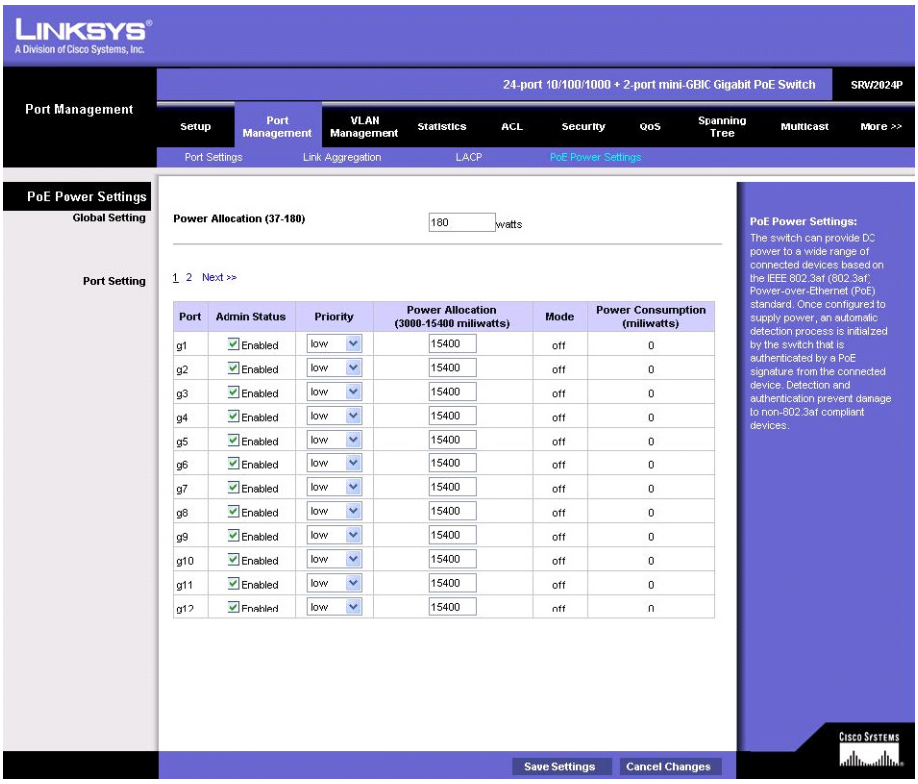
Port Priority—Defines the LACP priority value for the port. The field range is 1-65535.

LACP Timeout—Administrative LACP timeout. A short or long timeout value can be selected. Long is the default.

Port Management Tab - PoE Power Settings

If a device is connected to a switch port and the switch detects that it requires more than the power budget of the port, no power is supplied to the device (that is, port power remains off).

If the power demand from devices connected to switch ports exceeds the power budget set for the switch, the port power priority settings are used to control the supplied power.



Select **Enabled** to enable PoE power on selected ports, set the priority using the drop-down list provided, and set the power allocation for each port.

Port—Displays the port number.

Admin Status—Select **Enabled** to enable PoE power to be supplied to the connected device.

Priority—Set the priority of the supply using the drop-down list.

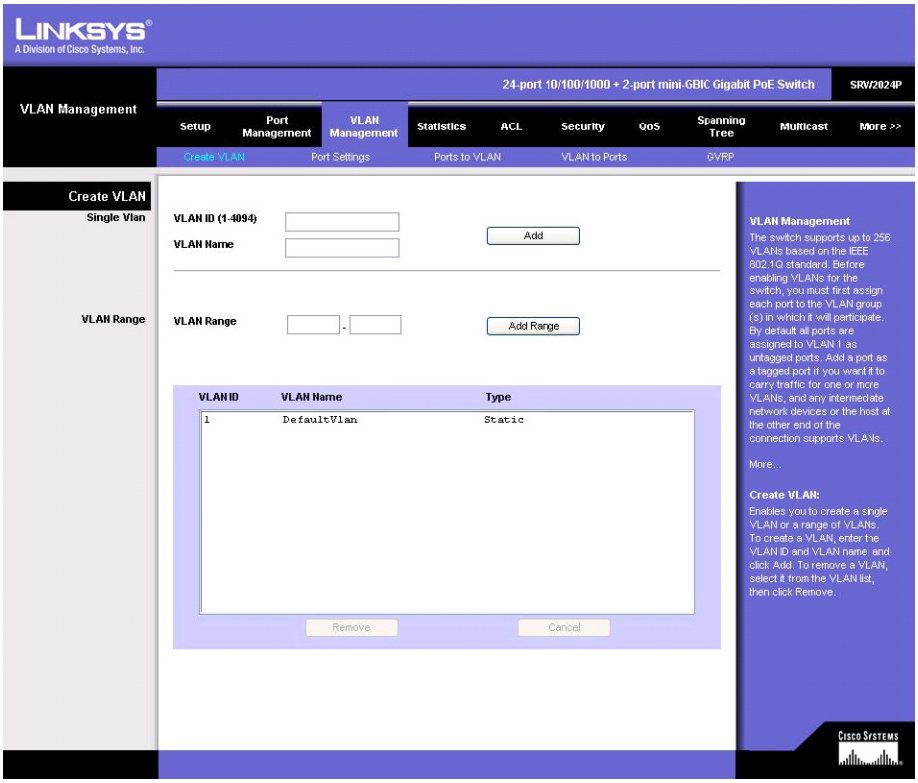
Power Allocation—Set the maximum power that can be supplied to the port, (3000-15400 milliwatts).

Mode—Displays whether the connected PoE device is on or off.

Power Consumption (milliwatts)—Displays the power currently being used by the connected PoE device.

VLAN Management Tab - Create VLAN

The *Create VLAN* screen provides information and global parameters for configuring and working with VLANs.



Single VLAN

VLAN ID (2-4094)—Indicates the ID number of the VLAN being configured. Up to 256 VLANs can be created. This field is used to add VLANs one at a time. To add the defined VLAN ID number, click the **Add** button.

VLAN Name—Displays the user-defined VLAN name.

VLAN Range

VLAN Range—Indicates a range of VLANs being configured. To add the defined range of VLAN ID numbers, press the **Add Range** button.

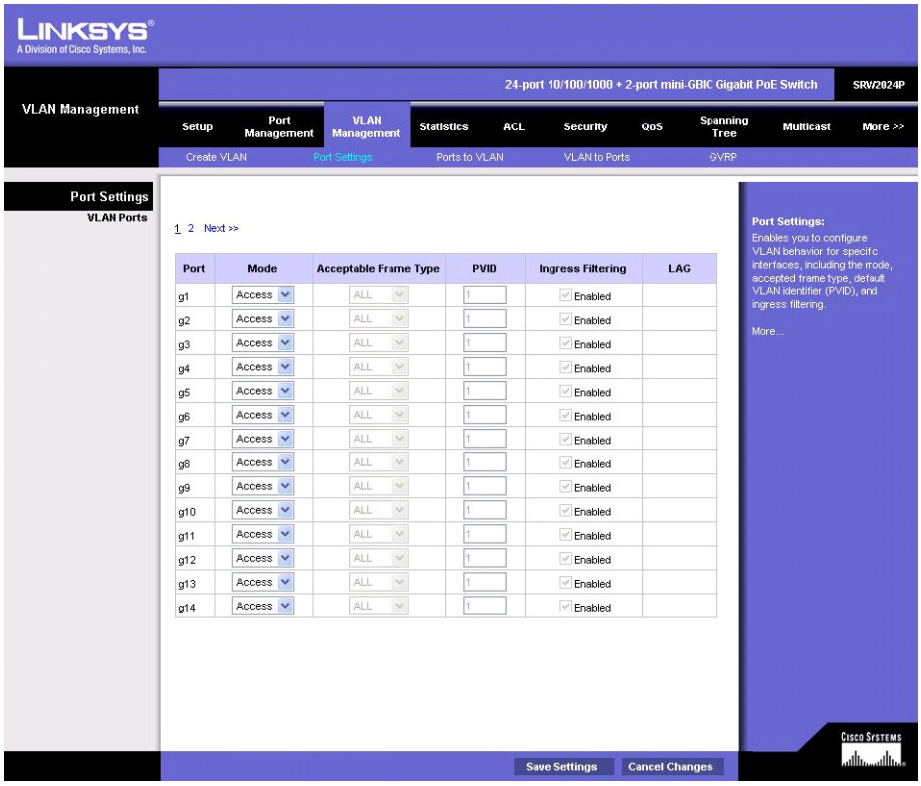
VLAN Table

The VLAN Table displays a list of all configured VLANs. The VLAN ID, VLAN Name, and status of the VLAN are displayed here. To remove a VLAN, click the **Remove** button.

NOTE: VLANs that are created dynamically using GVRP are assigned a VLAN name "Undefined".

VLAN Management Tab - Port Settings

The *VLAN Port Settings* screen provides parameters for managing ports that are part of a VLAN. The port default VLAN ID (PVID) is configured on the VLAN Port Settings screen. All untagged packets arriving to the device are tagged by the ports PVID.



Port—The port number included in the VLAN.

Mode—Indicates the port mode. Possible values are:

- **General—**The port belongs to VLANs, and each VLAN is user-defined as tagged or untagged (full 802.1Q mode).
- **Access—**The port belongs to a single untagged VLAN. When a port is in Access mode, the packet types which are accepted on the port (packet type) cannot be designated. It is also not possible to enable/disable ingress filtering on an access port.
- **Trunk—**The port belongs to VLANs in which all ports are tagged (except for an optional single native VLAN).

Acceptable Frame Type—Packet type accepted on the port. Possible values are:

- **Admit Tag Only—**Indicates that only tagged packets are accepted on the port.
- **Admit All—**Indicates that both tagged and untagged packets are accepted on the port.

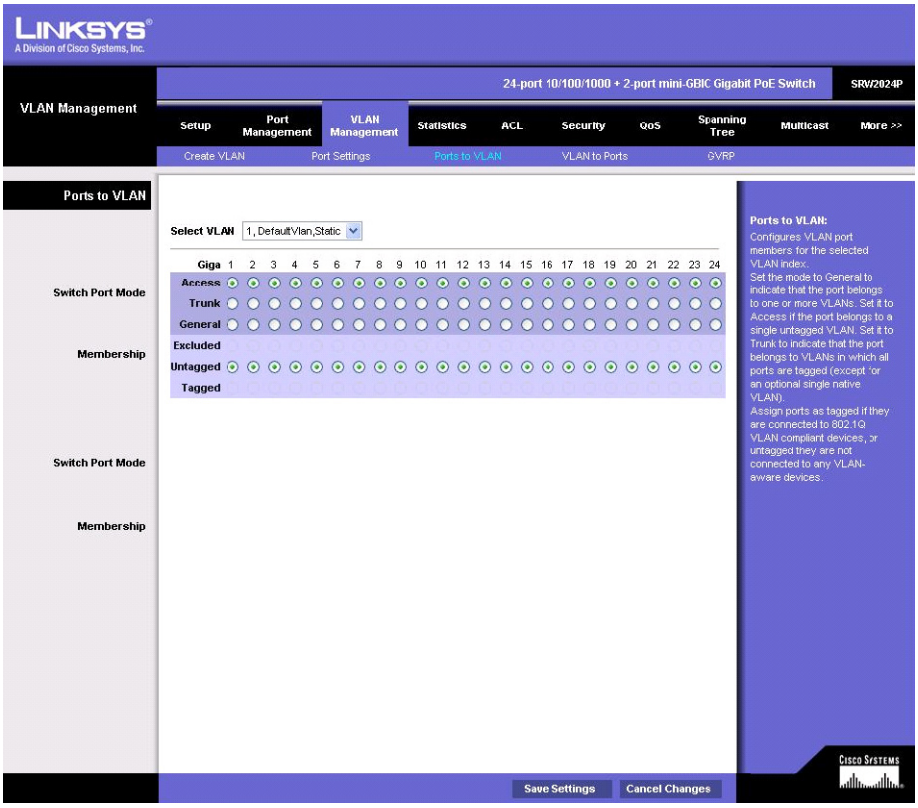
PVID—Assigns a VLAN ID to untagged packets. The possible values are 2 to 4094. VLAN 4095 is defined as per standard and industry practice as the discard VLAN. Packets classified to the Discard VLAN are dropped.

Ingress Filtering—Enables or disables Ingress filtering on the port. Ingress filtering discards packets which do not include an ingress port.

LAG—Indicates the LAG to which the VLAN is defined.

VLAN Management Tab - Ports to VLAN

Use the *Port to VLAN* screen to configure port members for the selected VLAN index. Assign ports as tagged if they are connected to 802.1Q VLAN compliant devices, or untagged they are not connected to any VLAN-aware devices.



Select VLAN—Select the VLAN number. from the drop-down list.

Switch Port Mode

Indicates VLAN membership mode for an interface. (Default: Access) Possible values are:

Access—Indicates the port belongs to a single untagged VLAN. When a port is in Access mode, the packet types which are accepted on the port cannot be designated. Ingress filtering cannot be enabled/disabled on an access port.

Trunk—Indicates the port belongs to VLANs in which all ports are tagged, except for one port that can be untagged.

General—Indicates the port belongs to VLANs, and each VLAN is user-defined as tagged or untagged (full 802.1Q mode).

Membership

Select VLAN membership for each interface by marking the appropriate radio button for a port or LAG, possible values are:

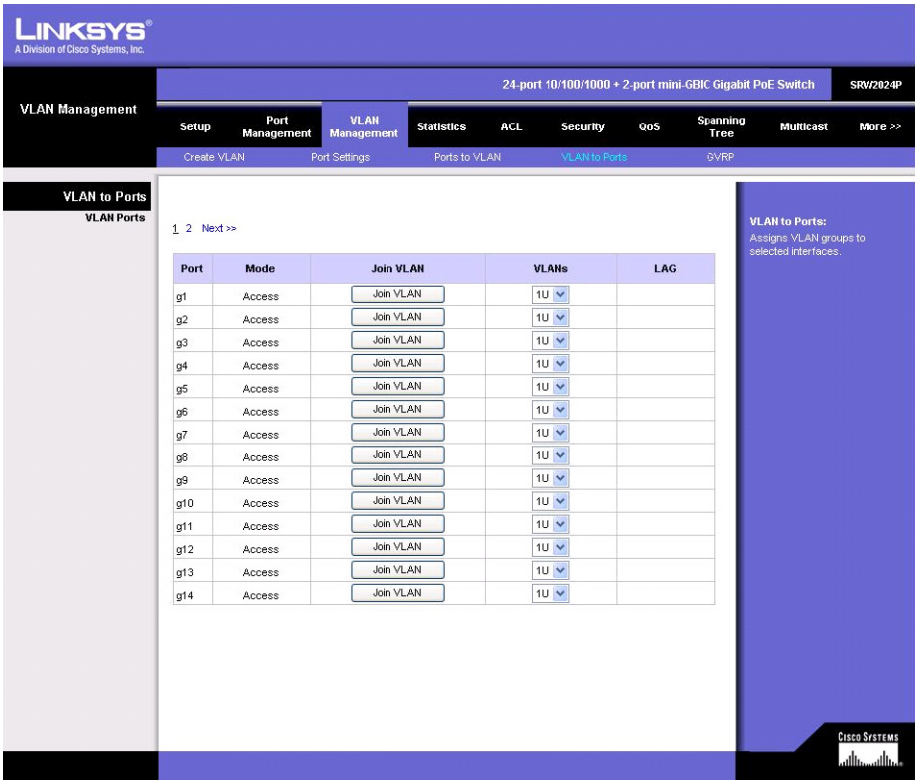
Excluded—Excludes the interface from the VLAN. However, the interface can be added to the VLAN through GVRP.

Untagged—Packets forwarded by the interface are untagged.

Tagged—Defines the interface as a tagged member of a VLAN. All packets forwarded by the interface are tagged. The packets contain VLAN information.

VLAN Management Tab - VLAN to Ports

The *VLAN to Ports* screen contains fields for configuring VLANs to a ports.



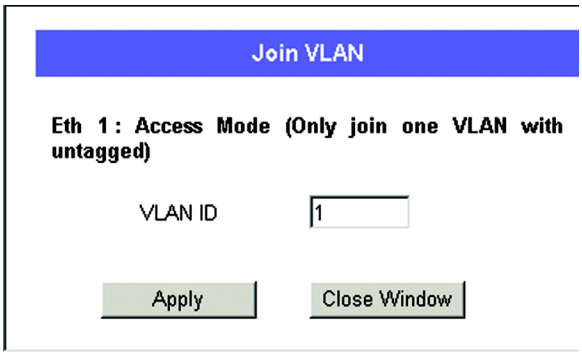
Port—Displays the interface number.

Mode—Indicates the port to VLAN mode. The possible field values are:

- **General—**Indicates the port belongs to VLANs, and each VLAN is user-defined as tagged or untagged (full 802.1Q mode).
- **Access—**Indicates the port belongs to a single untagged VLAN. When a port is in Access mode, the packet types which are accepted on the port cannot be designated. Ingress filtering cannot be enabled/disabled on an access port.

- **Trunk—**Indicates the port belongs to VLANs in which all ports are tagged, except for one port that can be untagged.

Join VLAN—Defines the VLANs to which the interface is joined. Select the VLAN ID, then click **Apply**.



VLANs—Displays the PVID tag.

LAG—Indicates if the port is a member of a LAG. If it is a member of a LAG, it cannot be configured to a VLAN. The LAG to which it belongs can be configured to a VLAN.

VLAN Management Tab—GVRP

The GVRP screen contains fields for configuring GVRP on each port. GVRP defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network.

Port—Displays the interface number.

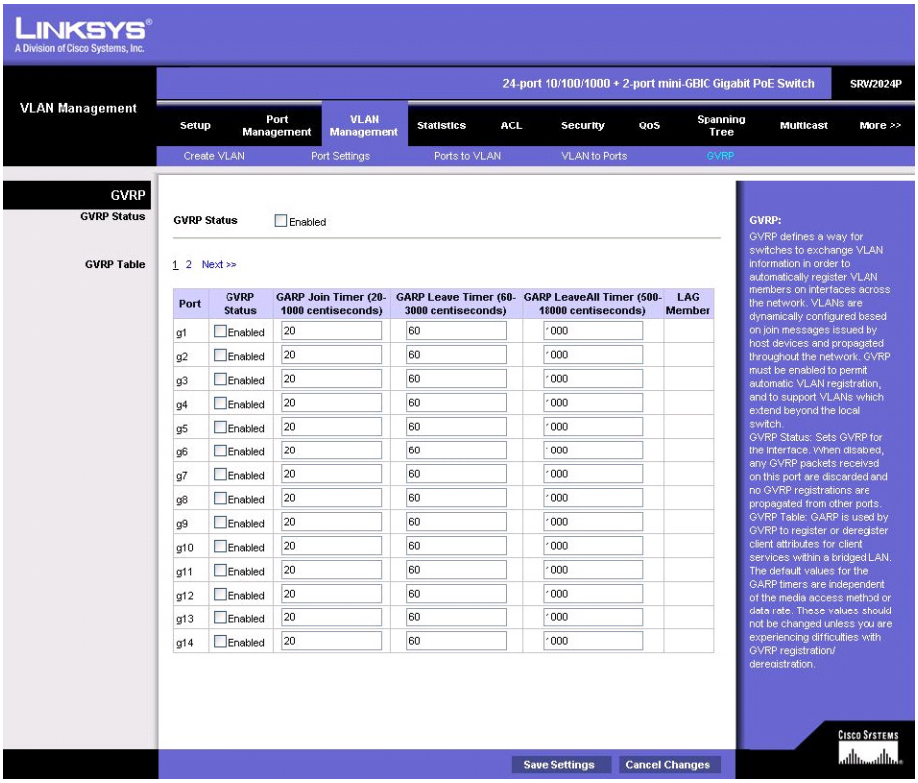
GVRP Status—Enables/disables GVRP for the interface. When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports.

GARP Join Timer (Centi Seconds) (20-1000)—The interval between transmitting requests/queries to participate in a VLAN group. The possible range is 20-1000 centiseconds. The default value is 20 centiseconds.

GARP Leave Timer (Centi Seconds) (60-3000)—The interval a port waits before leaving a VLAN group. This time should be set to more than twice the join time. This ensures that after a Leave or LeaveAll message has been issued, the applicants can rejoin before the port actually leaves the group. The possible range is 60-3000 centiseconds. The default value is 60 centiseconds.

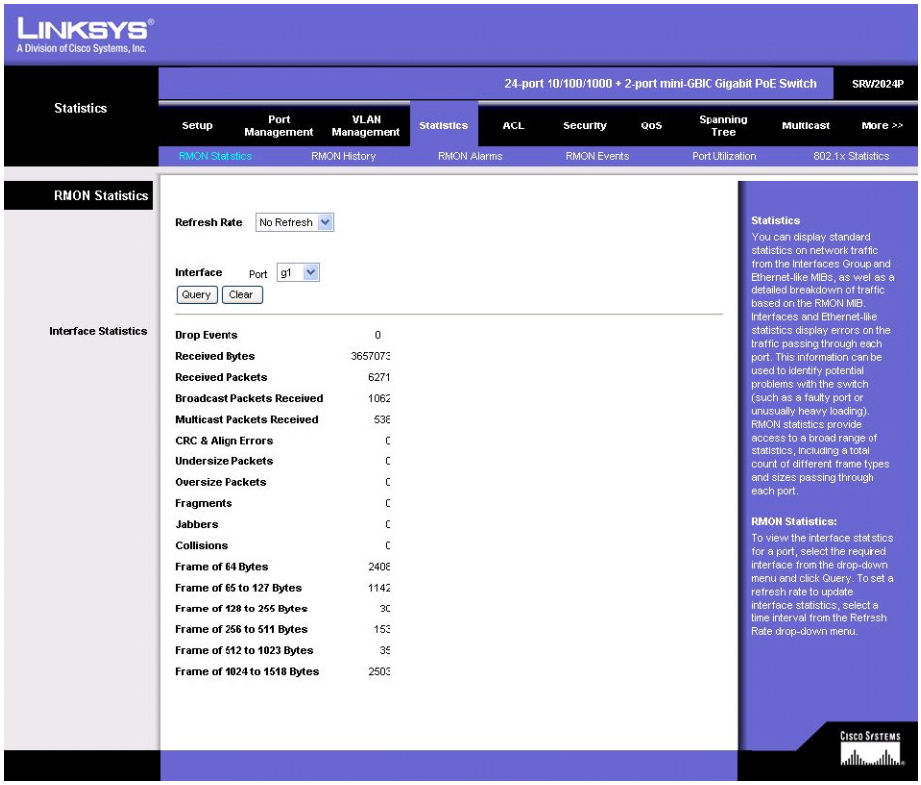
GARP LeaveAll Timer (Centi Seconds) (500-18000)—The interval between sending out a LeaveAll query message for VLAN group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group. The possible range is 500-18000 centiseconds. The default value is 1000 centiseconds.

LAG—Indicates if the port is a member of a LAG. If it is a member of a LAG, GVRP cannot be configured on it.



Statistics Tab - RMON Statistics

The *RMON Statistics* screen contains fields for viewing information about device utilization and errors that occurred on the device.



To view the interface statistics for a port, select the required interface from the drop-down list and click **Query**. To set a refresh rate or to update the interface statistics, select a time interval from the Refresh Rate drop-down list.

Refresh Rate—Defines the amount of time that passes before the interface statistics are refreshed. The possible field values are:

- **No Refresh**—Indicates that the RMON statistics are not refreshed.
- **15 Sec—**Indicates that the RMON statistics are refreshed every 15 seconds.
- **30 Sec—**Indicates that the RMON statistics are refreshed every 30 seconds.
- **60 Sec—**Indicates that the RMON statistics are refreshed every 60 seconds.

Interface—Indicates the device for which statistics are displayed. The possible field values are:

- **Port—**Defines the specific port for which RMON statistics are displayed.
- **LAG—**Defines the specific LAG for which RMON statistics are displayed.

Drop Events—Displays the number of dropped events that have occurred on the interface since the device was last refreshed.

Received Bytes (Octets)—Displays the number of octets received on the interface since the device was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.

Received Packets—Displays the number of packets received on the interface, including bad packets, multicast and broadcast packets, since the device was last refreshed.

Broadcast Packets Received—Displays the number of good broadcast packets received on the interface since the device was last refreshed. This number does not include Multicast packets.

Multicast Packets Received—Displays the number of good Multicast packets received on the interface since the device was last refreshed.

CRC & Align Errors—Displays the number of CRC and Align errors that have occurred on the interface since the device was last refreshed.

Undersize Packets—Displays the number of undersized packets (less than 64 octets) received on the interface since the device was last refreshed.

Oversize Packets—Displays the number of oversized packets (over 1518 octets) received on the interface since the device was last refreshed.

Fragments—Displays the number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received on the interface since the device was last refreshed.

Jabbers—Displays the total number of received packets that were longer than 1518 octets. This number excludes frame bits, but includes FCS octets that had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. The field range to detect jabbers is between 20 ms and 150 ms.

Collisions—Displays the number of collisions received on the interface since the device was last refreshed.

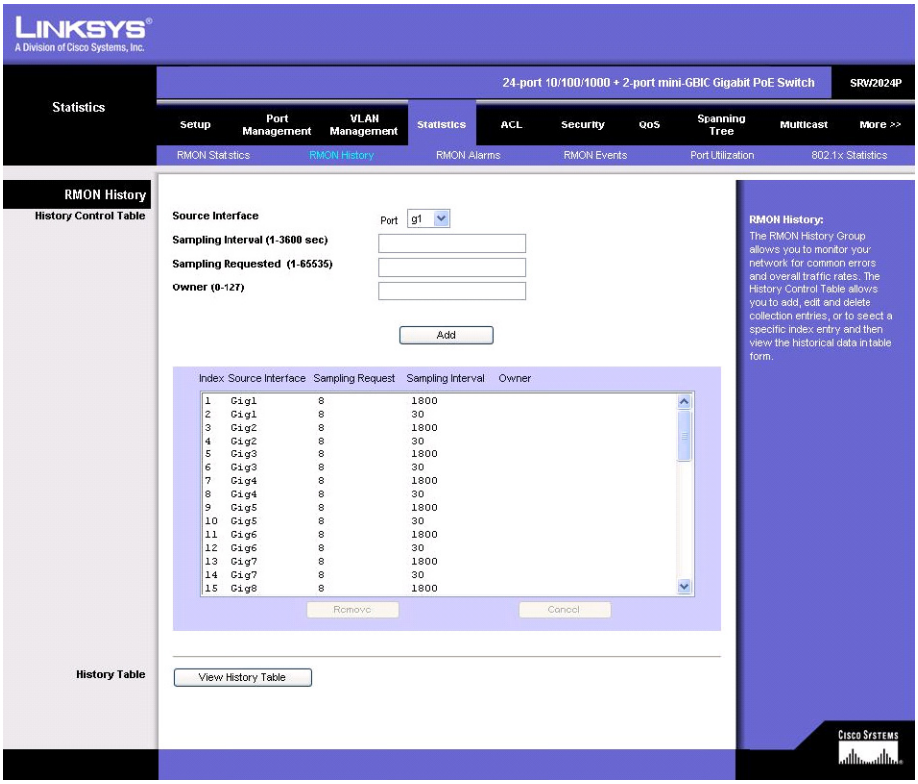
Frames of xx Bytes—Number of xx-byte frames received on the interface since the device was last refreshed.

Clear Counters—This option will reset all of the statistic counts.

Refresh Now—Use this option to refresh the statistics.

Statistics Tab - RMON History

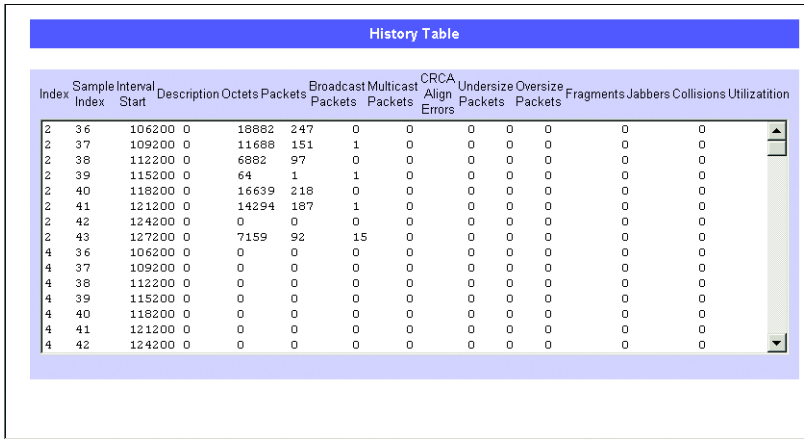
The *RMON History* screen allows you to monitor your network for common errors and overall traffic rates. The History Control Table allows you to add, edit and delete collection entries, or to select a specific index entry and then view the historical data in table form.



History Control Table

Source Interface—Displays the interface from which the history samples were taken. The possible field values are:

- **Port—**Specifies the port from which the RMON information was taken.
- **LAG—**Specifies the port from which the RMON information was taken.



Sampling Interval—Indicates (in seconds) the time that samplings are taken from the ports. The field range is 1-3600. The default is 1800 seconds (30 minutes).

Sampling Requested—Indicates the number of samples to save. (Range:1-65535)

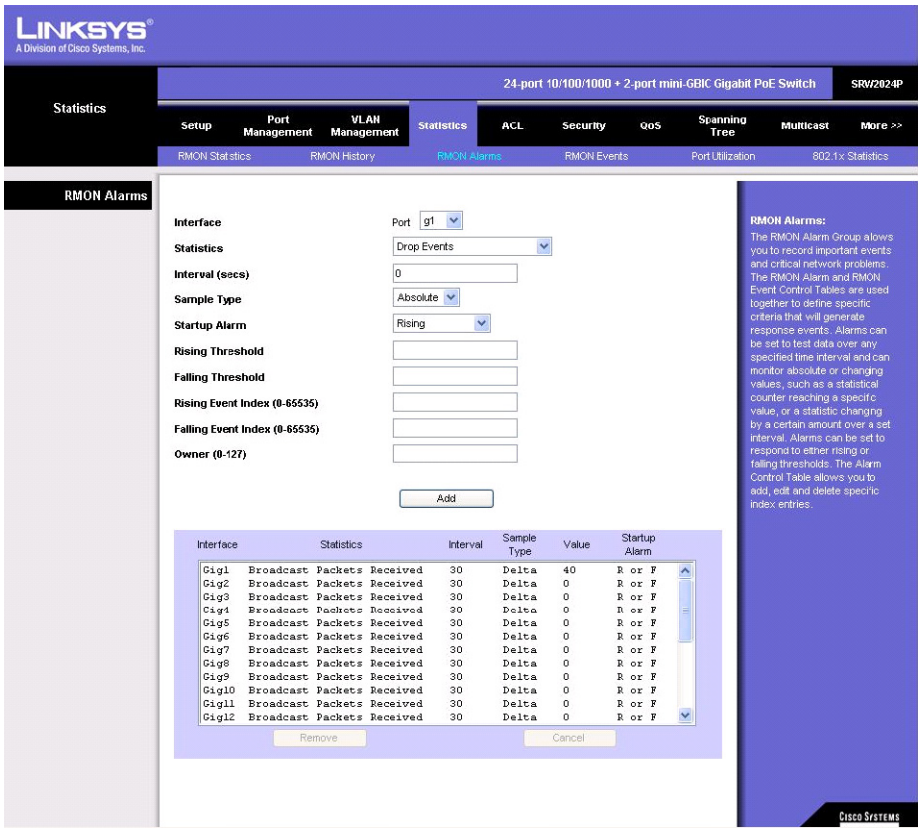
Owner—The name of the person who created this entry in the Control Table. (Maximum 127 characters)

Add to List—Adds the configured RMON sampling to the Log Table at the bottom of the screen.

View History Table—This button opens the History Table screen. The History Control Table allows you to add, edit and delete collection entries, or to select a specific index entry and then view the historical data in table form. The History Table lists the Index, Sample Index, Interval Start, Description, Octets, Packets, Broadcast Packets, Multicast Packets, CRCA Align Errors, Undersize Packets, Oversize Packets, Fragments, Jabbers, Collisions, and Utilization.

Statistics Tab - RMON Alarm

The *RMON Alarm* screen contains fields for setting network alarms. Network alarms occur when a network problem, or event, is detected. Rising and falling thresholds generate events.



The *RMON Alarms* screen allows you to record important events and critical network problems. The RMON Alarm and Event Control Tables are used together to define specific criteria that will generate response events.

Alarms can be set to test data over any specified time interval and can monitor absolute or changing values, such as a statistical counter reaching a specific value, or a statistic changing by a certain amount over a set interval. Alarms can be set to respond to either rising or falling thresholds.

The Alarm Control Table allows you to add, update and delete specific index entries.Interface. The selected interface on the switch.

Interface—Displays the interface for which RMON statistics are displayed. The possible field values are:

- **Port—**Displays the RMON statistics for the selected port.
- **LAG—**Displays the RMON statistics for the selected LAG.

Statistics—The traffic statistics to be sampled. Select from the drop-down list.

Interval—The time interval in seconds over which data is sampled and compared with the rising or falling threshold.

Sample Type—Defines the sampling method for the selected variable and comparing the value against the thresholds. The possible field values are:

- **Absolute—**Compares the values directly with the thresholds at the end of the sampling interval.
- **Delta—**Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold.

Startup Alarm—Determines how the alarm is activated when the variable is compared to the thresholds. This can be set to Rising, Falling, or Rising or Falling.

Rising Threshold—An alarm threshold for the sampled variable. If the current value is greater than or equal to the threshold, and the last sample value was less than the threshold, then an alarm will be generated. (After a rising event has been generated, another such event will not be generated until the sampled value has fallen below the Rising Threshold and reaches the Falling Threshold.)

Falling Threshold—An alarm threshold for the sampled variable. If the current value is less than or equal to the threshold, and the last sample value was greater than the threshold, then an alarm will be generated. (After a falling event has been generated, another such event will not be generated until the sampled value has risen above the Falling Threshold and reaches the Rising Threshold.)

Rising Event Index—Displays the mechanism in which the alarms are reported. The possible field values are:

- **LOG—**Indicates there is not a saving mechanism for either the device or in the management system. If the device is not reset, the entry remains in the Log Table.
- **TRAP—**Indicates that an SNMP trap is generated, and sent via the Trap mechanism. The Trap can also be saved using the Trap mechanism.

Both—Indicates that both the Log and Trap mechanisms are used to report alarms.

Falling Event—The index of the Event that will be used if a falling alarm is triggered. If there is no corresponding entry in the Event Control Table, or if this number is zero, then no event will be generated.

Owner—The name of the person who created this entry in the Control Table. (Maximum 127 characters)

Falling Event Index—Displays the mechanism in which the alarms are reported. The possible field values are:

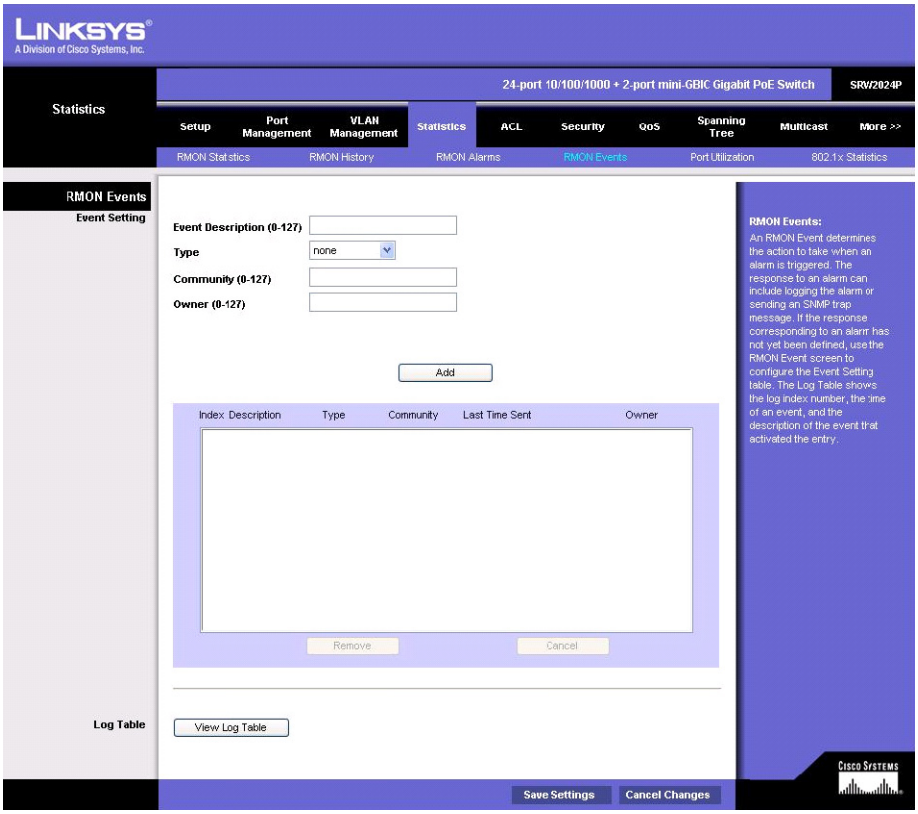
- **LOG—**Indicates there is not a saving mechanism for either the device or in the management system. If the device is not reset, the entry remains in the Log Table.
- **TRAP—**Indicates that a SNMP trap is generated, and sent via the Trap mechanism. The Trap can also be saved using the Trap mechanism.
- **Both**—Indicates that both the Log and Trap mechanism are used to report alarms.

Owner—Displays the device or user that defined the alarm.

The **Add** button adds the entry to the RMON Alarms Table.

Statistics Tab - RMON Events

The *RMON Events* screen contains fields for defining RMON events. An RMON Event determines the action to take when an alarm is triggered. The response to an alarm can include logging the alarm or sending an SNMP trap message.



Event Setting

Event Description—Displays the user-defined event description.

Type—Describes the event type. Possible values are:

- **None—**Indicates that no event occurred.
- **Log—**Indicates that the event is a log entry.
- **Trap—**Indicates that the event is a trap.
- **Log and Trap**—Indicates that the event is both a log entry and a trap.

Community—Displays the community to which the event belongs.

Owner—Displays the device or user that defined the event. (Maximum 127 characters).

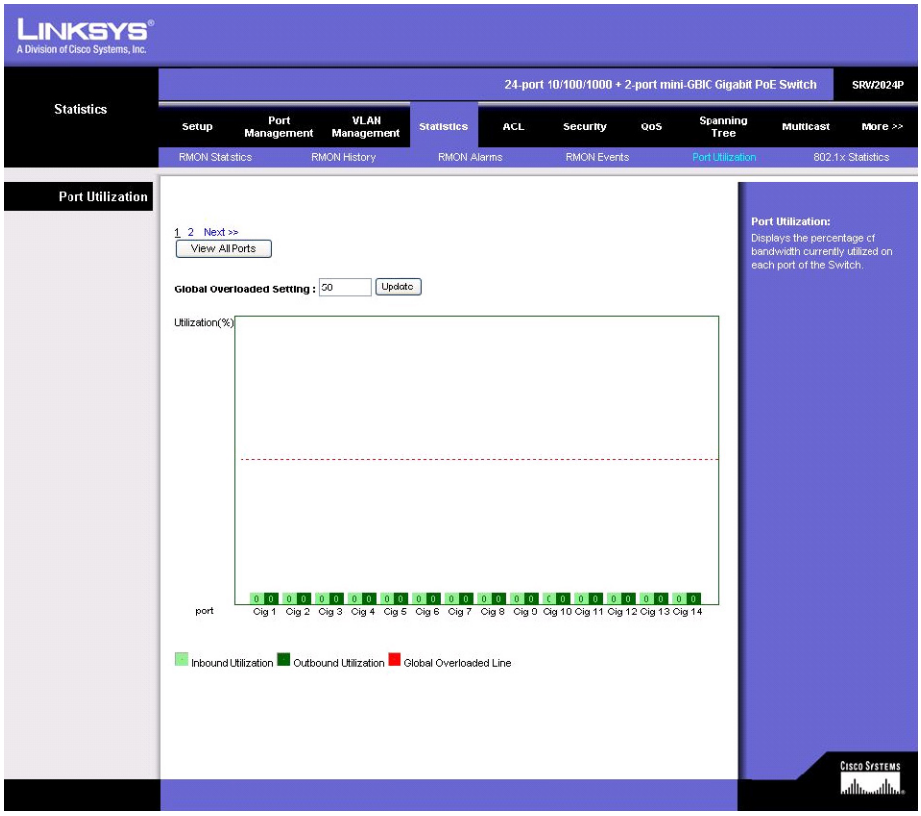
The **Add** button adds the configured RMON event to the Event Table at the bottom of the screen.

The Event Table area contains Index, Description, Type, Community, Last Time Sent, Owner.

To display each time an event was triggered by an alarm, first highlight an entry in the Event Control Table and then click on the **View Log Table** button. The Log Table shows the log index number, the time of an event, and the description of the event that activated the entry.

Statistics Tab - Port Utilization

The *Port Utilization* screen displays the amount of resources each interface is currently consuming. Ports in green are functioning normally, while ports in red are currently transmitting an excessive amount of network traffic.



Click the **View All Ports** button to view all 24 ports on the screen.

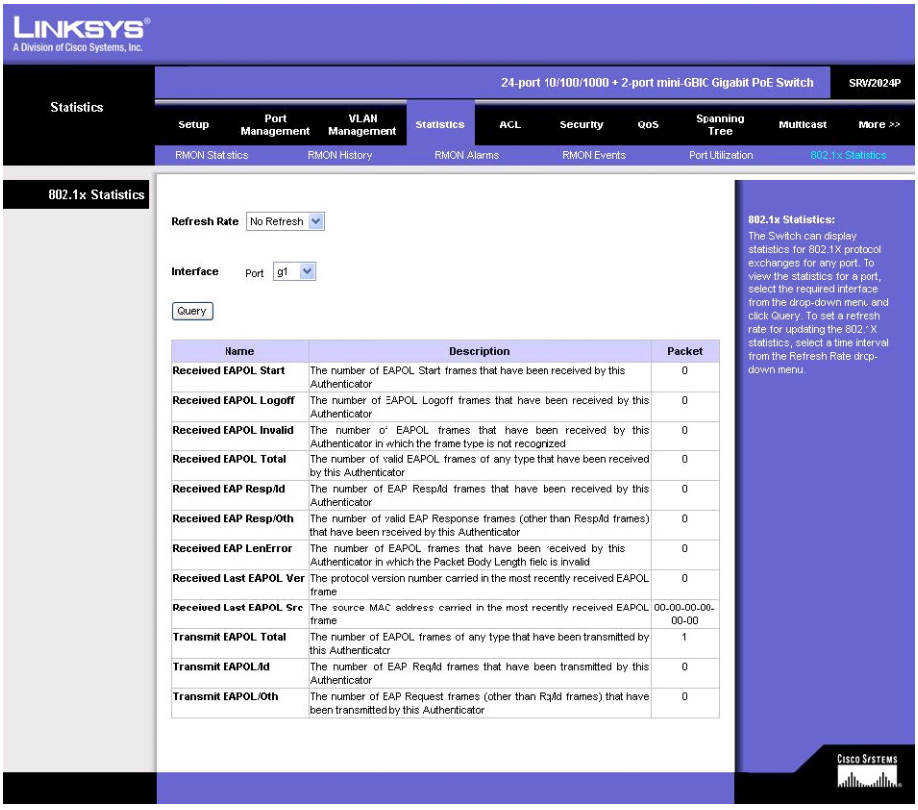
Global Overloaded Setting

Refresh Rate—Indicates the amount of time that passes before the port utilization statistics are refreshed. The possible field values are:

- **No Refresh**—Indicates that the statistics are not refreshed.
- **15 Sec**—Indicates that the statistics are refreshed every 15 seconds.
- **30 Sec**—Indicates that the statistics are refreshed every 30 seconds.
- **60 Sec**—Indicates that the statistics are refreshed every 60 seconds.

Statistics Tab - 802.1x Statistics

The *802.1X Statistics* screen contains information about EAP packets received on a specific port. To view the statistics for a port, select the required interface from the drop-down list and click **Query**.



Refresh Rate—Indicates the amount of time that passes before the EAP statistics are refreshed. The possible field values are:

- **No Refresh**—Indicates that the EAP statistics are not refreshed.
- **15 Sec**—Indicates that the EAP statistics are refreshed every 15 seconds.
- **30 Sec**—Indicates that the EAP statistics are refreshed every 30 seconds.
- **60 Sec**—Indicates that the EAP statistics are refreshed every 60 seconds.

Interface—Indicates the port, which is polled for statistics.

Name—Displays the measured 802.1x statistic.

Description—Describes the measured 802.1x statistic.

Packet—Displays the amount of packets measured for the particular 802.1x statistic.

ACL Tab - IP Based ACL

The *IP Based ACL* (Access Control List) screen contains information for defining IP Based ACLs. Access Control Lists (ACL) provide packet filtering for IP frames (based on address, protocol, Layer 4 protocol port number or TCP control code) or any frames (based on MAC address or Ethernet type). To filter incoming packets, first create an access list, add the required rules, specify a mask to modify the precedence in which the rules are checked, and then bind the list to a specific port.

Target—Select the New ACL Name radio button and enter an ACL name in the text field provided (with up to 16 characters). Or to add rules to an existing ACL, select ACL Name and select an ACL from the drop down list.

ACL Name—Displays the user-defined IP based ACLs.

New ACL Name—Define a new user-defined IP based ACL, the name cannot include spaces.

Action—Indicates the action assigned to the packet matching the ACL. Packets are forwarded or dropped. In addition, the port can be shut down, a trap can be sent to the network

administrator, or a packet assigned rate limiting restrictions for forwarding. The options are as follows:

- **Permit—**Forwards packets which meet the ACL criteria.
- **Deny—**Drops packets which meet the ACL criteria.
- **Shutdown—**Drops packet that meets the ACL criteria, and disables the port to which the packet was addressed. Ports are reactivated from the Port Management screen.

Protocol—Creates an ACE (Access Control Event) based on a specific protocol.

- **Select from List—**Selects from a protocols list on which ACE can be based. The possible field values are:
  - **Any—**Matches the protocol to any protocol.
  - **EIGRP—**Indicates that the Enhanced Interior Gateway Routing Protocol (EIGRP) is used to classify network flows.
  - **ICMP—**Indicates that the Internet Control Message Protocol (ICMP) is used to classify network flows.
  - **IGMP—**Indicates that the Internet Group Management Protocol (IGMP) is used to classify network flows.
  - **TCP—**Indicates that the Transmission Control Protocol is used to classify network flows.
  - **OSPF—**Matches the packet to the Open Shortest Path First (OSPF) protocol.
  - **UDP—**Indicates that the User Datagram Protocol is used to classify network flows.
- **Protocol ID To Match—**Adds user-defined protocols to which packets are matched to the ACE. Each protocol has a specific protocol number which is unique. The possible field range is 0-255.

TCP Flags—Filters packets by TCP flag. Filtered packets are either forwarded or dropped. Filtering packets by TCP flags increases packet control, which increases network security. The values that can be assigned are:

- **Set—**Enables filtering packets by selected flags.
- **Unset—**Disables filtering packets by selected flags.
- **Don't care—**Indicates that selected packets do not influence the packet filtering process.

The TCP Flags that can be selected are:

Urg—Indicates the packet is urgent.

Ack—Indicates the packet is acknowledged.

Psh—Indicates the packet is pushed.

Rst—Indicates the connection is dropped.

Syn—Indicates request to start a session.

Fin—Indicates request to close a session.

Source Port—Defines the TCP/UDP source port to which the ACE is matched. This field is active only if 800/6-TCP or 800/17-UDP are selected in the Select from List drop-down list. The possible field range is 0 - 65535.

Destination Port—Defines the TCP/UDP destination port. This field is active only if 800/6-TCP or 800/17-UDP are selected in the Select from List drop-down list. The possible field range is 0 - 65535.

Source IP Address—Matches the source port IP address to which packets are addressed to the ACE.

Wildcard Mask—Defines the source IP address wildcard mask. Wildcard masks specify which bits are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all the bits are important. For example, if the source IP address 149.36.184.198 and the wildcard mask is 255.36.184.00, the first eight bits of the IP address are ignored, while the last eight bits are used.

Destination IP Address—Matches the destination port IP address to which packets are addressed to the ACE.

Wildcard Mask—Defines the destination IP address wildcard mask.

Match DSCP—Matches the packet DSCP value to the ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is 0-63.

Match IP Precedence—Matches the packet IP Precedence value to the ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is 0-7.

The **Add to List** button adds the configured IP Based ACLs to the IP Based ACL Table at the bottom of the screen.

ACL Tab—IPv6 Based ACL

The IPv6 Based ACL screen allows an IPv6 based ACL to be defined. ACEs can be added only if the ACL is not bound to an interface.

Target—Select the New ACL Name radio button and enter an ACL name in the text field provided (with up to 16 characters). Or to add rules to an existing ACL select the ACL Name radio button and select an ACL from the drop-down menu.

ACL Name—Displays the user-defined IPv6 based ACLs.

New ACL Name—Specifies a new user-defined IPv6 based ACL name, the name cannot include spaces.

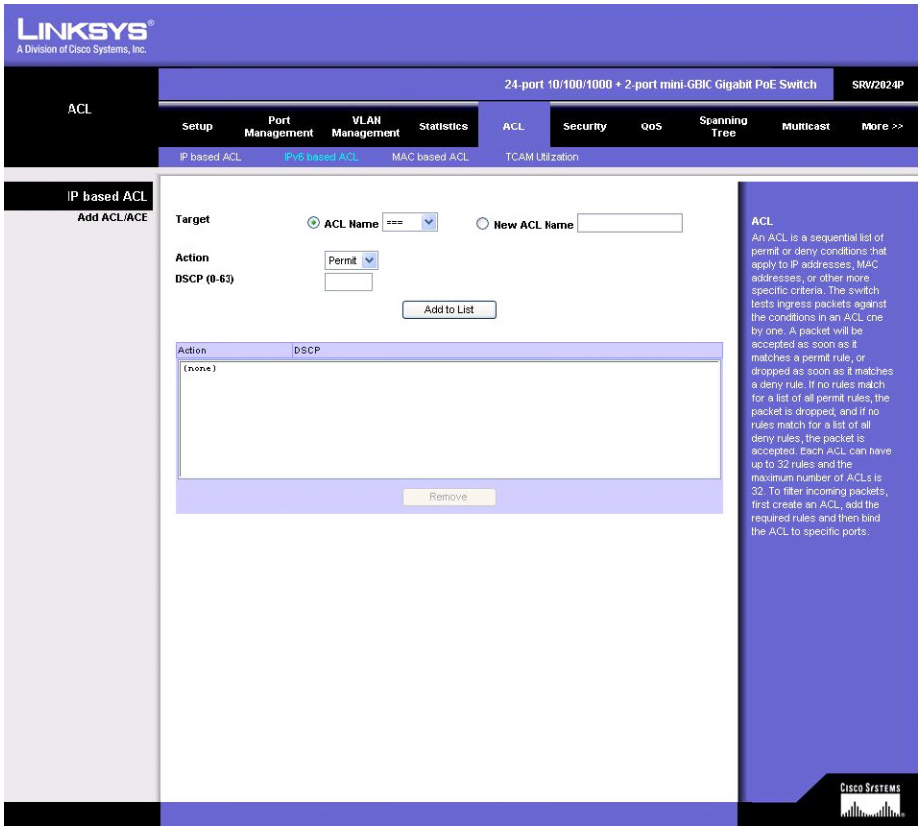
Action—Indicates the ACL forwarding action. Possible field values are:

Permit—Forwards packets which meet the ACL criteria.

Deny—Drops packets which meet the ACL criteria.

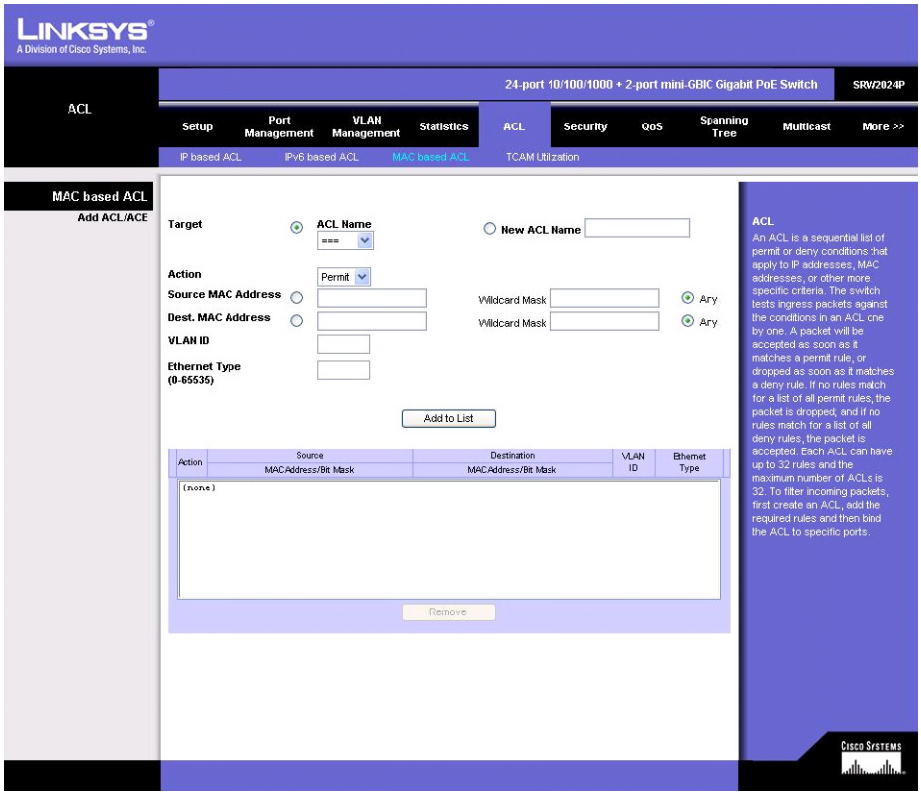
DSCP—Matches the packet DSCP value to the ACE. The possible field range is 0-63.

The **Add to List** button adds the configured IP Based ACLs to the IP Based ACL Table at the bottom of the screen.



ACL Tab - MAC Based ACL

The *MAC Based ACL* screen allows a MAC based ACL to be defined. ACEs can be added only if the ACL is not bound to an interface.



Target—Select the New ACL Name radio button and enter an ACL name in the text field provided (with up to 16 characters). Or to add rules to an existing ACL select the ACL Name radio button and select an ACL from the drop-down list.

ACL Name—Displays the user-defined MAC based ACLs.

New ACL Name—Specifies a new user-defined MAC based ACL name, the name cannot include spaces.

Action—Indicates the ACL forwarding action. Possible field values are:

- **Permit—**Forwards packets that meet the ACL criteria.
- **Deny—**Drops packets that meet the ACL criteria.
- **Shutdown—**Drops packet that meet the ACL criteria, and disables the port to which the packet was addressed.

Source MAC Address—Matches the source MAC address to which packets are addressed to the ACE.

Wildcard Mask—Defines the source IP address wildcard mask. Wildcard masks specify which bits are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all the bits are important. For example, if the

source IP address 149.36.184.198 and the wildcard mask is 255.36.184.00, the first eight bits of the IP address are ignored, while the last eight bits are used.

Destination MAC Address—Matches the destination MAC address to which packets are addressed to the ACE.

Wildcard Mask—Defines the destination IP address wildcard mask.

VLAN ID—Matches the packet's VLAN ID to the ACE. The possible field values are 2 to 4094.

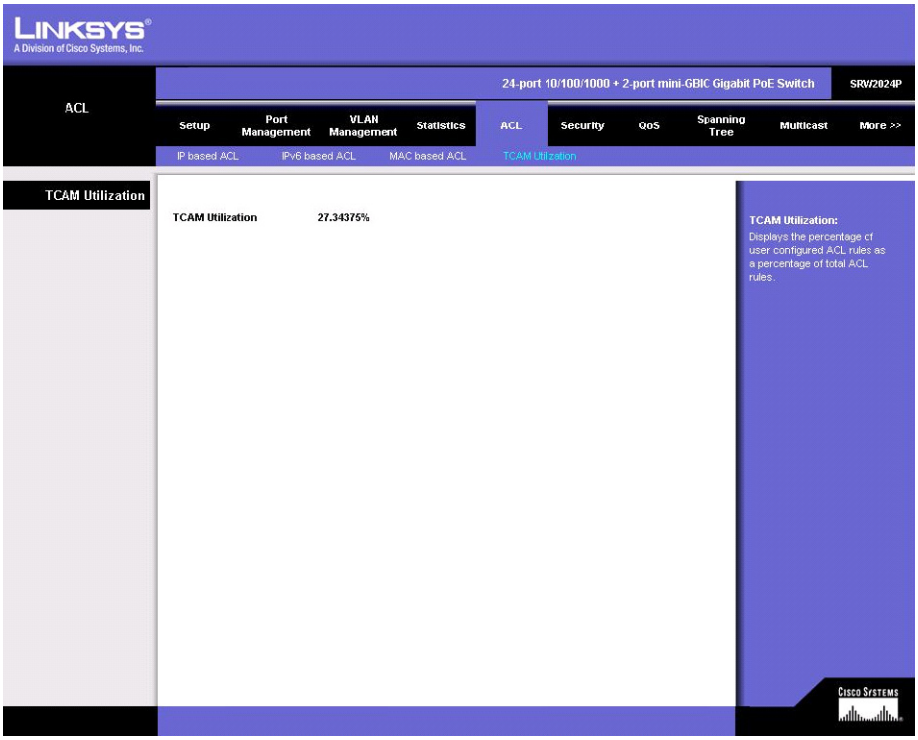
Ethernet Type—Specifies the packet's Ethernet type. This option can be used only to filter Ethernet II formatted packets. (Range: 0-65535) A detailed listing of Ethernet protocol types can be found in RFC 1060. Examples include 0800 (IP), 0806 (ARP), 8137 (IPX).

The **Add to List** button adds the configured MAC Based ACLs to the MAC Based ACL Table at the bottom of the screen.

To remove an ACL rule, select an ACL rule from the table and click **Remove**. When all rules are removed from the ACL, the ACL is also removed.

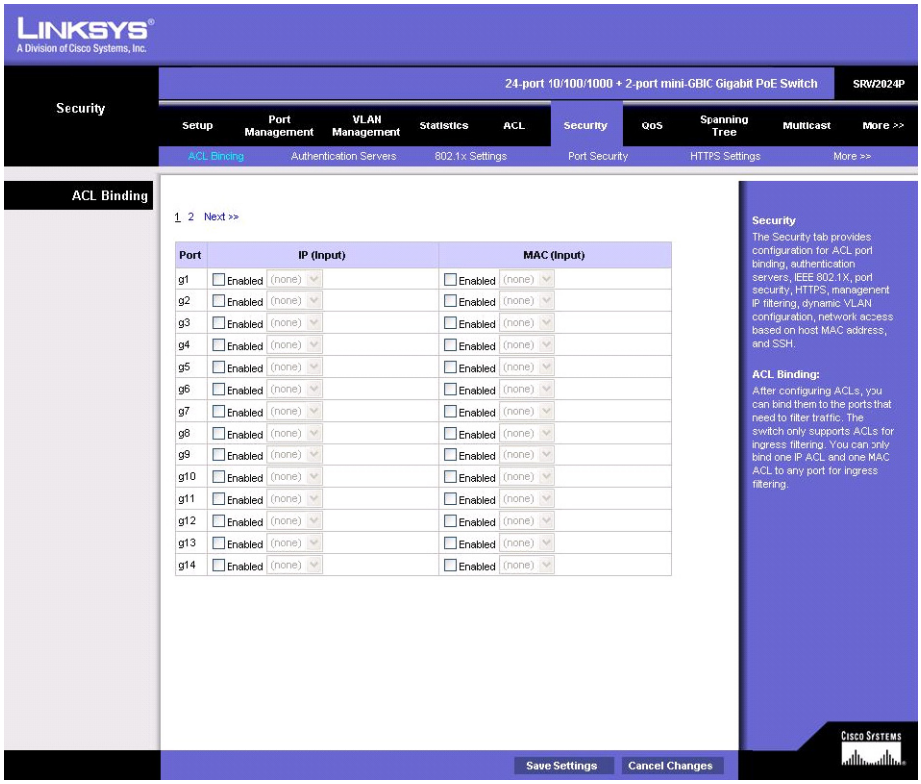
ACL Tab—TCAM Utilization

This switch supports ACL filtering with Ternary Content Addressable Memory (TCAM). This menu tab displays the percentage of user configured ACL rules as a percentage of total ACL rules.



Security Tab - ACL Binding

After configuring Access Control Lists (ACL), you should bind them to the ports that need to filter traffic. You can assign one IP or MAC access list to any port.



You must configure a mask for an ACL rule before you can bind it to a port.

This switch supports ACLs only for ingress filtering. You can only bind one IP or one MAC ACL to any port, for ingress filtering.

Check the Enable box for the port you want to bind to an ACL. Select the required ACL from the drop-down list.

Port—Fixed port or SFP module. (Range: 1-24).

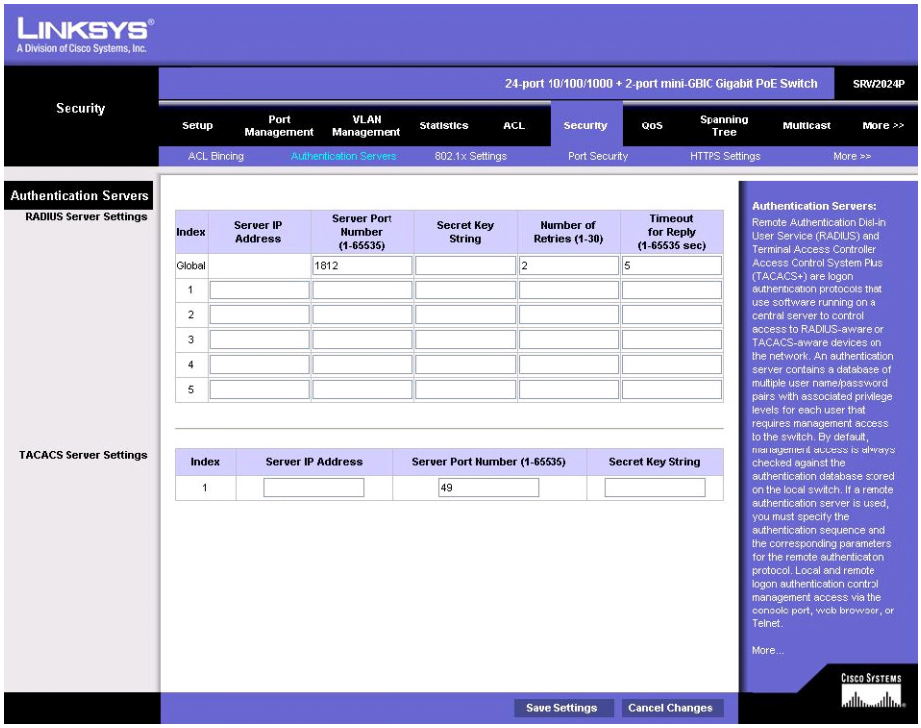
IP (Input)—Specifies the IP Access List to enable for a port.

MAC (Input)—Specifies the MAC Access List to enable globally.

Click **Save Settings** to save the changes.

Security Tab - Authentication Servers

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



This switch uses the Extensible Authentication Protocol over LANs (EAPOL) to exchange authentication protocol messages with the client, and a remote RADIUS authentication server to verify user identity and access rights. When a client (i.e., Supplicant) connects to a switch port, the switch (i.e., Authenticator) responds with an EAPOL identity request. The client provides its identity (such as a user name) in an EAPOL response to the switch, which it forwards to the RADIUS server. The RADIUS server verifies the client identity and sends an access challenge back to the client. The EAP packet from the RADIUS server contains not only the challenge, but also the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server. The authentication method must be MD5. The client responds to the appropriate method with its credentials, such as a password or certificate. The RADIUS server verifies the client credentials and responds with an accept or reject packet. If authentication is successful, the switch allows the client to access the network. Otherwise, network access is denied and the port remains blocked.

RADIUS Server Setting

Index—Indicates the server number or global setting.

Server IP Address—Enter the IP address of the server.

Server Port Number (1-6535)—Enter the authentication port. The authentication port is used during RADIUS server authentication. The authentication port default is 1812.

Secret Key String—Enter the secret key string as defined on the RADIUS server. The secret key string is used for authenticating and encrypting communications between the device and the RADIUS server.

Number of Retries (1-30)—Defines the number of transmitted requests sent to the RADIUS server before a failure occurs. The possible field values are 1 - 30. 2 is the default value.

Timeout for Reply (1-6535 sec)—Defines the amount of the time in seconds the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server. The possible field values are 1 - 65535. 5 is the default value.

TACACS Server Setting

The Switch provides Terminal Access Controller Access Control System (TACACS+) client support. TACACS+ provides centralized security for validation of users accessing the device. TACACS+ provides a centralized user management system, while still retaining consistency with RADIUS and other authentication processes. The TACACS+ protocol ensures network integrity through encrypted protocol exchanges between the device and TACACS+ server.

Server IP Address—Enter the TACACS+ Server IP address.

Server Port Number (1-6535)**—**Defines the port number through which the TACACS+ session occurs. The default port is 49.

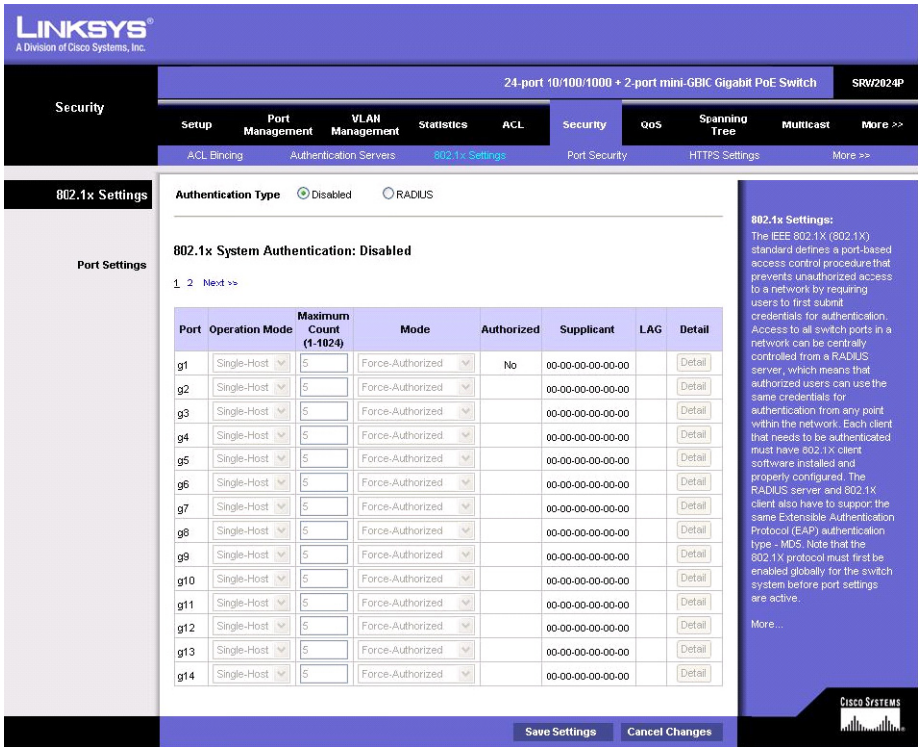
Secret Key String—Defines the authentication and encryption key for TACACS+ server. The key must match the encryption key used on the TACACS+ server.

Click **Save Settings** to save the changes.

Security Tab - 802.1x Settings

Port-based authentication enables authenticating system users on a per-port basis via an external server. Only authenticated and approved system users can transmit and receive data.

Ports are authenticated via the RADIUS server using the Extensible Authentication Protocol (EAP).



The IEEE 802.1X (dot1X) standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. Access to all switch ports in a network can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

The operation of 802.1X on the switch requires the following:

- The switch must have an IP address assigned.
- RADIUS authentication must be enabled on the switch and the IP address of the RADIUS server specified.
- 802.1X must be enabled globally for the switch.
- Each switch port that will be used must be set to dot1X “Auto” mode.
- Each client that needs to be authenticated must have dot1X client software installed and properly configured.
- The RADIUS server and 802.1X client support EAP. (The switch only supports EAPOL in order to pass the EAP packets from the server to the client.)
- The RADIUS server and client also have to support the same EAP authentication type – MD5. (Some clients have native support in Windows, otherwise the dot1x client must support it.)

To enable 802.1X System Authentication Control, select **Radius**.

When 802.1X is enabled, you need to configure the parameters for the authentication process that runs between the client and the switch (that is, authenticator), as well as the client identity lookup process that runs between the switch and authentication server. These parameters are described in this section.

Operation Mode—Allows single or multiple hosts (clients) to connect to an 802.1X-authorized port. (Options: Single-Host, Multi-Host; Default: Single-Host)

Maximum Count—The maximum number of hosts that can connect to a port when the Multi-Host operation mode is selected. (Range: 1-1024; Default: 5)

Mode—Sets the authentication mode to one of the following options:

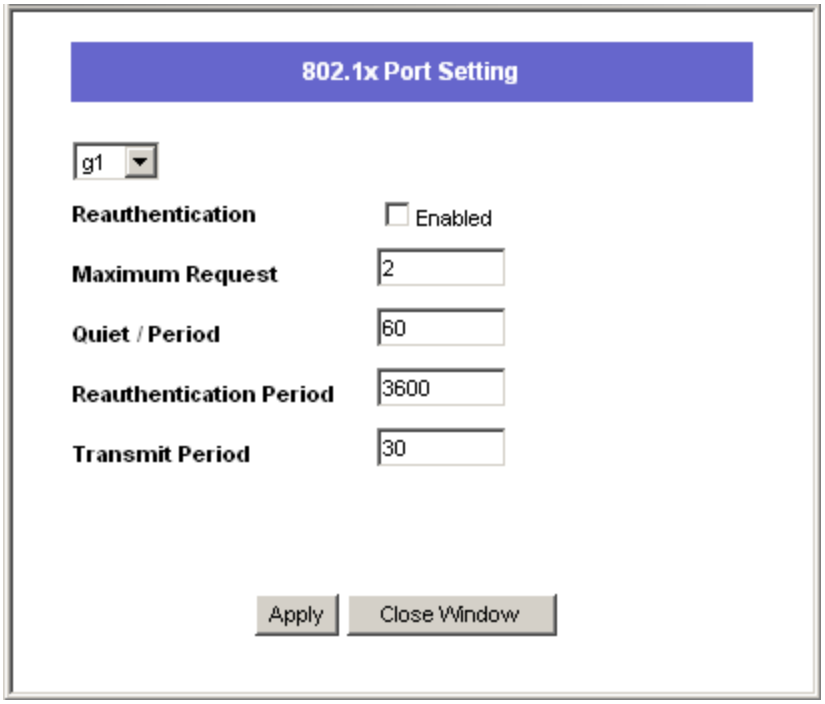
- **Auto**—Requires a dot1x-aware client to be authorized by the authentication server. Clients that are not dot1x-aware will be denied access.
- **Force-Authorized**—Forces the port to grant access to all clients, either dot1x-aware or otherwise. (This is the default setting.)
- **Force-Unauthorized**—Forces the port to deny access to all clients, either dot1x-aware or otherwise.

Authorized—Indicates the current status of the port:

- **Yes**—A connected client is authorized.
- **No**—No connected clients are authorized.
- **Blank**—Displays nothing when there is no connection on a port.

Supplicant—Indicates the MAC address of a connected client.

Modify the parameters required using the drop-down lists and fields provided for each port, then click **Detail** to configure the 802.1X settings for that port.



The *802.1x Port Settings* screen allows configuration of the following parameters:

Reauthentication—To reauthenticate a client, select Enabled.

Maximum Request—Sets the maximum number of times the switch port will retransmit an EAP request packet to the client before it times out the authentication session. (Range: 1-10; Default 2)

Quiet Period—Sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client. (Range: 1-65535 seconds; Default: 60 seconds)

Reauthentication Period—Sets the time period after which a connected client must be re-authenticated. (Range: 1-65535 seconds; Default: 3600 seconds)

Transmit Period—Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet. (Range: 1-65535; Default: 30 seconds)

Click **Save Settings** to apply the changes.

Enable 802.1x—Select this to enable 802.1x authentication.

Port—Indicates the port name.

Status Port Control—Specifies the port authorization state. The possible field values are as follows:

- **Force-Authorized—**The controlled port state is set to Force-Authorized (forward traffic).

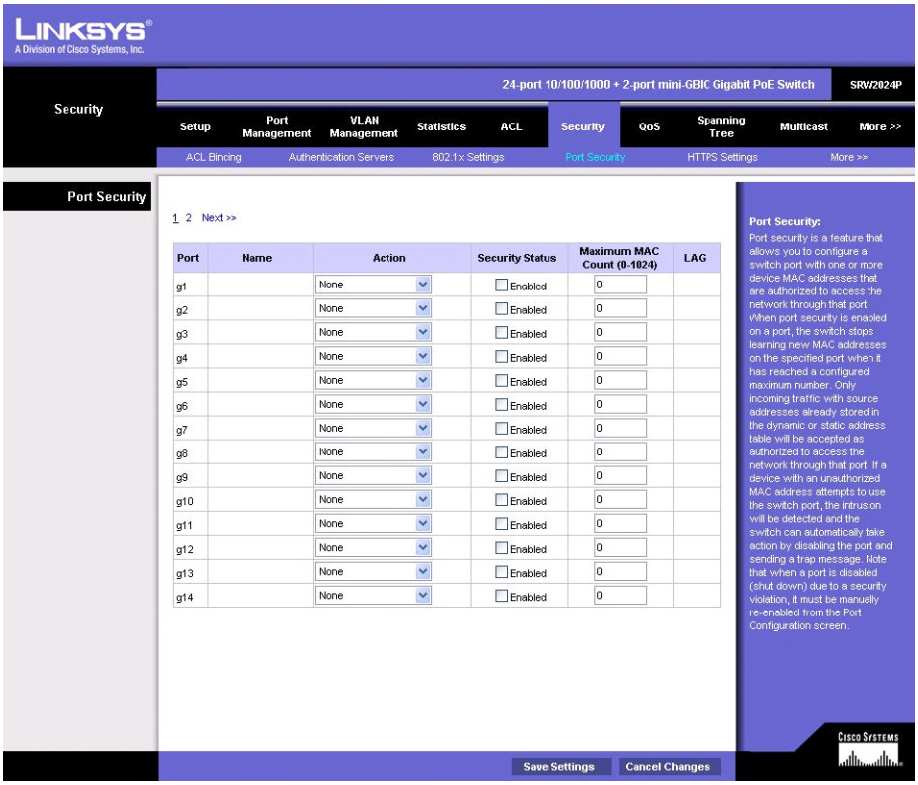
- **Force-Unauthorized—**The controlled port state is set to Force-Unauthorized (discard traffic).

Enable Periodic Reauthentication—Permits immediate port reauthentication.

The **Setting Timer** button opens the *Setting Timer* screen to configure ports for 802.1x functionality.

Security Tab - Port Security

Port security is a feature that allows you to configure a switch port with one or more device MAC addresses that are authorized to access the network through that port. When port security is enabled on a port, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted as authorized to access the network through that port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.



To use port security, specify a maximum number of addresses to allow on the port and then let the switch dynamically learn the <source MAC address, VLAN> pair for frames received on the port. When the port has reached the maximum number of MAC addresses, the selected port will stop learning. The MAC addresses already in the address table will be retained and will not expire. Any other device that attempts to use the port will be prevented from accessing the switch.

Set the action to take when an invalid address is detected on a port, select **Security Status** to enable security for a port, set the maximum number of MAC addresses allowed on a port.

Interface—Displays the port or LAG name.

Lock Interface—Selecting this option locks the specified interface.

Learning Mode—Defines the locked port type. The Learning Mode field is enabled only if Locked is selected in the Interface Status field. The possible field values are:

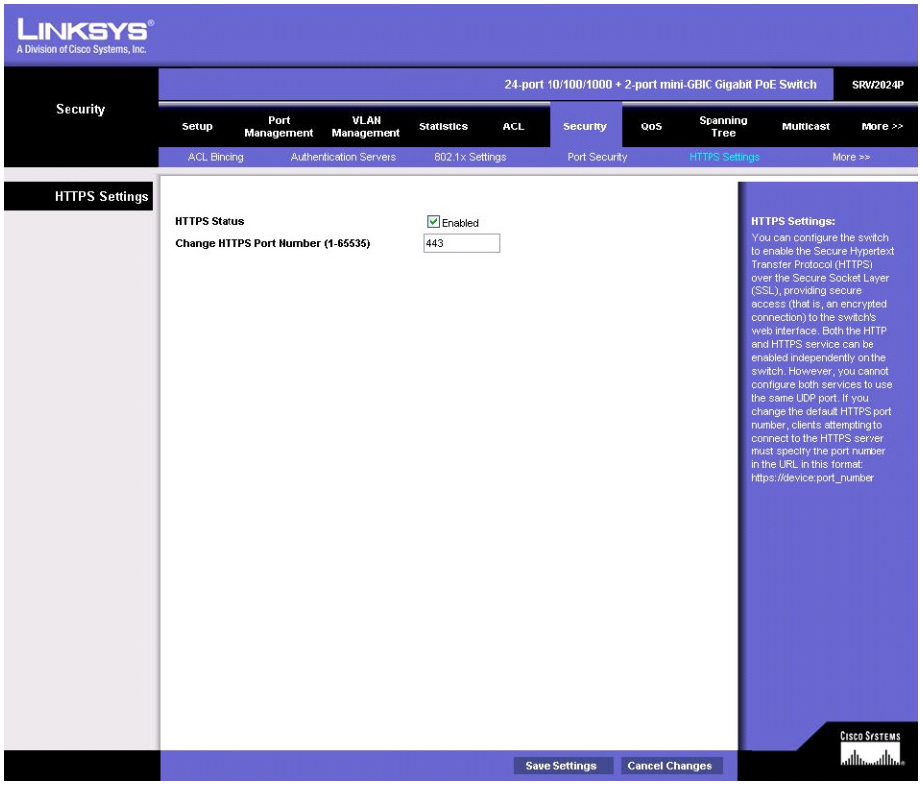
- **Classic Lock**— Locks the port using the classic lock mechanism. The port is immediately locked, regardless of the number of addresses that have already been learned.
- **Limited Dynamic Lock**—Locks the port by deleting the current dynamic MAC addresses associated with the port. The port learns up to the maximum addresses allowed on the port. Both relearning and aging MAC addresses are enabled.

In order to change the Learning Mode, the Lock Interface must be set to Unlocked. Once the mode is changed, the Lock Interface can be reinstated.

Click **Save Changes** to save the changes.

Security Tab - HTTPS Settings

You can configure the switch to enable the Secure Hypertext Transfer Protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (that is, an encrypted connection) to the switch's web interface.

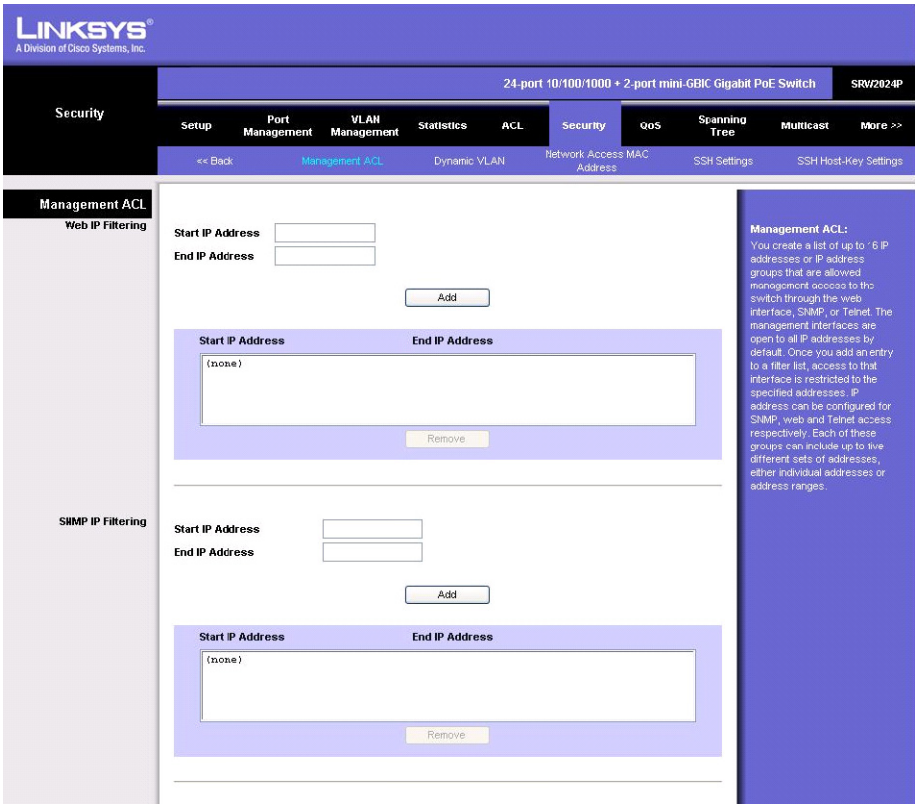


To enable HTTPS, select **HTTPS Status** and specify the port number.

Click **Save Settings** to save the changes.

Security Tab - Management ACL

Management ACL You can create a list of up to 16 IP addresses or IP address groups that are allowed access to the switch through the web interface, SNMP, or Telnet.



The management interfaces are open to all IP addresses by default. When you add an entry to a filter list, access to that interface is restricted to the specified addresses. If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.

IP addresses can be configured for web, SNMP, and Telnet access. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges. When entering addresses for the same group (i.e., SNMP, web or Telnet), the switch will not accept overlapping address ranges. When entering addresses for different groups, the switch will accept overlapping address ranges.

You cannot delete an individual address from a specified range. You must delete the entire range, and reenter the addresses. You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

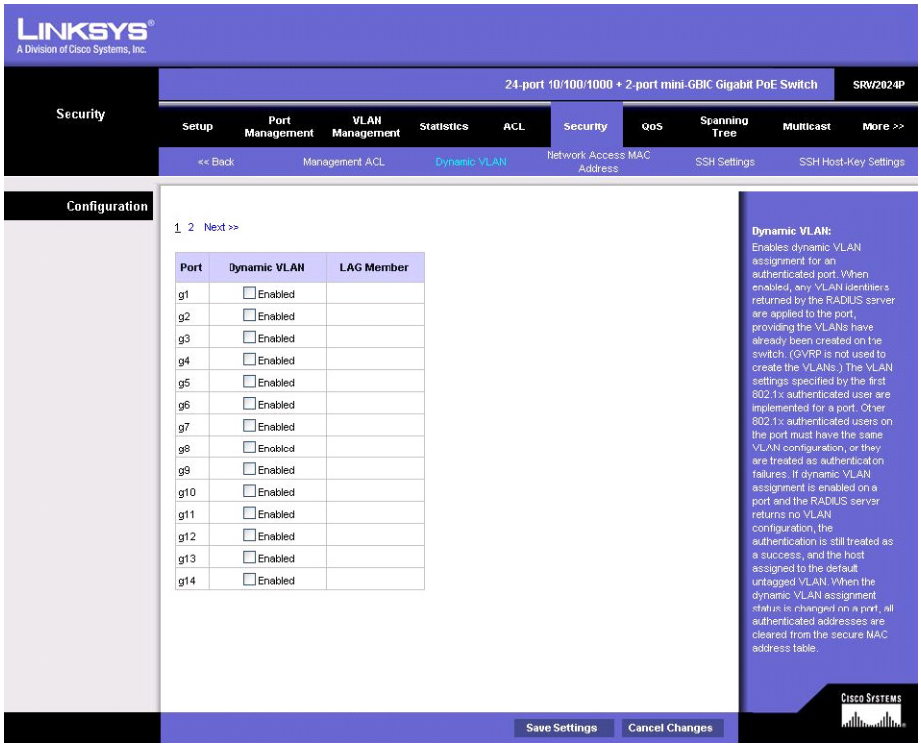
Security Tab—Dynamic VLAN

Dynamic VLAN—Enables or disables dynamic VLAN assignment for an authenticated port. When enabled, any VLAN identifiers returned by the RADIUS server are applied to the port, providing the VLANs have already been created on the switch. (GVRP is not used to create the VLANs.)

The VLAN settings specified by the first 802.1x authenticated user are implemented for a port. Other 802.1X authenticated users on the port must have the same VLAN configuration, or they are treated as authentication failures.

If dynamic VLAN assignment is enabled on a port and the RADIUS server returns no VLAN configuration, the authentication is still treated as a success, and the host assigned to the default untagged VLAN.

When the dynamic VLAN assignment status is changed on a port, all authenticated addresses are cleared from the secure MAC address table.



Security Tab—Network Access MAC Address

Authenticated MAC addresses are stored in the secure MAC address table. Information on the secure MAC entries can be displayed and selected entries can be removed from the table.

Query By—Specifies parameters to use in the MAC address query.

Port – Specifies a port interface.

MAC Address – Specifies a single MAC address information.

Attribute – Displays static or dynamic addresses.

Address Table Sort Key – Sorts the information displayed based on MAC address or port interface.

The Authentication Table displays the following information.

Unit/Port – The port interface associated with a secure MAC address.

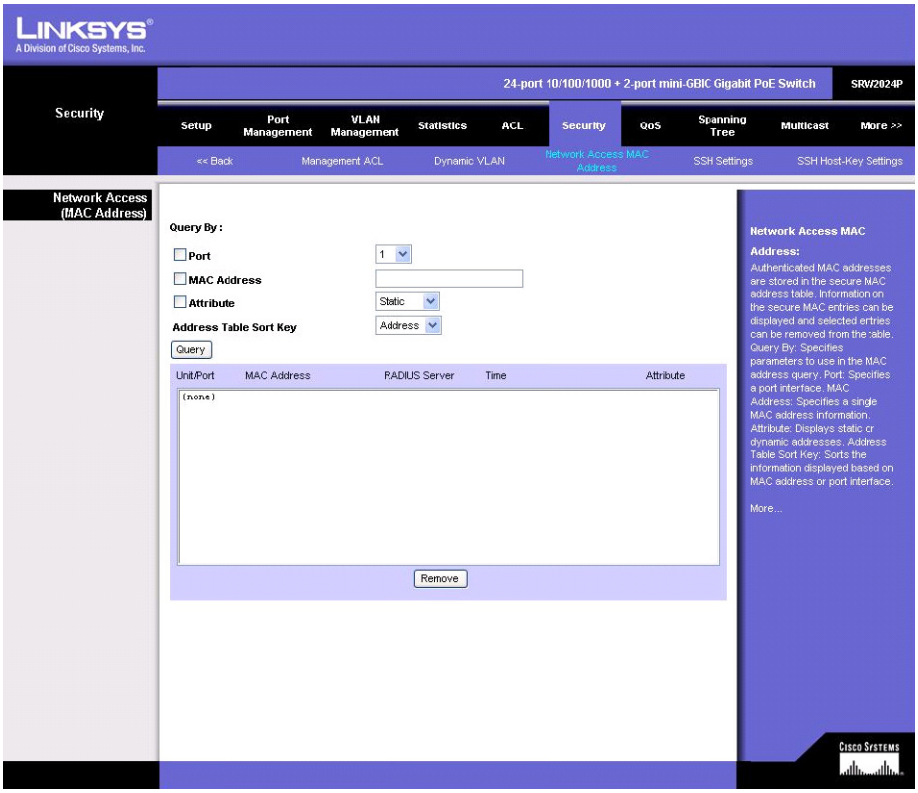
MAC Address – The authenticated MAC address.

RADIUS Server – The IP address of the RADIUS server that authenticated the MAC address.

Time – The time when the MAC address was last authenticated.

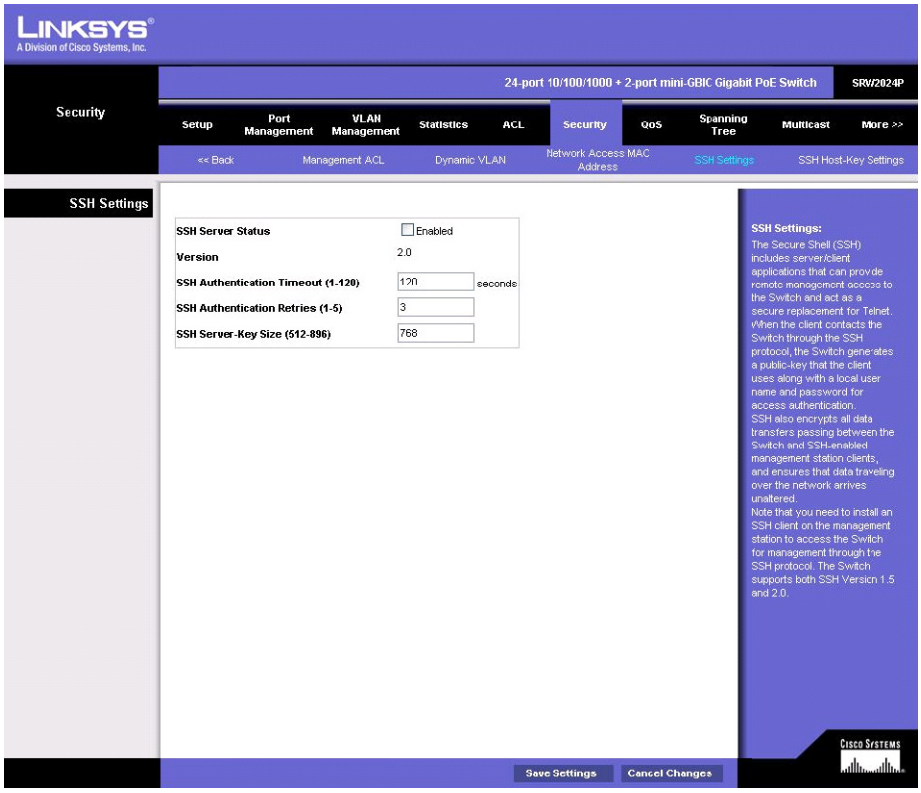
Attribute – Indicates a static or dynamic address.

Remove—Click the **Remove** button to remove selected MAC addresses from the secure MAC address table.



Security Tab - SSH Settings

The Secure Shell (SSH) includes server/client applications that can provide remote management access to the switch and act as a secure replacement for Telnet.



When the client contacts the switch through the SSH protocol, the switch generates a public-key that the client uses along with a local user name and password for access authentication. SSH also encrypts all data transfers passing between the switch and SSH-enabled management station clients, and ensures that data traveling over the network arrives unaltered.

Note that you need to install an SSH client on the management station to access the switch for management through the SSH protocol. The switch supports both SSH Version 1.5 and 2.0.

SSH Server Status—Allows you to enable/disable the SSH server on the switch. (Default: Disabled)

Version—The Secure Shell version number. Version 2.0 is displayed, but the switch supports management access via either SSH Version 1.5 or 2.0 clients.

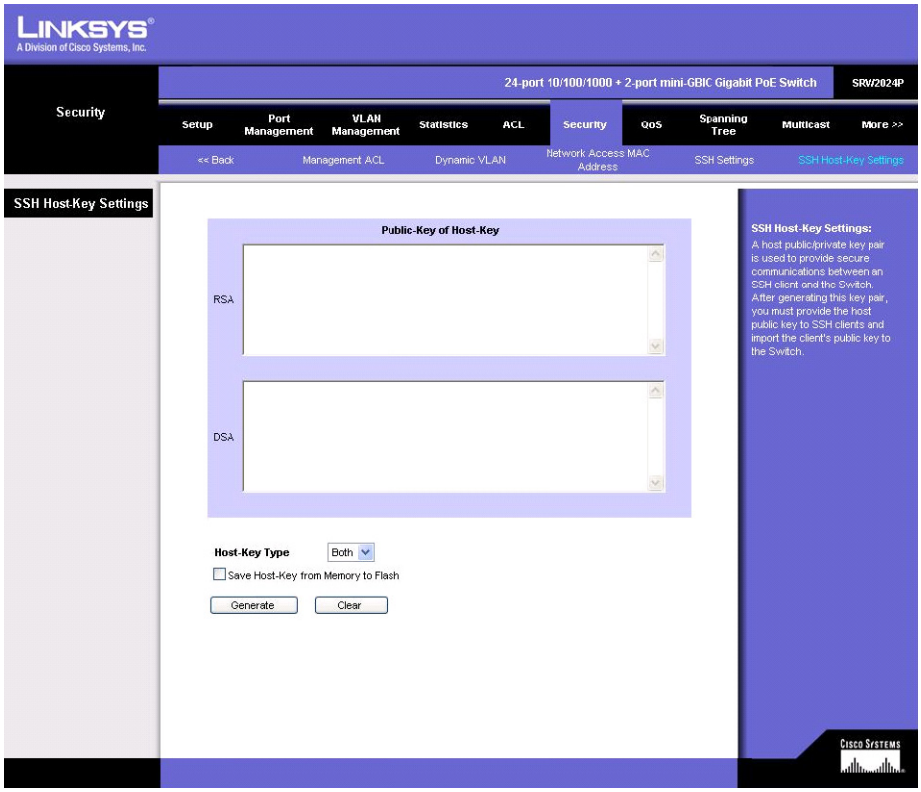
SSH Authentication Timeout—Specifies the time interval in seconds that the SSH server waits for a response from a client during an authentication attempt. (Range: 1-120 seconds; Default: 120 seconds)

SSH Authentication Retries—Specifies the number of authentication attempts that a client is allowed before authentication fails and the client has to restart the authentication process. (Range: 1-5 times; Default: 3)

SSH Server-Key Size—Specifies the SSH server key size. The server key is a private key that is never shared outside the switch.The host key is shared with the SSH client, and is fixed at 1024 bits. (Range: 512-896 bits; Default:768)

SSH Host-Key Settings

A host public/private key pair is used to provide secure communications between an SSH client and the switch. After generating this key pair, you must provide the host public key to SSH clients and import the client's public key to the switch.



Public-Key of Host-Key—The public key for the host.

- **RSA (Version 1)**—The first field indicates the size of the host key (e.g., 1024), the second field is the encoded public exponent (e.g., 65537), and the last string is the encoded modulus.
- **DSA (Version 2)**—The first field indicates that the encryption method used by SSH is based on the Digital Signature Standard (DSS). The last string is the encoded modulus.

Host-Key Type—The key type used to generate the host key pair (i.e., public and private keys). (Range: RSA (Version 1), DSA (Version 2), Both: Default: RSA) The SSH server uses RSA or DSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.

Save Host-Key from Memory to Flash—Saves the host key from RAM (volatile memory) to flash memory. Otherwise, the host key pair is stored to RAM by default. Note that you must select this item prior to generating the host-key pair.

Generate—This button is used to generate the host key pair. Note that you must first generate the host key pair before you can enable the SSH server.

Clear—This button clears the host key from both volatile memory (RAM) and non-volatile memory (Flash).

QoS Tab

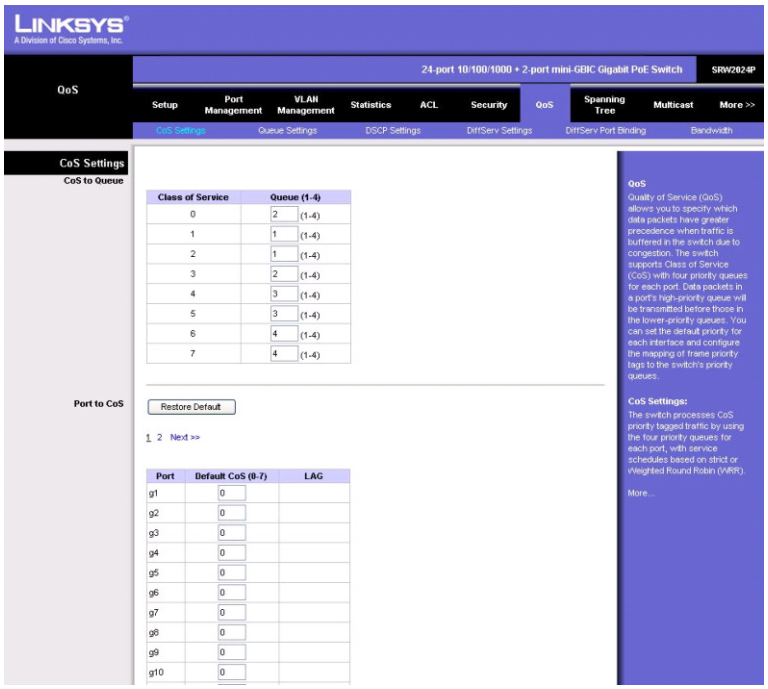
Network traffic is usually unpredictable, and the only basic assurance that can be offered is best effort traffic delivery. To overcome this challenge, Quality of Service (QoS) is applied throughout the network. This ensures that network traffic is prioritized according to specified criteria, and that specific traffic receives preferential treatment.

CoS provides varying Layer 2 traffic services—Class of Service (CoS) refers to classification of traffic to traffic-classes, which are handled as an aggregate whole, with no per-flow settings. CoS is usually related to the 802.1p service that classifies flows according to their Layer 2 priority, as set in the VLAN header.

QoS refers to Layer 2 traffic and above. QoS handles per-flow settings, even within a single traffic class.

QoS Tab - CoS Settings

Class of Service (CoS) allows you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. The switch supports CoS with four priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, and configure the mapping of frame priority tags to the switch's priority queues.The priority levels recommended in the IEEE 802.1p standard for various network applications are shown in the following table. However, you can map the priority levels to the switch's output queues in any way that benefits application traffic for your own network.



The *CoS Settings* screen contains fields for enabling or disabling CoS. In addition, the Trust mode can be selected. The Trust mode relies on predefined fields within the packet to determine the egress queue settings.

Priority Level	Traffic Type
1	Background
2	(Spare)0(default) Best Effort
3	Excellent Effort
4	Controlled Load
5	Video, less than 100 milliseconds latency and jitter
6	Voice, less than 10 milliseconds latency and jitter
7	Network Control

CoS to Queue

Assign priorities to the traffic classes (output queues) for the selected interface.

Class of Service—CoS value. (Range: 0-7, where 7 is the highest priority queue)

Queue (0-3)—The output priority queue. (Range: 0-3, where 3 is the highest CoS priority queue)

Port to CoS

Modify the default priority for any interface using the text field provided.

Default CoS (0-7)—The priority that is assigned to untagged frames received on the interface. (Range: 0-7, where 7 is the highest priority)

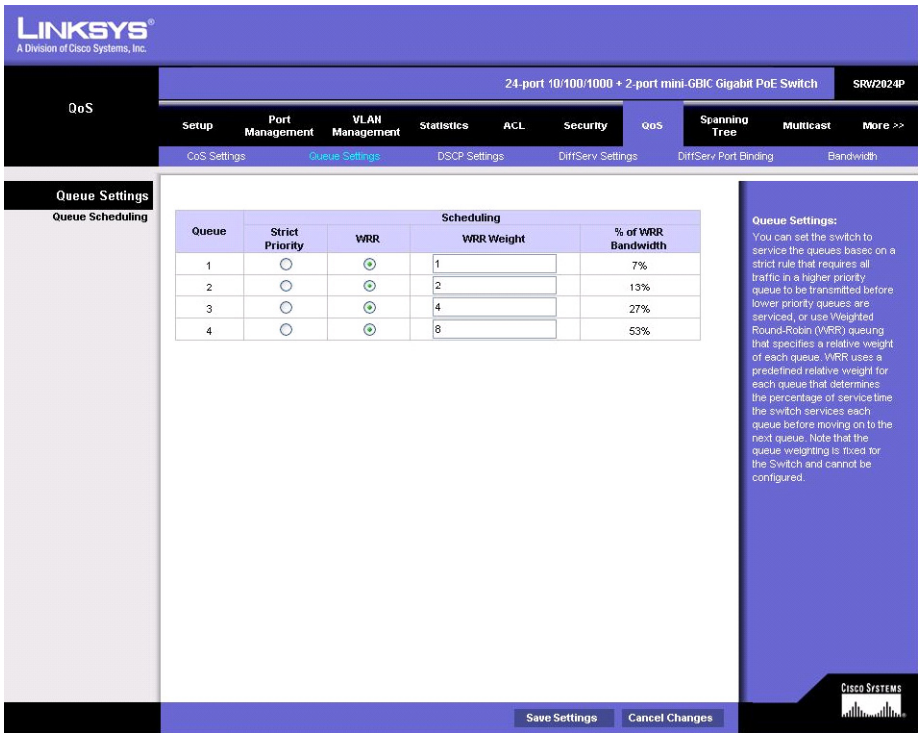
LAG—Indicates if ports are members of a LAG. To configure the default priority for LAGs, go to the table entry for the LAG number, which is listed after port g24 at the end of the table.

Default settings can be restored using the **Restore Defaults** button.

Click **Save Settings** to save the changes.

QoS Tab - Queue Settings

The *Queue Settings* screen contains fields for defining the QoS queue forwarding types.



Queue—Displays the queue for which the queue settings are displayed. The possible field range is 1 - 4.

Strict Priority—Indicates that traffic scheduling for the selected queue is based strictly on the queue priority.

WRR—Indicates that traffic scheduling for the selected queue is based strictly on the WRR.

WRR Weight—Displays the WRR weights to queues.

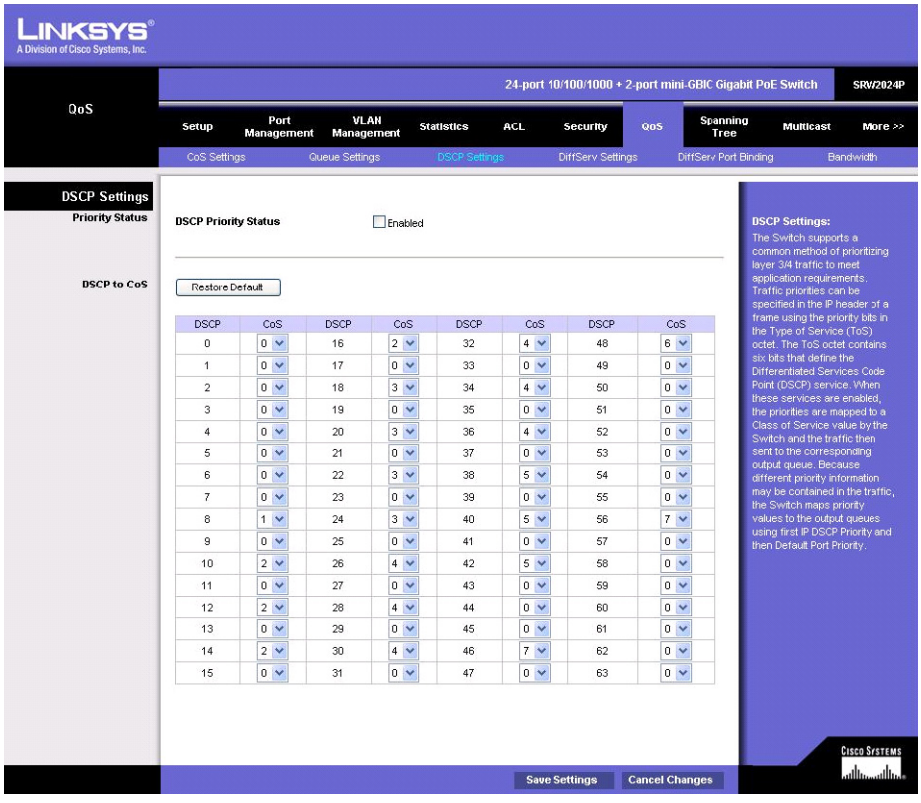
% of WRR Bandwidth—Displays the amount of bandwidth assigned to the queue. These values are fixed and are not user defined.

QoS Tab - DSCP Settings

The switch supports a common method of prioritizing layer 3/4 traffic to meet application requirements. Traffic priorities can be specified in the IP header of a frame using the priority bits in the Type of Service (ToS) octet. If priority bits are used, the ToS octet may contain six bits for Differentiated Services Code Point (DSCP) service. When these services are enabled, the priorities are mapped to a CoS value by the switch and the traffic is then sent to the corresponding output queue. Because different priority information may be contained in the traffic, the switch maps priority values to the output queues in the following manner:

The precedence for priority mapping is DSCP Priority and then Default Port Priority.

To enable DSCP priority mapping, select **DSCP Priority Status**.



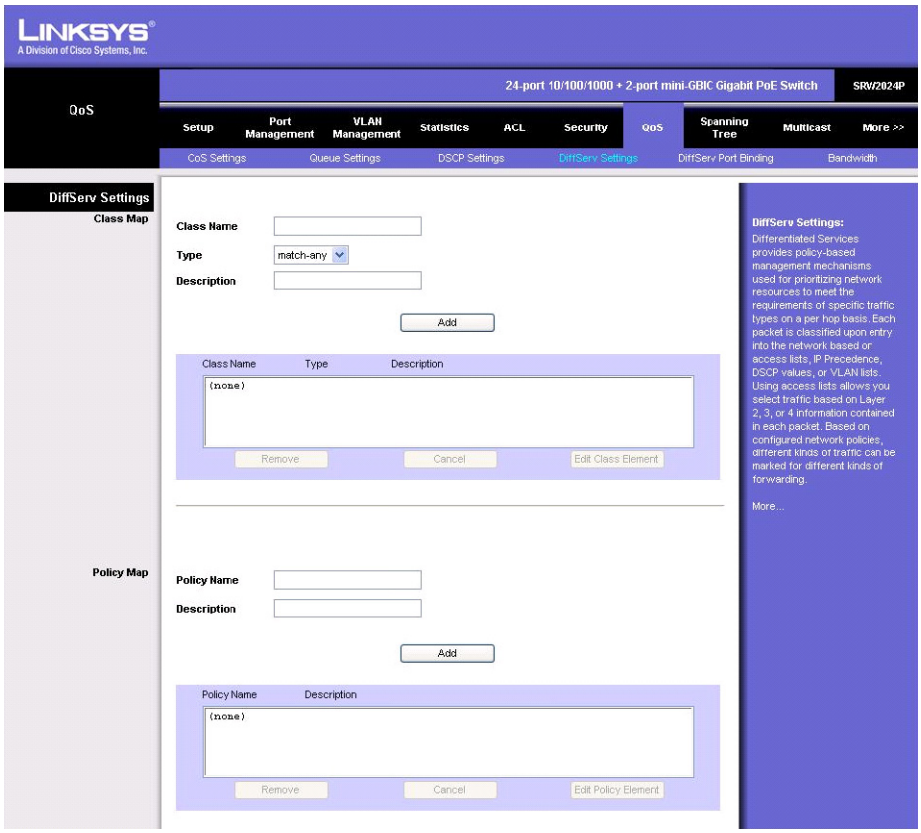
Priority Status—Enables the DSCP priority mapping. (Enabled is the default setting.)

DSCP to CoS—Maps Differentiated Services Code Point values to CoS values.

Click **Save Settings** to save the changes.

QoS Tab - Diffserv Settings

The commands described in this section are used to configure Quality of Service (QoS) classification criteria and service policies. Differentiated Services (DiffServ) provides policy-based management mechanisms used for prioritizing network resources to meet the requirements of specific traffic types on a per hop basis. Each packet is classified upon entry into the network based on access lists, IP Precedence, DSCP values, or VLAN lists. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet. Based on configured network policies, different kinds of traffic can be marked for different kinds of forwarding.

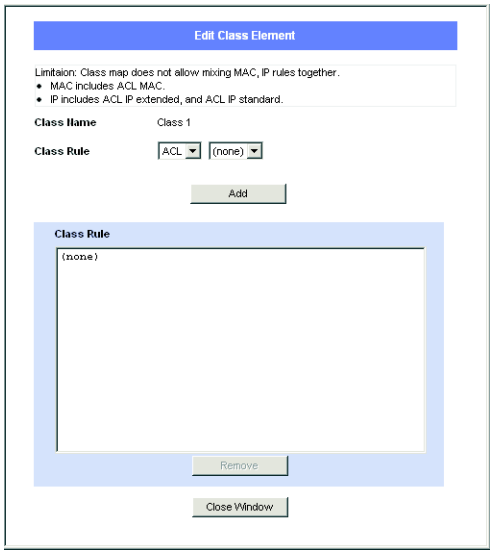


All switches or routers that access the Internet rely on class information to provide the same forwarding treatment to packets in the same class. Class information can be assigned by end hosts, or switches or routers along the path. Priority can then be assigned based on a general policy, or a detailed examination of the packet. However, note that detailed examination of packets should take place close to the network edge so that core switches and routers are not overloaded.switches and routers along the path can use class information to prioritize the resources allocated to different traffic classes. The manner in which an individual device handles traffic in the DiffServ architecture is called per-hop behavior. All devices along a path should be configured in a consistent manner to construct a consistent end-to-end QoS solution.

Class Map

A class map is used for matching packets to a specified class. The class map uses the Access Control List filtering engine, so you must also set an ACL to enable filtering for the criteria specified in the class map.

The class map is used with a policy map to create a service policy for a specific interface that defines packet classification, service tagging, and bandwidth policing. Note that one or more class maps can be assigned to a policy map.



Class Name—Name of the class map. (Range: 1-32 characters)

Description—A brief description of a class map. (Range: 1-256 characters)

Add—Creates a new class map using the entered class name and description.

Edit Class Element—Modifies the class map criteria used to classify ingress traffic.

Remove—Removes the selected class from the list.

Select the entry from the table that you wish to change, then click **Edit Class Element**. Add rules to a selected class using the ACL list drop-down list or the IP DSCP, IP Precedence and VLAN text fields provided, then click **Add**.

Class Rule—Edits the rules for the class by specifying the type of traffic based on an access list, a DSCP or IP Precedence value, or a VLAN.

- **ACL**—Name of an access control list. Any type of ACL can be specified, including standard or extended IP ACLs and MAC ACLs. (Range: 1-16 characters)
- **IP DSCP**—A DSCP value. (Range: 0-63)
- **IP Precedence**—An IP Precedence value. (Range: 0-7)
- **VLAN**—A VLAN value. (Range: 1-4094)

Add—Adds the specified criteria to the class. Only one entry is permitted per class.

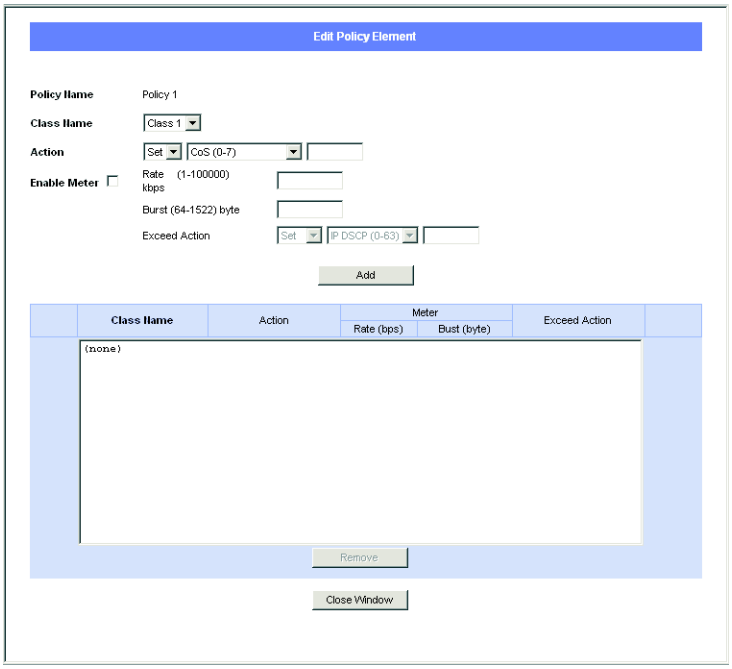
Remove—Deletes the selected criteria from the class.

Policy Map

A policy map can contain multiple class statements that can be applied to the same interface with the Service Policy Settings. You can configure up to 63 policers (that is, class maps) for Fast Ethernet and Gigabit Ethernet ingress ports.

Policing is based on a token bucket, where bucket depth (that is, the maximum burst before the bucket overflows) is by specified the "Burst" field, and the average rate tokens are removed from the bucket is by specified by the "Rate" option.

After using the policy map to define packet classification, service tagging, and bandwidth policing, it must be assigned to a specific interface by a service policy to take effect.



Policy name—The name of the policy map. (Range: 1-32 characters for the name)

Description—A brief description of the Policy. (Range 1-256 characters for the description)

Click **Add** to create a new policy, or select a policy and click **Edit Policy Element** to change the policy rules of the selected policy, or Remove Policy to delete the policy.

Class Name—Name of class map. Use the drop-down list to select a different policy.

Action—Configures the service provided to ingress traffic by setting a CoS, DSCP, or IP Precedence value in a matching packet. (Range - CoS: 0-7, DSCP: 0-63, IP Precedence: 0-7)

Enable Meter—Check this box to define the maximum throughput, burst rate, and the action that results from a policy violation.

- **Rate** (kbps)—Rate in kilobits per second. (Range: 1-100000 kbps or maximum port speed, whichever is lower)
- **Burst** (byte)—Burst in bytes. (Range: 64-1522)
- **Exceed Action**—Specifies whether to drop the traffic that exceeds the specified rate or burst or to reduce the DSCP service level.
- **Set**—Decreases DSCP priority for non-conforming traffic. (Range: 0-63).
- **Drop**—Drops non-conforming traffic.

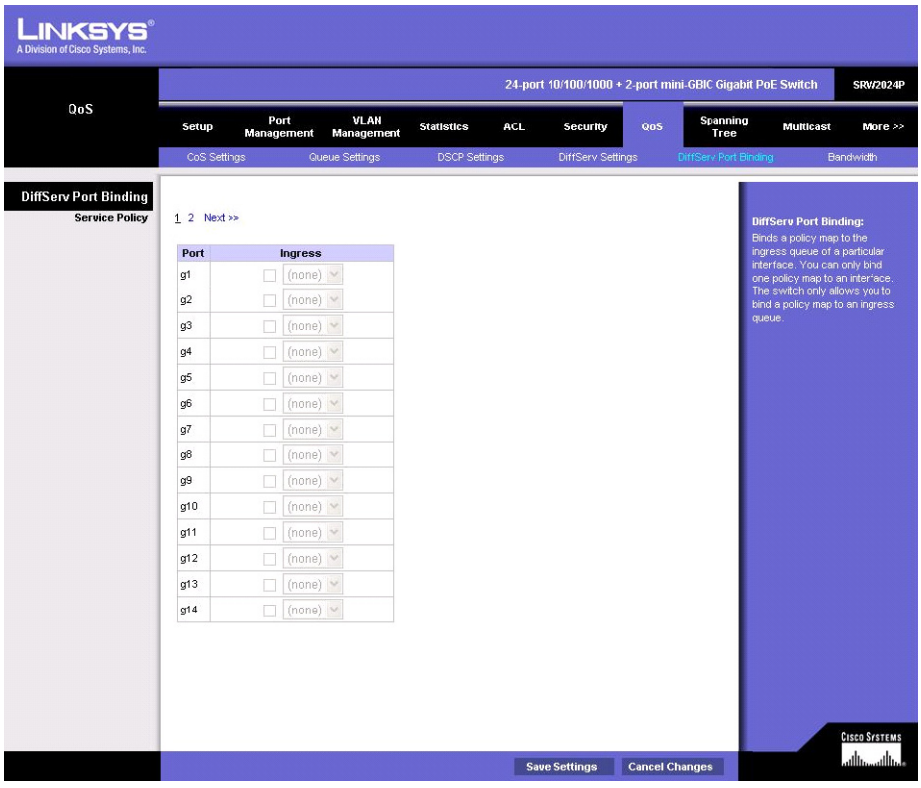
Add—Adds the specified criteria to the policy map.

Remove—Deletes a class from a policy.

Add classes to a selected policy and set the Action, Meter, Rate, Burst and Exceed values using the drop-down lists and fields provided then click **Add**.

QoS Tab - Diffserv Port Binding

This function binds a policy map to the ingress queue of a particular interface. You must first define a class map and set an ACL mask to match the criteria defined in the class map. Then define a policy map. Finally bind the service policy to the required interface. You can bind only one policy map to an interface. The current firmware does not allow you to bind a policy map to an egress queue.



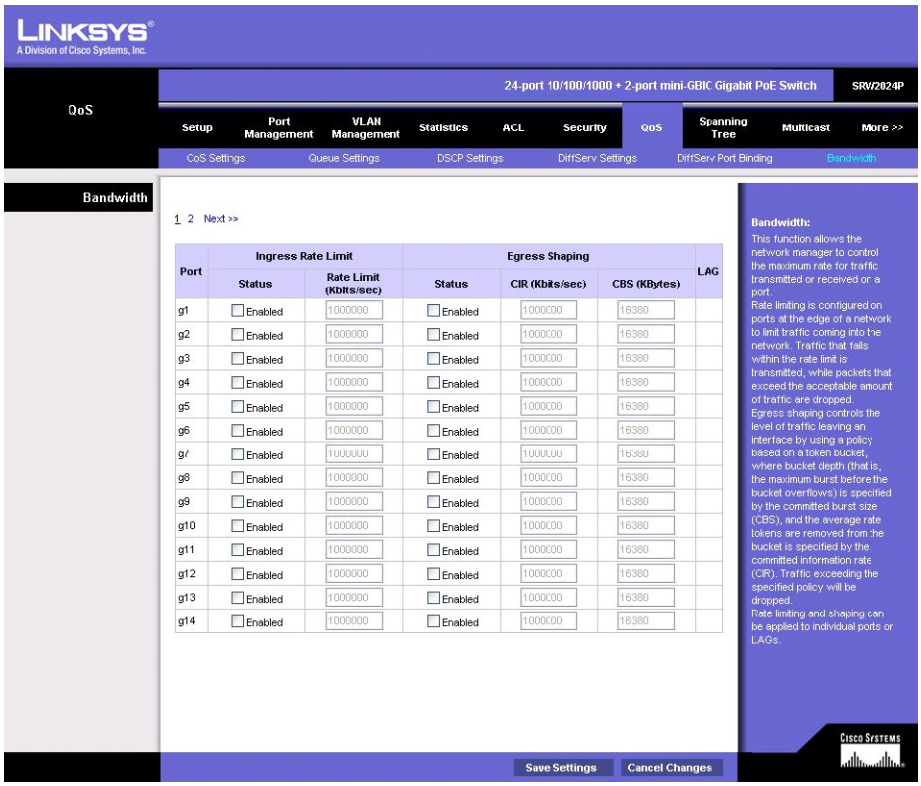
Select **Policy Map** for a port from the drop-down list.

Click **Save Settings** to save the changes.

QoS Tab - Bandwidth

This function allows the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic coming out of the switch. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or LAGs. When an interface is configured with this feature, the traffic rate is monitored by the hardware to verify conformity. Non-conforming traffic is dropped, and conforming traffic is forwarded without any changes.



Port—Displays the port or LAG number.

Status—Enables the rate limit (input or output) for the port or LAG. (Default: Disabled)

Rate Limit (Kbits/sec)—Sets the rate limit level for the port or LAG. For Fast Ethernet ports the default is 100000Kbits/sec (Range: 64-100000). For Gigabit Ethernet ports the default is 1000000Kbits/sec (Range: 64-1000000).

LAG—Indicates if ports are members of a LAG. To configure a rate limit for LAGs, go to the table entry for the LAG number, which is listed after port g24 at the end of the table.

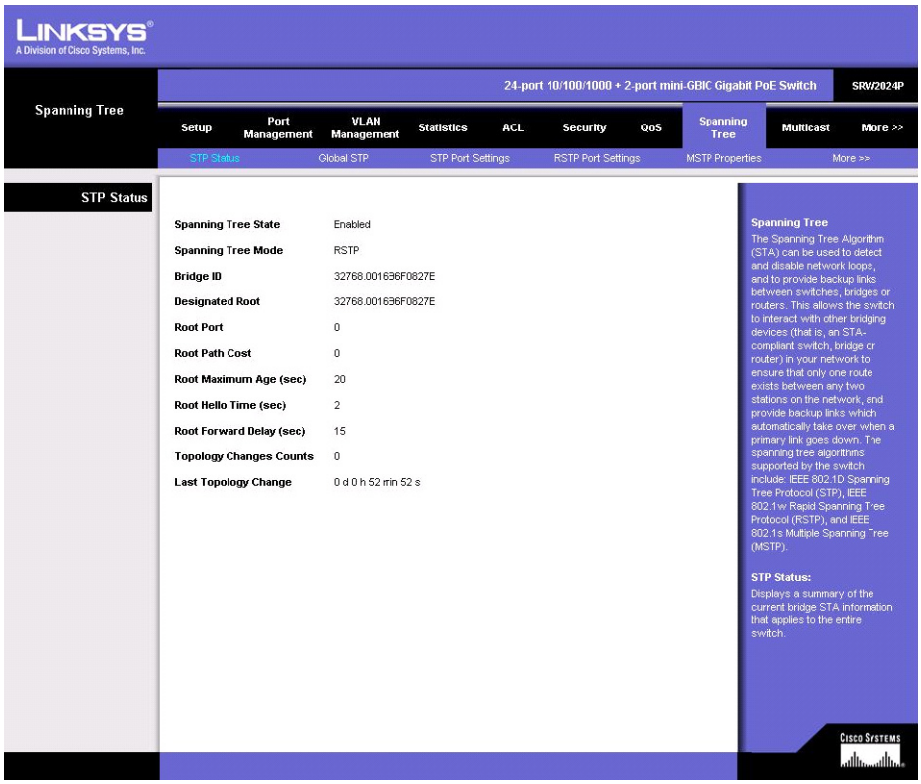
Set the Input Rate Limit Status or Output Rate Limit Status, then set the rate limit for individual interfaces or LAGs, and then click **Save Settings**.

Spanning Tree Tab

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This algorithm allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down. Loops occur when alternate routes exist between hosts. Loops in an extended network can cause bridges to forward traffic indefinitely, resulting in increased traffic and reducing network efficiency.

Spanning Tree Tab - STP Status

You can display a summary of the current bridge STA information that applies to the entire switch using the Information screen. This screen displays the following information.



Spanning Tree State—Indicates if STA is enabled on the device.

Spanning Tree Mode—Indicates the STA mode by which STP is enabled on the device.

Bridge ID—Identifies the bridge priority and MAC address.

Designated Root—Indicates the ID of the bridge with the lowest path cost to the instance ID.

Root Port—Indicates the port number that offers the lowest path cost from this bridge to the Root Bridge. It is significant when the Bridge is not the Root. The default is zero.

Root Path Cost—The cost of the path from this bridge to the root.

Root Maximum Age—Indicates the amount of time in seconds a bridge waits before sending configuration messages. The default max age is 20 seconds. The range is 6 to 40 seconds.

Root Hello Time—Indicates the number of seconds a root bridge waits between configuration messages. The default is 2 seconds. The range is 1 to 10 seconds.

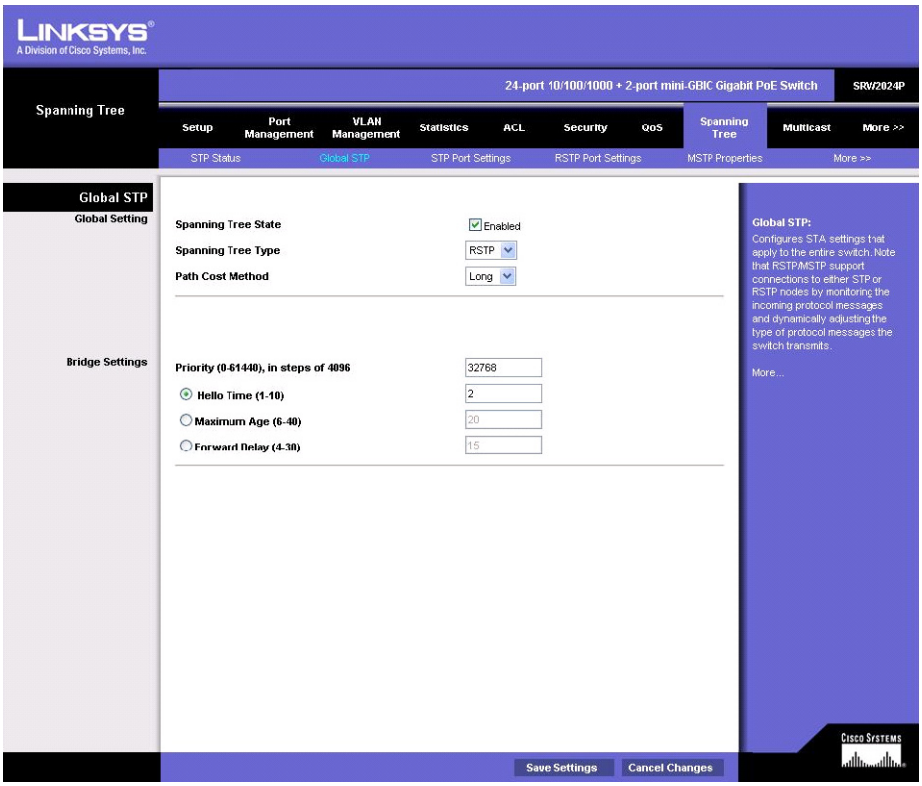
Root Forward delay—Indicates the number of seconds a bridge remains in a listening and learning state before forwarding packets. The default is 15 seconds. The range is 4 to 30 seconds.

Topology Changes Counts—Indicates the total amount of STP state changes that have occurred.

Last Topology Change—Indicates the amount of time that has elapsed since the bridge was initialized or reset, and the last topographic change occurred. The time is displayed in days, hours, minutes, and seconds, for example, 2 days 5 hours 10 minutes and 4 seconds.

Spanning Tree Tab - Global STP

Configure the global settings for STP using this screen. Global settings apply to the entire switch.



Spanning Tree State—Indicates if STP is enabled on the device.

Spanning Tree Type—Specifies the type of spanning tree used on the switch:

- **STP**—Spanning Tree Protocol (IEEE 802.1D); i.e., when this option is selected, the switch will use RSTP set to STP forced compatibility mode).

- **RSTP**—Rapid Spanning Tree Protocol (IEEE 802.1w); RSTP is the default.

Priority—Specifies the bridge priority value. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the device with the lowest priority value becomes the Root Bridge. The default value is 32768. The port priority value is provided in increments of 4096. For example, 4096, 8192, 12288, etc. The range is 0 to 65535.

Hello Time—Specifies the number of seconds a root bridge waits between configuration messages. The default is 2 seconds. The range is 1 to 10 seconds.

Maximum Age—The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STP information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to "ports" in this section mean "interfaces," which includes both ports and LAGs.) The default max age is 20 seconds. The range is 6 to 40 seconds.

Forward Delay—The maximum time (in seconds) this device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result. The default is 15 seconds. The range is 4 to 30 seconds.

Path Cost Method—The path cost is used to determine the best path between devices. The path cost method is used to determine the range of values that can be assigned to each interface

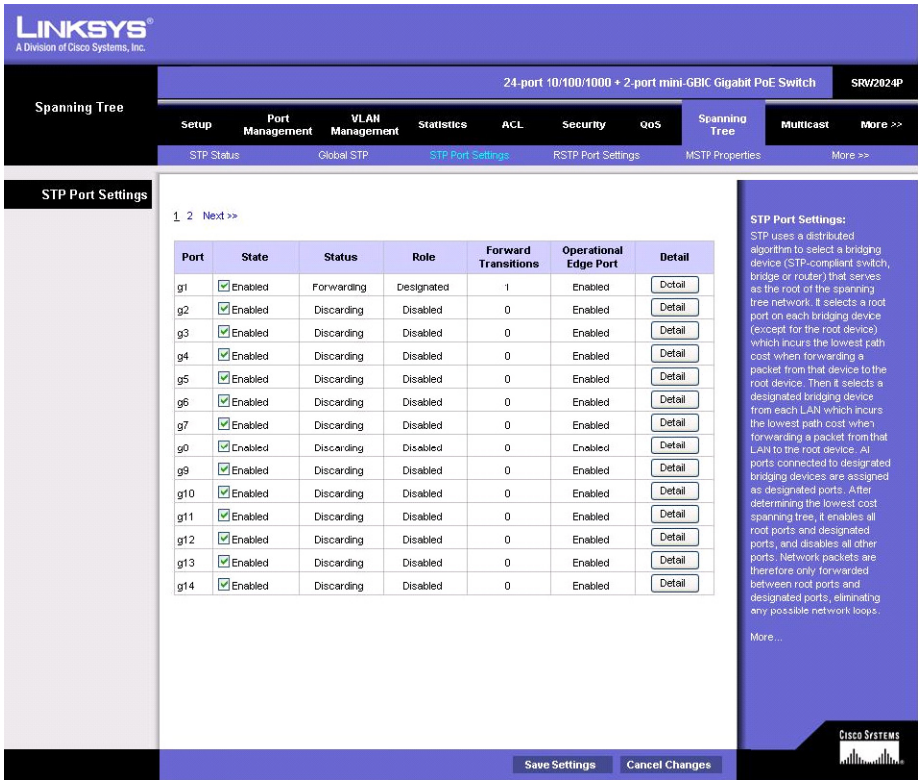
- **Long**—Specifies 32-bit based values that range from 1-200,000,000. (This is the default.
- **Short**—Specifies 16-bit based values that range from 1-65535.

Transmission Limit—The maximum transmission rate for BPDUs. This limit is specified by setting the minimum interval between the transmission of consecutive protocol messages. (Range: 1-10; Default: 3) Modify the required attributes for STP.

Click **Save Settings** to save the changes.

Spanning Tree Tab - STP Port Settings

The Port Information and LAG Information screens display the current status of ports and LAGs in the Spanning Tree.



State—Shows if Spanning Tree has been enabled on this interface.

Status—Displays current state of this port within the Spanning Tree:

- **Discarding**—Port receives STA configuration messages, but does not forward packets.
- **Learning**—Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
- **Forwarding**—Port forwards packets, and continues learning addresses.

Forward Transitions—The number of times this port has transitioned from the Learning state to the Forwarding state.

Operational Edge Port—This parameter is initialized to the setting for Administrative Edge Port in STP Port Setting detail, but will be set to false if a BPDU is received indicating that another bridge is attached to this port.

Operational Link Type—The operational point-to-point status of the LAN segment attached to this interface. This parameter is determined by manual configuration or by auto-detection, as described for Administrative Link Type in the STP Port Setting detail.

LAG—Indicates if ports are members of a LAG. To configure STP port settings for LAGs, go to the table entry for the LAG number, which is listed after port g24 at the end of the table.

Click **Detail** to configure STP Port Settings for an interface.

Click **Detail** to configure Path Cost, Priority, Administrative Edge Port (Fast Forwarding), and Administrative Link Type. Use the text fields provided to edit the values, then click **Apply**.

Designated Cost—The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.

Designated Port—The port priority and number of the port on the designated port.

Designated Bridge—The bridge priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.

Path Cost—This parameter is used by the STP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values should be assigned to ports with slower media. (Path cost takes precedence over port priority.) Note that when the Path Cost Method is set to "short," the maximum path cost is 65,535.

- **Range**—Ethernet: 200,000-20,000,000
  Fast Ethernet: 20,000-2,000,000
  Gigabit Ethernet: 2,000-200,000

- **Default**—Ethernet – Half duplex: 2,000,000; full duplex: 1,000,000; LAG: 500,000
  Fast Ethernet – Half duplex: 200,000; full duplex: 100,000; LAG: 50,000
  Gigabit Ethernet – Full duplex: 10,000; LAG: 5,000

Priority—Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch is the same, the port with the highest priority (i.e., lowest value) is configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with the lowest numeric identifier is enabled.

- **Default**—128

- **Range**—0-240, in steps of 16

Administrative Edge Port (Fast Forwarding)—You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers has the following benefits:

- Retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events

- Does not cause the spanning tree to initiate reconfiguration when the interface changes state

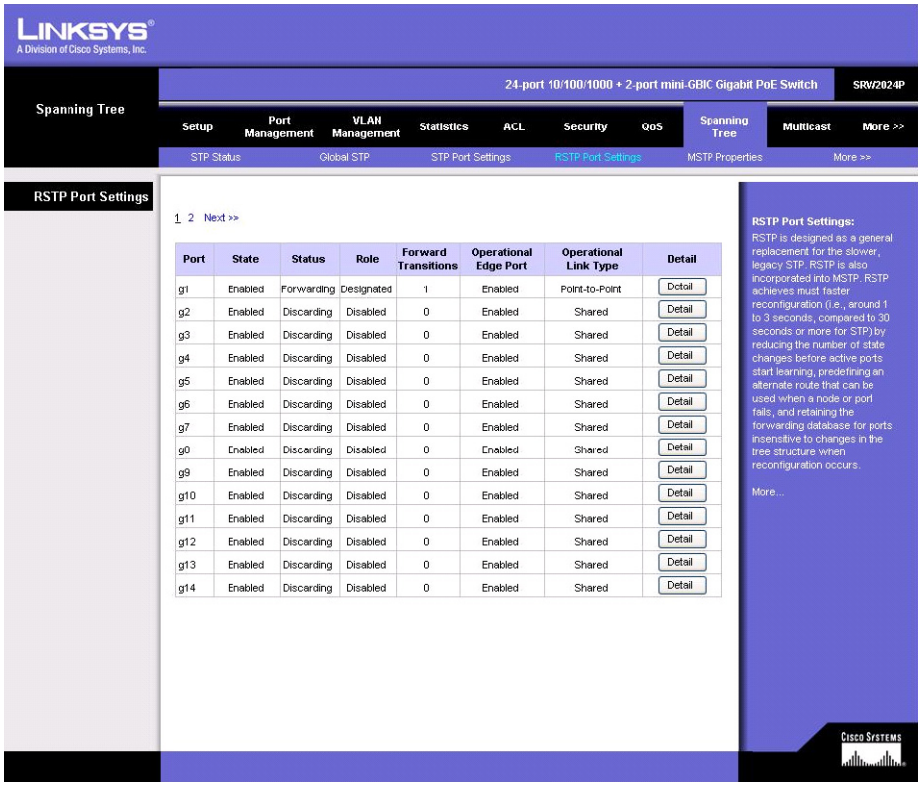
- Overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device. (Default: Disabled)

Administrative Link Type—The link type attached to this interface.

- **Point-to-Point**—A connection to exactly one other bridge.
- **Shared**—A connection to two or more bridges.
- **Auto**—The switch automatically determines if the interface is attached to a point-to-point link or to shared media. (This is the default setting.)

Spanning Tree Tab—RSTP Port Settings

This screen displays the current status of ports and LAGs for the Rapid Spanning Tree Protocol.



State—Shows if Spanning Tree has been enabled on this interface.

Status—Displays current state of this port within the Spanning Tree:

Discarding—Port receives STA configuration messages, but does not forward packets.

Learning—Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.

Forwarding—Port forwards packets, and continues learning addresses.

Role—Roles are assigned according to whether the port is part of the active topology connecting the bridge to the root bridge (i.e., root port), connecting a LAN through the bridge to the root bridge (i.e., designated port), or is the MSTI regional root (i.e., master port); or is an alternate or backup port that may provide connectivity if other bridges, bridge ports, or LANs

fail or are removed. The role is set to disabled (i.e., disabled port) if a port has no role within the spanning tree.

Forward Transitions—The number of times this port has transitioned from the Learning state to the Forwarding state.

Operational Edge Port—This parameter is initialized to the setting for Administrative Edge Port in STP Port Setting detail, but will be set to false if a BPDU is received indicating that another bridge is attached to this port.

Operational Link Type—The link type attached to this interface.

Point-to-Point—A connection to exactly one other bridge.

Shared—A connection to two or more bridges.

Auto—The Switch automatically determines if the interface is attached to a point-to-point link or to shared media.

Click **Detail** to configure RSTP Port Settings for an interface.

Click **Detail** to activate the protocol migration test, or to configure the Administrative Link Type. After completing any configuration changes, click Apply.

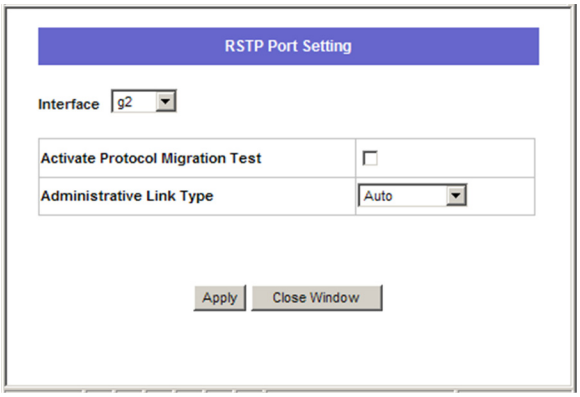
Activate Protocol Migration Test—If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the Protocol Migration button to manually re-check the appropriate BPDU format (RSTP or STP-compatible) to send on the selected interfaces. (Default: Disabled)

Administrative Link Type—The link type attached to this interface.

Point-to-Point—A connection to exactly one other bridge.

Shared—A connection to two or more bridges.

Auto—The Switch automatically determines if the interface is attached to a point-to-point link or to shared media. (This is the default setting).



Spanning Tree Tab—MSTP Properties

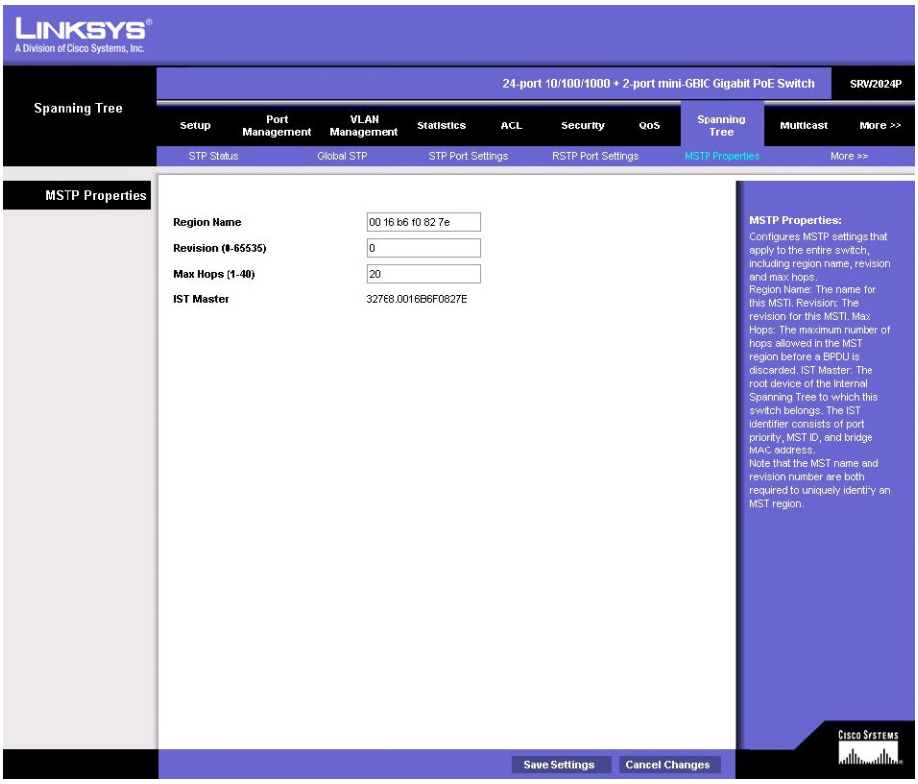
This screen includes configuration settings for the Multiple Spanning Tree Protocol.

Region Name—The name for this MSTI. (Maximum length: 32 characters)

Revision—The revision for this MSTI. (Range: 0-65535; Default: 0)

Max Hops—The maximum number of hops allowed in the MST region before a BPDU is discarded. (Range: 1-40; Default: 20)

IST Master—The root device of the Internal Spanning Tree of which this switch is a member. The IST identifier consists of port priority, MST ID, and bridge MAC address.



Spanning Tree Tab—MSTP Instance Settings

By default all VLANs are assigned to the Internal Spanning Tree (MST Instance 0) that connects all bridges and LANs within the MST region. This switch supports up to 9 instances. You should try to group VLANs which cover the same general area of your network. However, remember that you must configure all bridges within the same MSTI Region with the same set of instances, and the same instance (on each bridge) with the same set of VLANs. Also, note that RSTP treats each MSTI region as a single node, connecting all regions to the Common Spanning Tree.

MST ID—Instance identifier to configure. (Range: 0-4094; Default: 0)

VLAN ID—VLAN to assign to this selected MST instance. (Range: 1-4093)

Instance ID—Instance identifier of this spanning tree. (Default: 0)

Included VLAN—VLANs assigned to this instance.

Bridge Priority—Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. Note that lower numeric values indicate higher priority. (Range: 0-61440, in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440; Default: 32768)

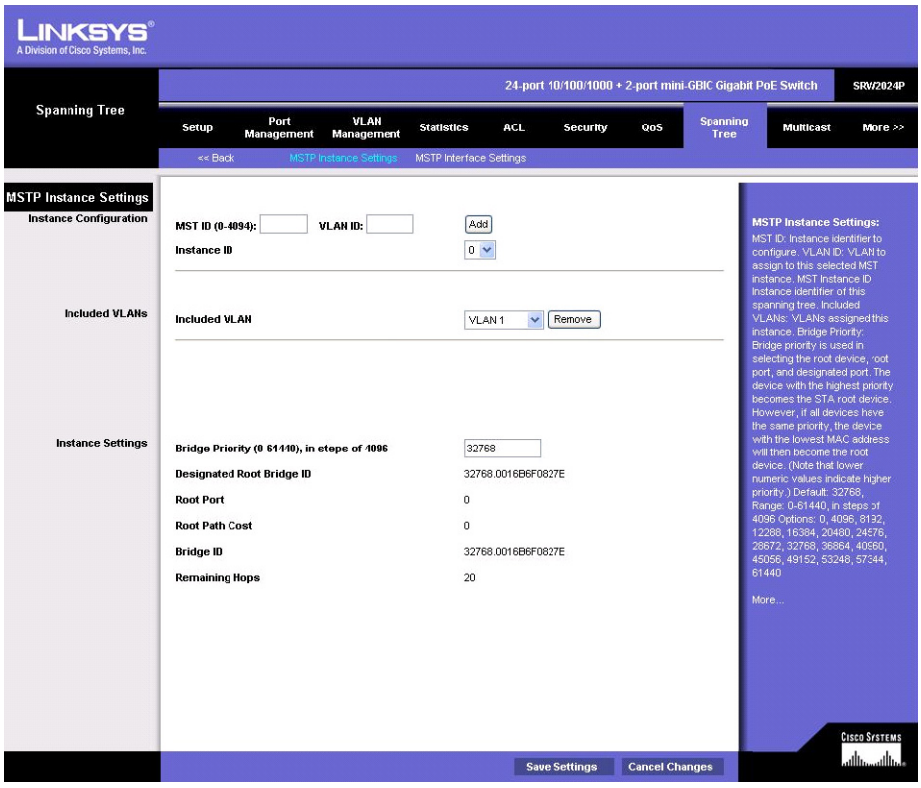
Designated Root Bridge ID—The priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.

Root Port—The port priority and number of the port on the designated bridging device through which this switch must communicate with the root of the Spanning Tree.

Root Path Cost—The contribution of this port to the path cost of paths towards the spanning tree root which include this port.

Bridge ID—The priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.

Remaining Hops—The number of hops allowed in the MST region before a BPDU is discarded. (Range: 1-40; Default: 20)



Spanning Tree Tab—MSTP Interface Settings

This screen displays the current status of ports and LAGs for the Multiple Spanning Tree Protocol.

State—Shows if Spanning Tree has been enabled on this interface.

Status—Displays current state of this port within the Spanning Tree.

Discarding—Port receives STA configuration messages, but does not forward packets.

Learning—Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.

Forwarding—Port forwards packets, and continues learning addresses.

Role—Roles are assigned according to whether the port is part of the active topology connecting the bridge to the root bridge (i.e., root port), connecting a LAN through the bridge to the root bridge (i.e., designated port), or is the MSTI regional root (i.e., master port); or is an alternate or backup port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed. The role is set to disabled (i.e., disabled port) if a port has no role within the spanning tree.

Forward Transitions—The number of times this port has transitioned from the Learning state to the Forwarding state.

Operational Edge Port—This parameter is initialized to the setting for Administrative Edge Port in STP Port Setting detail, but will be set to false if a BPDU is received indicating that another bridge is attached to this port.

Click **Detail** to configure MSTP Interface Settings for an interface.

Click **Detail** to path cost and interface priority. After completing any configuration changes, click **Apply**.

Designated Cost—The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.

Designated Port—The port priority and number of the port on the designated port.

Designated Bridge—The bridge priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.

Path Cost—This parameter is used by the STP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Also, note that path cost takes precedence over port priority.

(**Range**— 0 for auto-configuration, 1-65535 for the short path cost method, 1-200,000,000 for the long path cost method)

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost “0” is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

Range—Ethernet: 200,000-20,000,000

Fast Ethernet—20,000-2,000,000

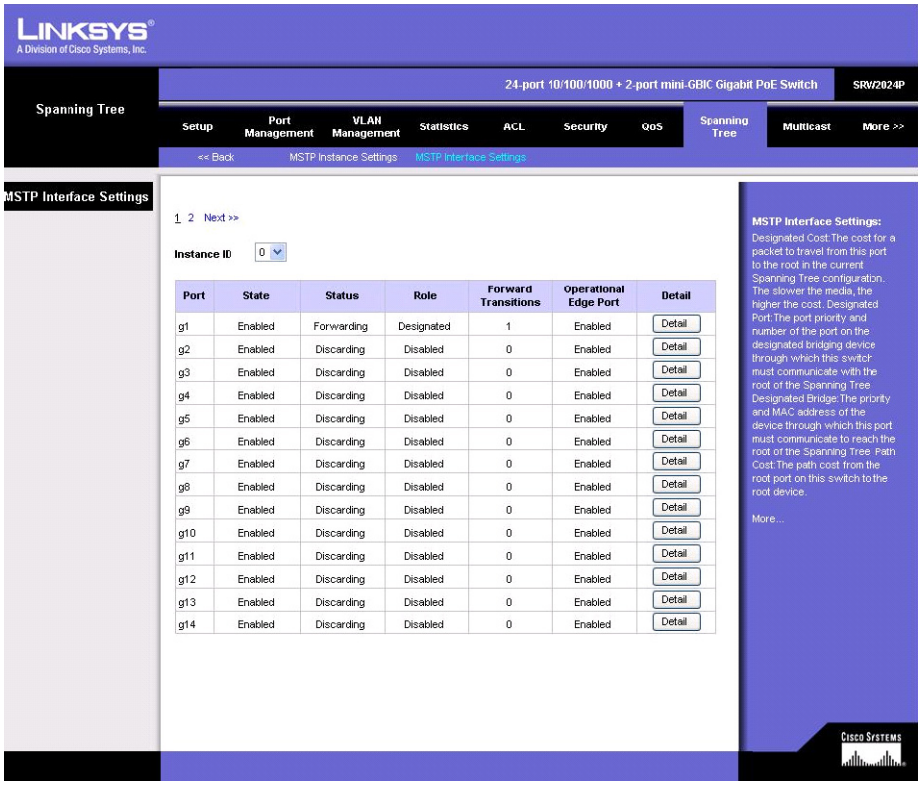
Gigabit Ethernet—2,000-200,000

Default—Ethernet – Half duplex: 2,000,000; full duplex: 1,000,000; LAG: 500,000

Fast Ethernet—Half duplex: 200,000; full duplex: 100,000; LAG: 50,000

Gigabit Ethernet—Full duplex: 10,000; LAG: 5,000

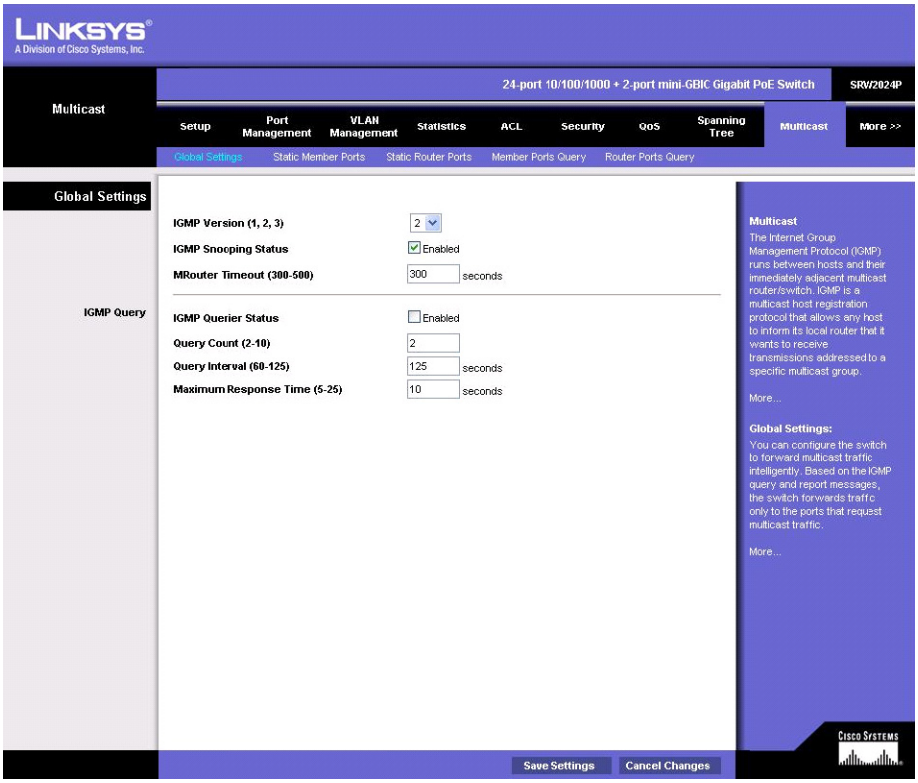
Interface Priority—Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. (Range: 0-240, in steps of 16; Default: 128)



Multicast Tab - Global Settings

You can configure the switch to forward multicast traffic intelligently. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request multicast traffic.

This setting prevents the switch from broadcasting the traffic to all ports and possibly disrupting network performance.



IGMP Version (1,2,3)

IGMP Snooping Status—When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. This function is also referred to as IGMP Snooping. (Default: Enabled).

IGMP Querier Status—When enabled, the switch can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic. (Default: Enabled).

IGMP Query Count—Sets the maximum number of queries that can be issued to a client without receiving a response. When this limit is met, the switch drops the non-responsive client from the multicast group. (Range: 2-10; Default: 2)

IGMP Query Interval—Sets the number of seconds that elapse between IGMP host-query messages. (Range: 60-125 seconds; Default: 125)

IGMP Report Delay—Sets the number of seconds that elapse between receiving an IGMP Report for an IP multicast address on a port before the switch sends an IGMP Query out of that port and removes the entry from its list. (Range: 5-25 seconds; Default: 10)

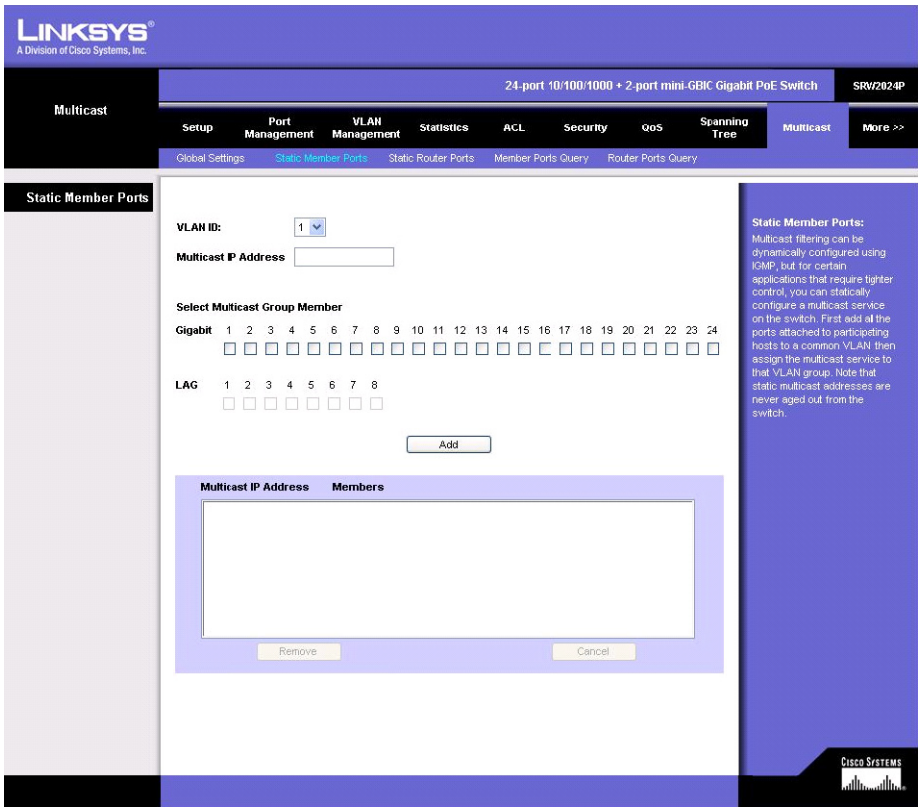
IGMP Query Timeout—The number of seconds the switch waits after the previous querier stops before it considers the router port (i.e., the interface which had been receiving query packets) to have expired. (Range: 300-500 seconds; Default: 300)

IGMP Version—Sets the protocol version for compatibility with other devices on the network. (Range: 1-2; Default: 2)

Click **Save Settings** to save the changes.

Multicast Tab - Static Member Ports

Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages. For certain applications that require tighter control, you may need to statically configure a multicast service on the switch. First add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.

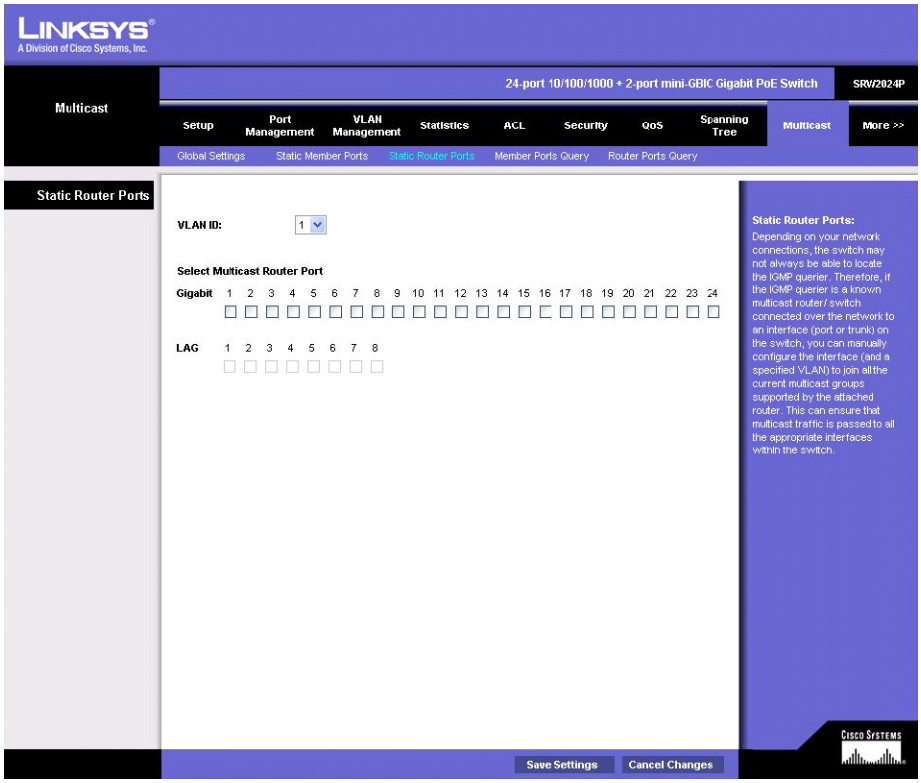


Specify the interface attached to a multicast service (via an IGMP-enabled switch or multicast router), indicate the VLAN that will propagate the multicast service, specify the multicast IP address, and click **Add**.

Multicast Tab - Static Router Ports

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/ switch connected over the network to an interface (port or lag) on the switch, you can manually configure the interface (and a specified VLAN) to join all the current multicast groups supported by the

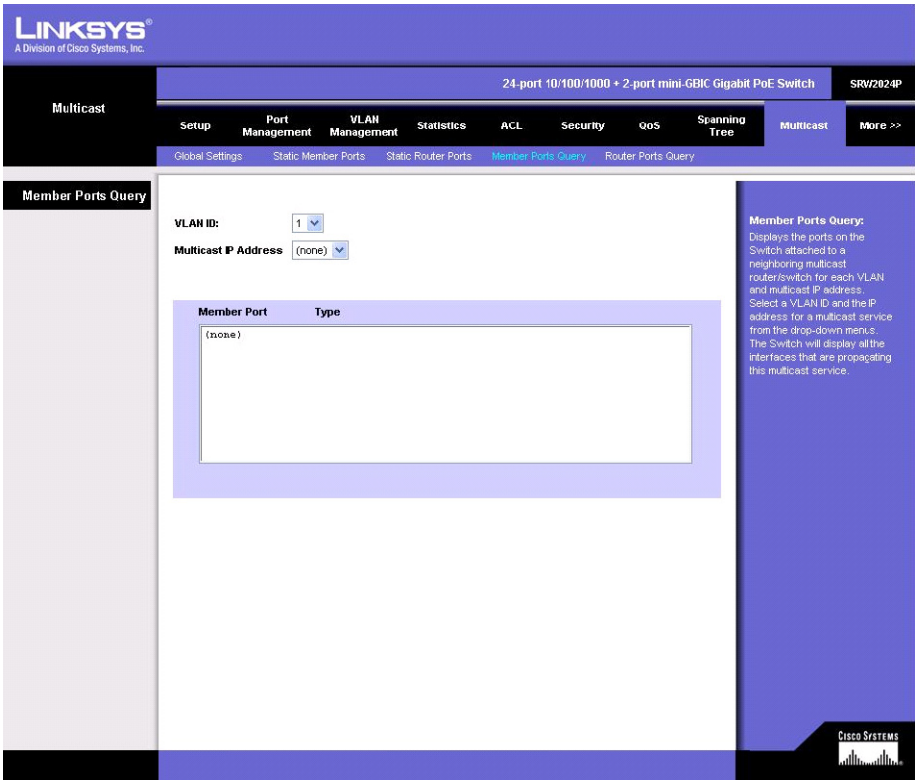
attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the switch.



Specify the interfaces attached to a multicast router, indicate the VLAN which will forward all the corresponding multicast traffic, and then click **Add**.

Multicast Tab - Member Ports Query

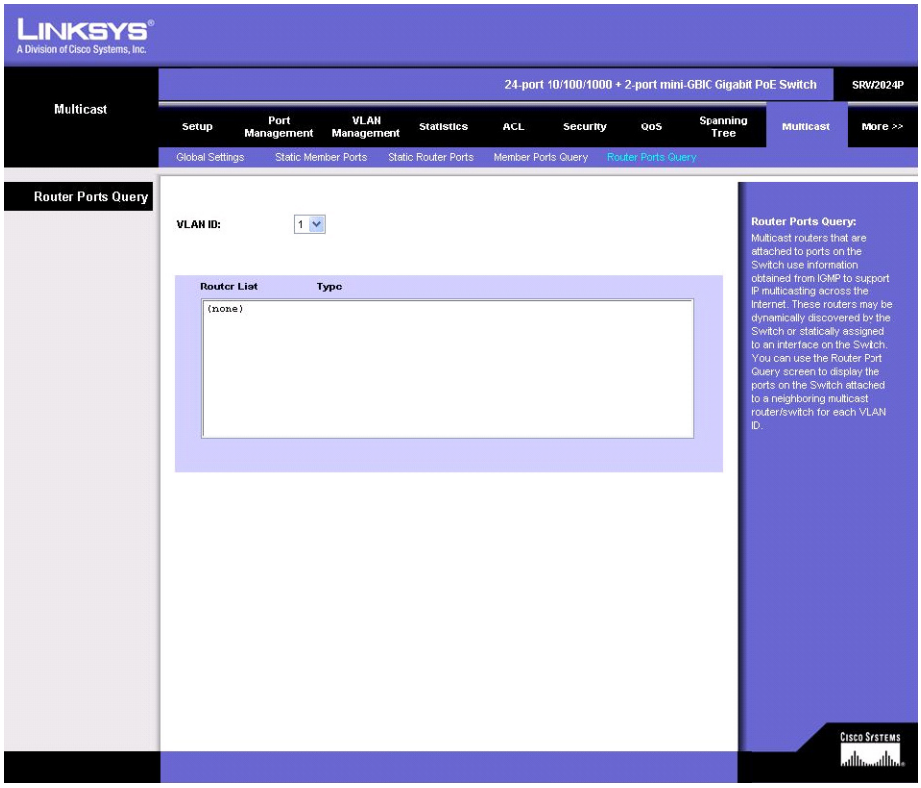
You can use the *Member Port Query* screen to display the ports on the switch attached to a neighboring multicast router/switch for each VLAN and multicast IP address.



Select a VLAN ID and the IP address for a multicast service from the drop-down lists. The switch displays all the interfaces that are propagating this multicast service

Multicast Tab - Router Ports Query

Multicast routers that are connected to the switch use information obtained from IGMP to support IP multicasting across the Internet. These routers may be dynamically discovered by the switch or statically assigned to an interface on the switch.



You can use the *Router Port Query* screen to display the ports on the switch attached to a neighboring multicast router/switch for each VLAN ID.

Select a VLAN ID from the drop-down lists. The switch will display all the interfaces that have attached multicast routers dynamically discovered by the switch, or those that have been statically assigned to an interface on the switch.

SNMP Tab

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

The switch includes an onboard agent that supports SNMP versions 1, 2c, and 3. This agent continuously monitors the status of the switch hardware, as well as the traffic passing through its ports. A network management station can access this information using network management platforms such as HP OpenView.

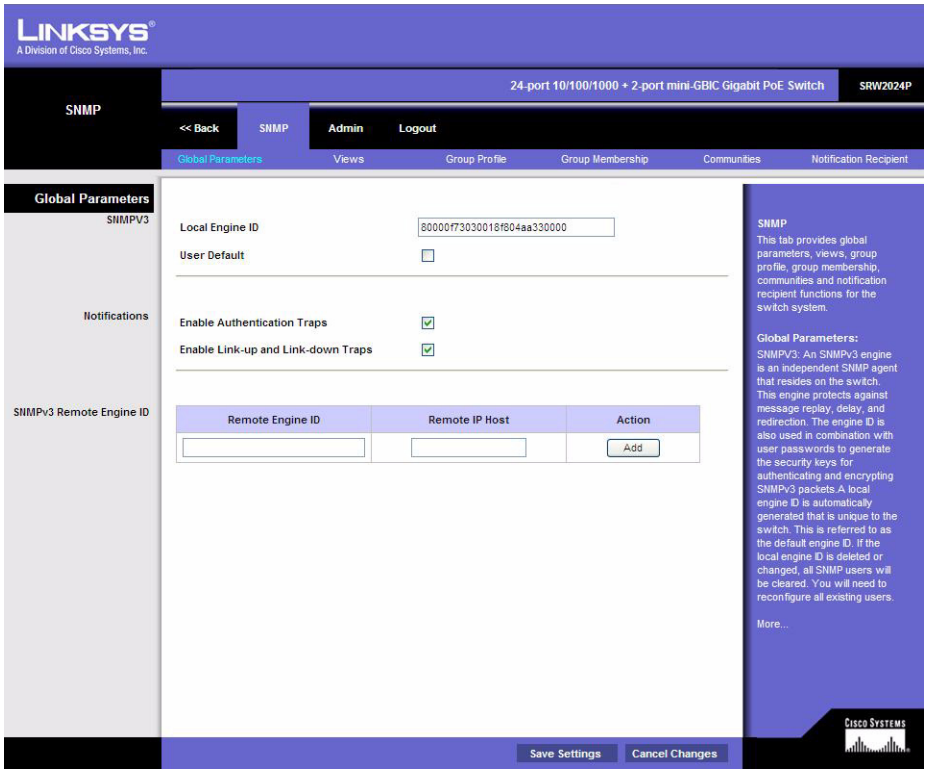
Access to the onboard agent from clients using SNMP v1 and v2c is controlled by community strings. To communicate with the switch, the management station must first submit a valid

community string for authentication. Access to the switch from clients using SNMPv3 provides additional security features that cover message integrity, authentication, and encryption; as well as controlling user access to specific areas of the MIB tree.

This tab provides global parameters, views, group profile, group membership, communities and notification recipient functions for the switch system.

SNMP Tab—Global Parameters

The Global Parameters screen includes configuration settings for the local and remote engine identifiers used by SNMPv3, and enabling or disabling trap messages sent to designated management stations.



SNMPv3

Local Engine ID. An SNMPv3 engine is an independent SNMP agent that resides on the switch. This engine protects against message replay, delay, and redirection. The engine ID is also used in combination with user passwords to generate the security keys for authenticating and encrypting SNMPv3 packets.A local engine ID is automatically generated that is unique to the switch. This is referred to as the default engine ID. If the local engine ID is deleted or changed, all SNMP users will be cleared. You will need to reconfigure all existing users.

A new engine ID can be specified by entering 1 to 26 hexadecimal characters. If less than 26 characters are specified, trailing zeroes are added to the value. For example, the value “1234” is equivalent to “1234” followed by 22 zeroes.

User Default—Check this box to restore the default local engine ID.

Notifications

Enable Authentication Traps—Issues a notification message to specified IP trap managers whenever an invalid community string is submitted during the SNMP access authentication process. (Default: Enabled)

Enable Link-up and Link-down Traps—Issues a notification message whenever a port link is established or broken. (Default: Enabled)

SNMPv3 Remote Engine ID

Remote Engine ID. To send inform messages to an SNMPv3 user on a remote device, you must first specify the engine identifier for the SNMP agent on the remote device where the user resides. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.

SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it.

A new engine ID can be specified by entering 1 to 26 hexadecimal characters. If less than 26 characters are specified, trailing zeroes are added to the value. For example, the value “1234” is equivalent to “1234” followed by 22 zeroes.

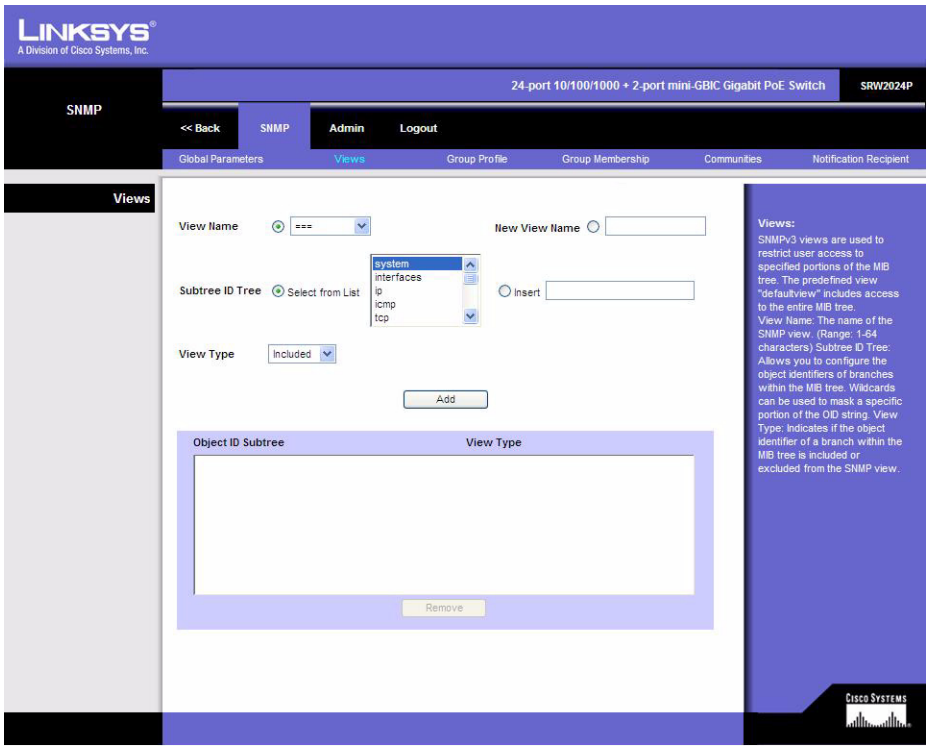
Remote IP Host—This is the address of a new management station to receive trap messages.

Specify both the remote engine ID and IP address of the remote host, and then click Add.

After configuring the required entries, click **Save Settings** to save the changes.

SNMP Tab—Views

The Views screen includes configuration settings used to restrict user access to specified portions of the MIB tree.



View Name—Select a existing name from the scroll-down list to show the currently configured object identifiers of branches within the MIB tree that define the SNMP view.

New View Name—Use this field to create a new SNMP view. (Range: 1-64 characters)

Subtree ID Tree—Specifies the object identifiers of branches within the MIB tree to include in the view.

Select from List—A list of commonly used MIB branches.

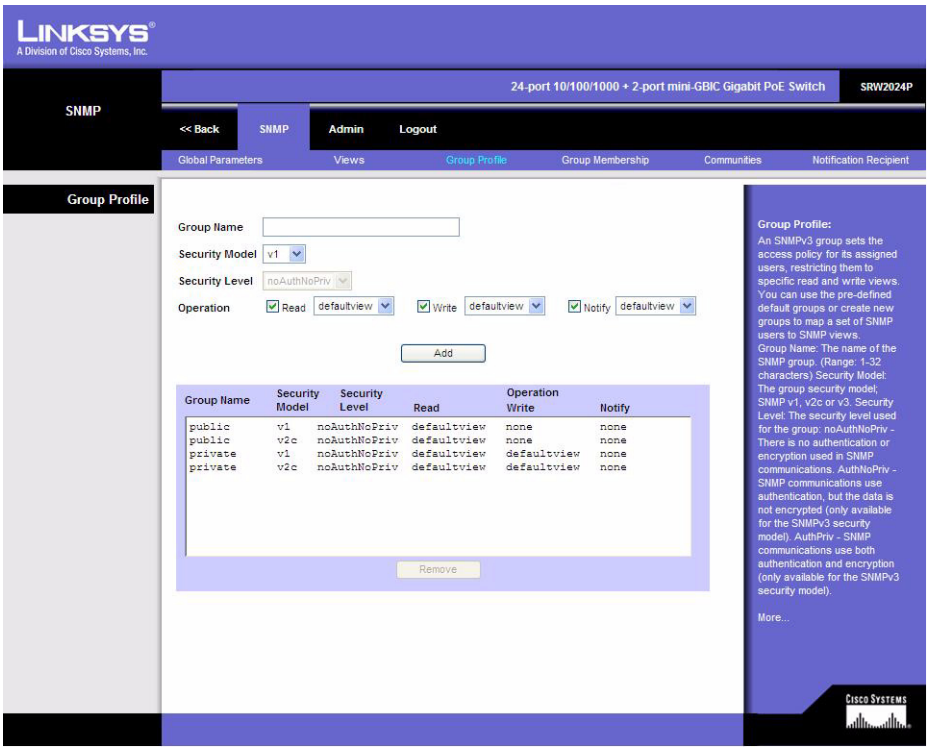
Insert—Allows you to configure the object identifiers of branches within the MIB tree. Wild cards can be used to mask a specific portion of the OID string. For example, 1.3.6.1.2.1.2.2.1.1.* includes the MIB-2 interfaces table, and the wildcard mask selects all index entries.

View Type—Indicates if the object identifier of a branch within the MIB tree is included or excluded from the SNMP view.

To configure an SNMP view, enter the view name, specify OID subtrees in the switch MIB to be included or excluded in the view, and then click **Add**.

SNMP Tab—Group Profile

The Group Profile screen is used to set the access policy for a group of users, restricting them to specific read, write and notify views.



Group Name—The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)

Security Model—The user security model; SNMP v1, v2c or v3.

Security Level—The security level used for the group:

noAuthNoPriv—There is no authentication or encryption used in SNMP communications. (This is the default for SNMPv3.)

AuthNoPriv—SNMP communications use authentication, but the data is not encrypted (only available for the SNMPv3 security model).

AuthPriv—SNMP communications use both authentication and encryption (only available for the SNMPv3 security model).

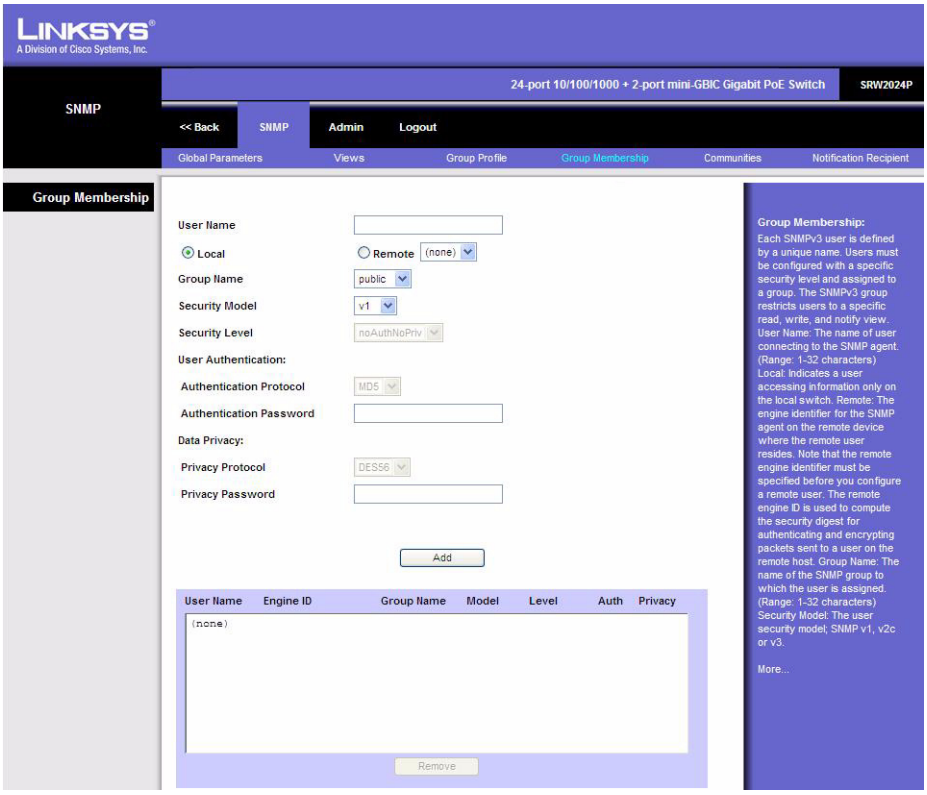
Operation—Specifies the view type for read, write and notify operations.

To configure an SNMP group, enter the group name, specify the security model and security level, select the view for read and notify operations, and then click **Add**.

SNMP Tab—Group Membership

The Group Membership screen is used to configure local and remote SNMPv3 users. Each SNMPv3 user is defined by a unique name. Users must be configured with a specific security

level and assigned to a group. The SNMPv3 group restricts users to a specific read, write, and notify view.



User Name—The name of user connecting to the SNMP agent. (Range: 1-32 characters)

Local—Indicates a user accessing information only on the local switch.

Remote—The engine identifier for the SNMP agent on the remote device where the remote user resides. Note that the remote engine identifier must be specified before you configure a remote user. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.

Group Name—The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)

Security Model—The user security model; SNMP v1, v2c or v3. (Default: v1)

Security Level—The security level used for the user:

noAuthNoPriv—There is no authentication or encryption used in SNMP communications. (This is the default for SNMPv3.)

AuthNoPriv—SNMP communications use authentication, but the data is not encrypted (only available for the SNMPv3 security model).

AuthPriv—SNMP communications use both authentication and encryption (only available for the SNMPv3 security model).

User Authentication

Authentication Protocol—The method used for user authentication. (Options: MD5, SHA; Default: MD5)

Authentication Password—A minimum of eight plain text characters is required.

Data Privacy

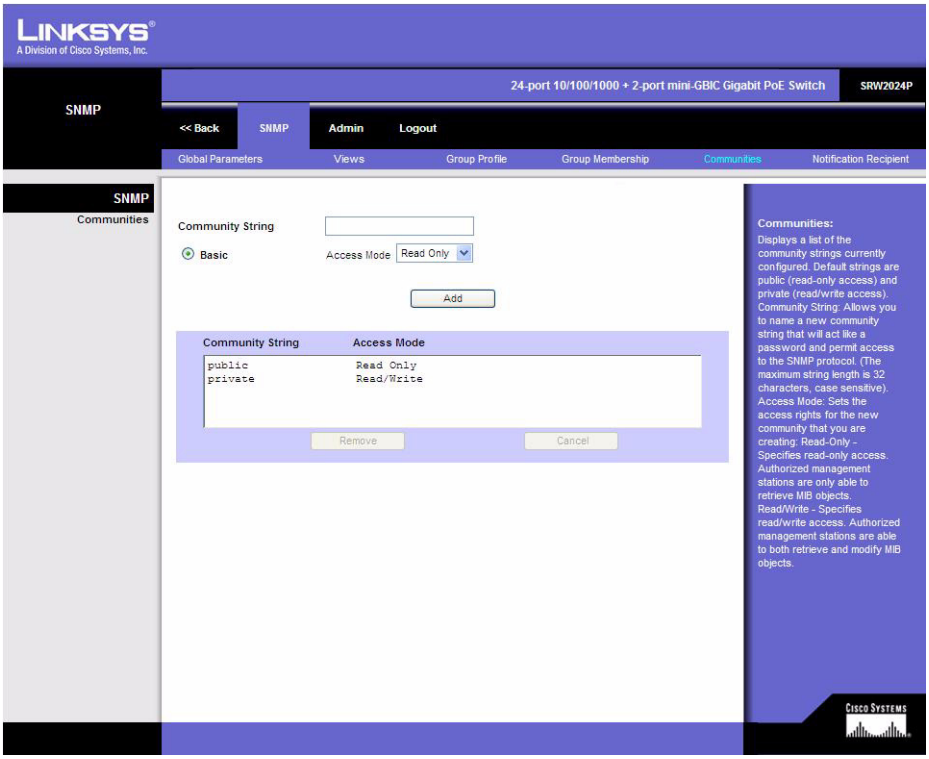
Privacy Protocol—The encryption algorithm use for data privacy; only 56-bit DES is currently available.

Privacy Password—A minimum of eight plain text characters is required.

After configuring each user, click **Add**.

SNMP Tab—Communities

The Communities screen is used to configure community strings which control access to the onboard agent from SNMP v1 or v2c clients. To communicate with the switch, the management station must first submit a valid community string for authentication. You may configure up to five community strings. The default strings are "public" (read-only access) and "private" (read/write access).



Community String—A community string that acts like a password and permits access to the SNMP protocol. (Range: 1-32 characters, case sensitive)

Access Mode—Specifies the access rights for the community string.

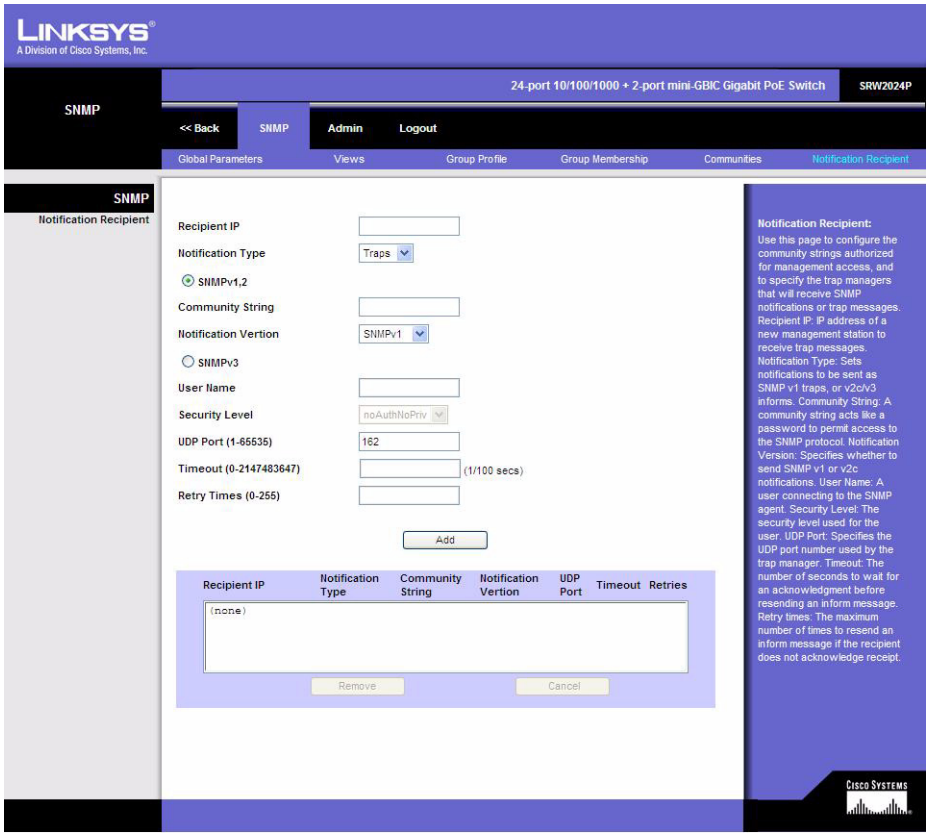
Read-Only – Authorized management stations are only able to retrieve MIB objects.

Read/Write—Authorized management stations are able to both retrieve and modify MIB objects.

After configuring each community string, click **Add**.

SNMP Tab—Notification Recipient

The Notification Recipient screen is used to configure the trap managers that will receive SNMP notifications or trap messages, and the community strings by which these devices are authorized management access.



Traps indicating status changes are issued by the Switch to specified trap managers. You must specify trap managers so that key events are reported by the Switch to your management station (using network management platforms such as HP OpenView).

You can specify up to five management stations that will receive authentication failure messages and other notification messages from the Switch.

Recipient IP—IP address of a new management station to receive trap messages.

Notification Type—Specifies whether to send notifications as SNMP v1 traps, or v2c/v3 informs. (Default: Version 1 traps)

SNMP v1,2

Community String—Allows you to name a new community string that will act like a password and permit access to the SNMP protocol. (The maximum string length is 32 characters, case sensitive).

Notification Version—Specifies whether to send notifications using SNMP v1 or SNMP v2c. (Default: Version 1)

SNMP v3

User Name—The name of user connecting to the SNMP agent. (Range: 1-32 characters)

Security Level—The security level used for the user.

noAuthNoPriv—There is no authentication or encryption used in SNMP communications. (This is the default for SNMPv3.)

AuthNoPriv—SNMP communications use authentication, but the data is not encrypted (only available for the SNMPv3 security model).

AuthPriv—SNMP communications use both authentication and encryption (only available for the SNMPv3 security model).

General Settings

UDP Port—Specifies the UDP port number used by the trap manager. (Range: 1-65535; Default: 162)

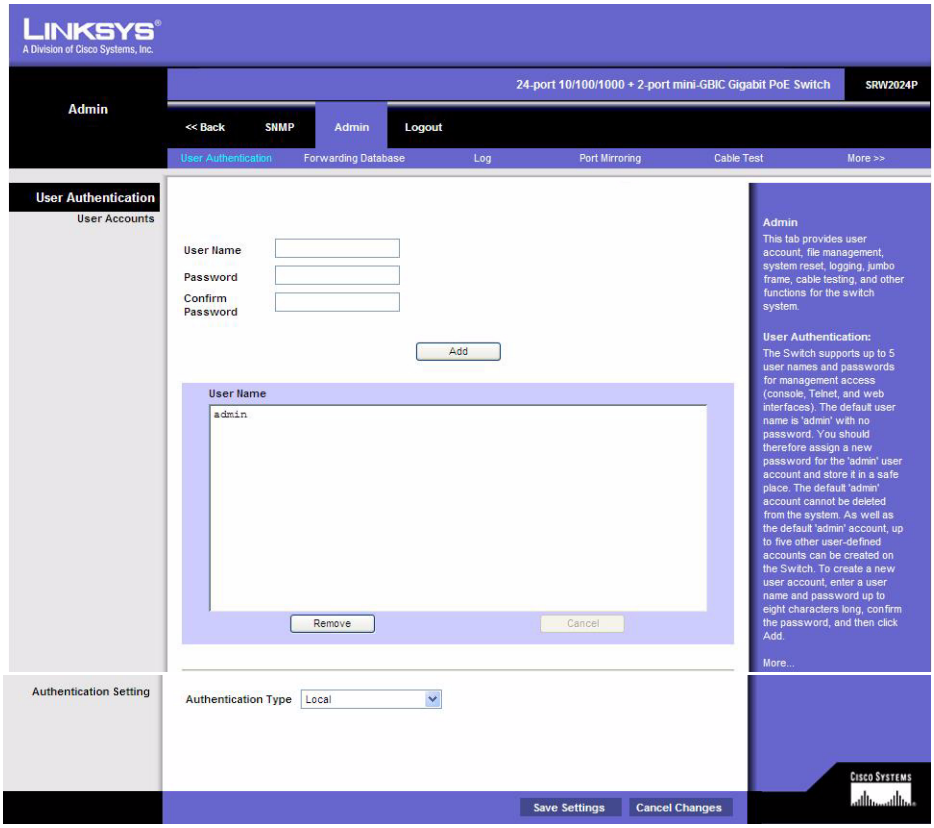
Timeout—The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)

Retry times—The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)

Enter a notification recipient based on an SNMPv1/v2 community string or an SNMPv3 user, then click **Add**.

Admin Tab - User Authentication

The switch supports up to five user names and passwords for management access (console and web interfaces). The default user name is “admin” with no password. You should therefore assign a new password for the “admin” user account and store it in a safe place. The default "admin" account cannot be deleted from the system.



As well as the default “admin” account, up to five other user-defined accounts can be created on the switch. To create a new user account, enter a user name and password up to eight characters long, confirm the password, and then click **Add**.

To change the password for a specific user, select the user name from the list, enter the new password, confirm the password by entering it again, and then click **Update**.

User Name—Displays the user name.

Password—Specifies the new password. The password is not displayed. As each character is entered an asterisk (*) appears in the field. (Range: 1-159 characters)

Confirm Password—Confirms the new password. The password entered into this field must match the password entered in the Password field.

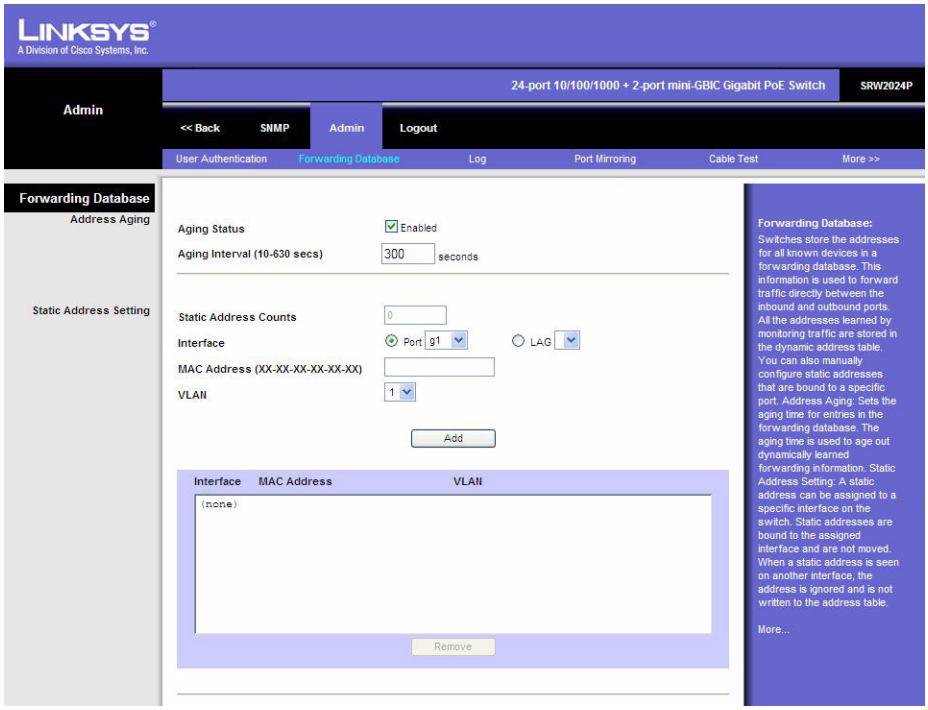
The Add button adds the user configuration to the table. The Remove button removes a user configuration from the table.

Authentication Type—Defines the user authentication methods. Combinations of all the authentication methods can be selected. The possible field values are:

- **Local—**Authenticates the user at the device level. The device checks the user name and password for authentication.
- **RADIUS—**Authenticates the user at the RADIUS server.
- **TACACS+—**Authenticates the user at the TACACS+ server.

Admin Tab - Forwarding Database

Switches store the addresses for all known devices in a forwarding database. This information is used to forward traffic directly between the inbound and outbound ports. All the addresses learned by monitoring traffic are stored in the dynamic address table. You can also manually configure static addresses that are bound to a specific port.



Address Aging

Sets the aging time for entries in the forwarding database. The aging time is used to discard outdated forwarding information.

Aging Status—When enabled, dynamic MAC addresses are discarded after the Aging Interval has expired.

Aging Interval—This is the amount of time in seconds after which dynamic address table entries are discarded. The range is 10-10000.

Set the Aging Interval by entering the number of seconds into the text field.

Click **Save Settings** to save the changes.

Static Address Setting

A static address can be assigned to a specific interface on the switch. Static addresses are bound to the assigned interface and will not be reassigned. When a static address is detected on another interface, the address will be ignored and will not be written to the address table.

Static Address Counts—The number of manually configured addresses. The switch allows 1000 Static Address Counts.

Interface—Port or LAG associated with the device assigned a static address.

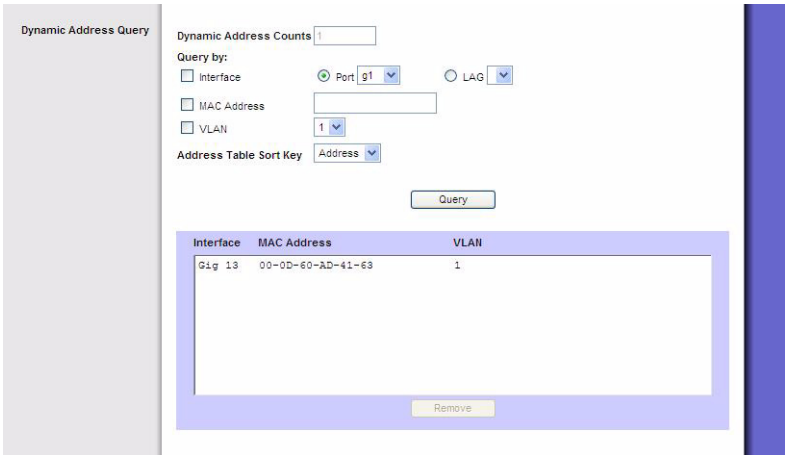
MAC Address—Physical address of a device mapped to this interface.

VLAN—ID of a configured VLAN (1-4094).

Specify the interface, the static MAC address, and VLAN, then click **Add**. The current static addresses on the switch are all listed text box. To delete a static MAC address from the forwarding database, select the entry in the displayed list, then click **Remove**.

Dynamic Address Query

The switch's dynamic address table contains the MAC addresses learned by monitoring the source address for traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports.



You can query the forwarding database to find specific dynamic MAC addresses, or view MAC addresses associated with a specific interface or VLAN.

Dynamic Address Counts—The number of addresses dynamically learned on the switch.

Interface—Indicates to display MAC addresses for a specific port or LAG.

MAC Address—Indicates to display details for a specific MAC address.

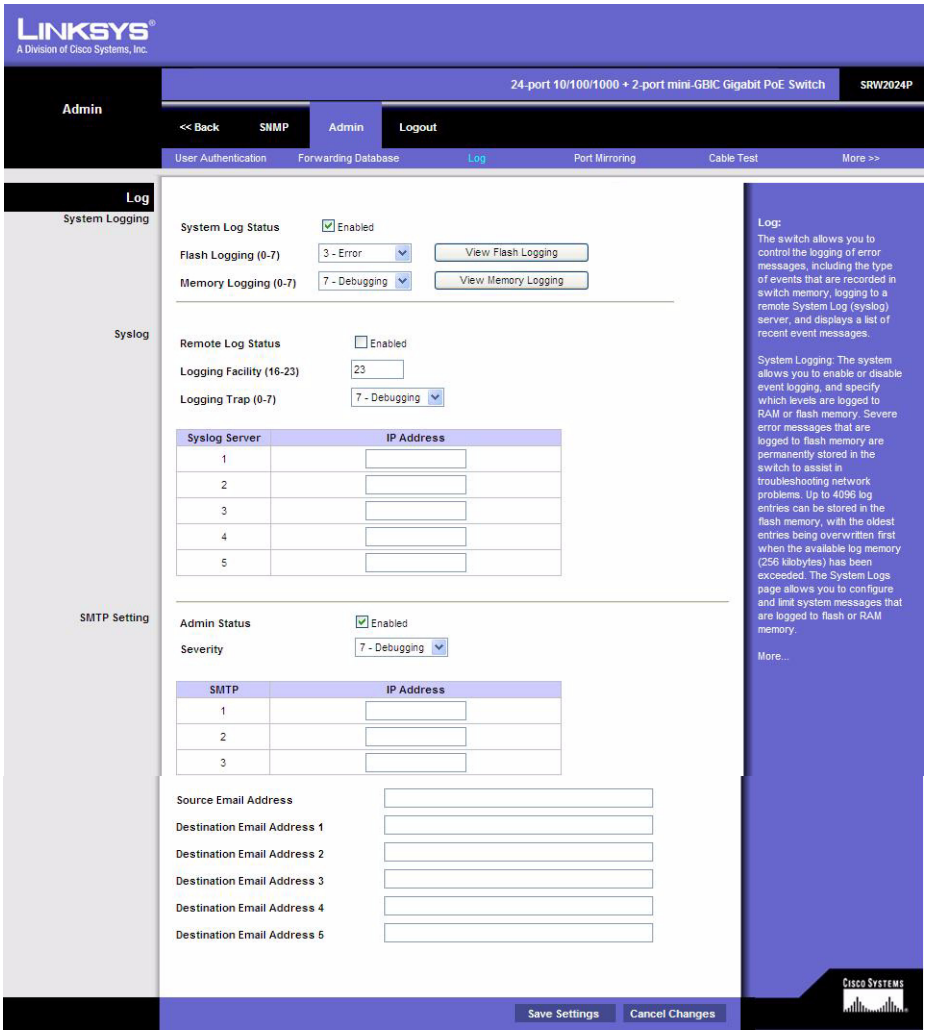
VLAN—Indicates to display MAC addresses for a specific configured VLAN (1-4094).

Address Table Sort Key—Sorts the information displayed based on MAC address, VLAN, or interface (port or LAG).

Check the Interface, MAC Address, or VLAN checkbox to specify the search type. Then select the method of sorting the displayed addresses. Finally, click **Query**. The dynamic addresses that conform to the search criteria are listed in the text box. To delete a MAC address from the forwarding database, select the entry in the displayed list, then click **Remove**.

Admin Tab - Log

The switch allows you to configure and limit system messages that are logged to flash or RAM memory, configure the logging of messages that are sent to remote System Log (Syslog) servers, and set an event-level threshold for sending email alert messages to system administrators.



The following table describes the system event levels.

Level*	Severity Name	Description
7	Debug	Debugging messages
6	Informational	Informational messages only

Level*	Severity Name	Description
5	Notice	Normal but significant condition, such as a cold start
4	Warning	Warning conditions, such as return false or unexpected return
3	Error	Error conditions, such as invalid input or default used
2	Critical	Critical conditions, such as memory allocation, free memory error, or resource exhausted
1	Alert	Immediate action needed
0	Emergency	System unusable

* The current firmware release supports only Level 2, 5 and 6 event messages.

System Logging

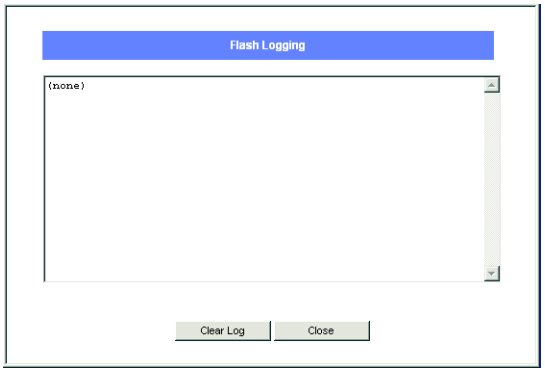
The system allows you to enable or disable event logging, and specify which event levels are logged to RAM or flash memory. Severe error messages that are logged to flash memory are permanently stored in the switch to assist in troubleshooting network problems.

System Log Status—Enables/disables the logging of debug or error messages to the logging process. (Default: Enabled)

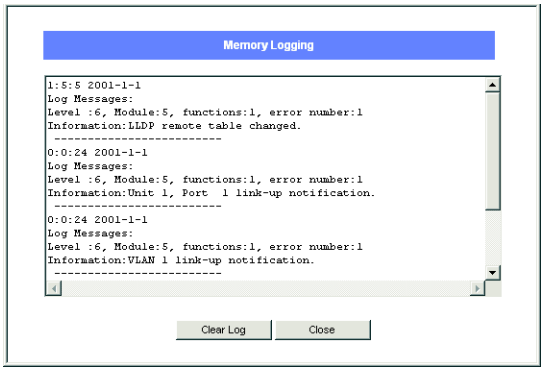
Flash Level (0-7)—Limits log messages saved to the switch's permanent flash memory for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be logged to flash. Note that the Flash Level must be equal to or less than the RAM Level. (Range: 0-7, Default: 3) R

Ram Level (0-7)—Limits log messages saved to the switch's temporary RAM memory for all levels up to the specified level. For example, if level 7 is specified, all messages from level 0 to level 7 will be logged to RAM. (Range: 0-7, Default: 7)

View Flash Logging—Click the button to display log messages stored in the switch's flash memory.



View Memory Logging—Click the button to display log messages stored in the switch's RAM memory.



Enable the System Log Status, set the level of event messages to be logged to RAM and flash memory, then click **Save Settings**.

Syslog

Allows you to configure the logging of messages that are sent to remote Syslog servers. You can limit the event messages sent to only those messages at or above a specified level.

Remote Log Status—Enables/disables the logging of debug or error messages to the remote logging process. (Default: Disabled)

Logging Facility—Sets the facility type for remote logging of Syslog messages. There are eight facility types specified by values of 16 to 23. The facility type is used by the Syslog server to dispatch log messages to an appropriate service. The attribute specifies the facility type tag sent in Syslog messages. (See RFC 3164.) This type has no effect on the kind of messages reported by the switch. However, it may be used by the Syslog server to process messages, such as sorting or storing messages in the corresponding database. (Range: 16-23, Default: 23)

Logging Trap—Limits log messages that are sent to the remote Syslog server for all levels up to the specified level. For example, if level 2 is specified, all messages from level 0 to level 2 will be sent to the remote server. (Range: 0-7, Default: 7)

Syslog Server—Displays the list of remote server IP addresses that will receive Syslog messages. The maximum number of host IP addresses allowed is five.

Enable Remote Log Status, set the Logging Facility type number, and configure the level of event messages to be sent to Syslog servers. Enter up to five Syslog server IP addresses in the server list. Click **Save Settings**.

SMTP Setting

To alert system administrators of problems, the switch can use SMTP (Simple Mail Transfer Protocol) to send email messages when triggered by logging events of a specified level. The messages are sent to specified SMTP servers on the network and can be retrieved using POP or IMAP clients.

Admin Status—Enables/disables the SMTP function. (Default: Enabled)

Severity—Sets the Syslog severity threshold level used to trigger alert messages. All events at this level or higher are sent to the configured email recipients. For example, using Level 6 will report all events from level6 to level 0. (Default: Level 7)

SMTP (1-3)—Specifies a list of up to three recipient SMTP server IP addresses. The switch attempts to connect to the other listed servers if the first fails.

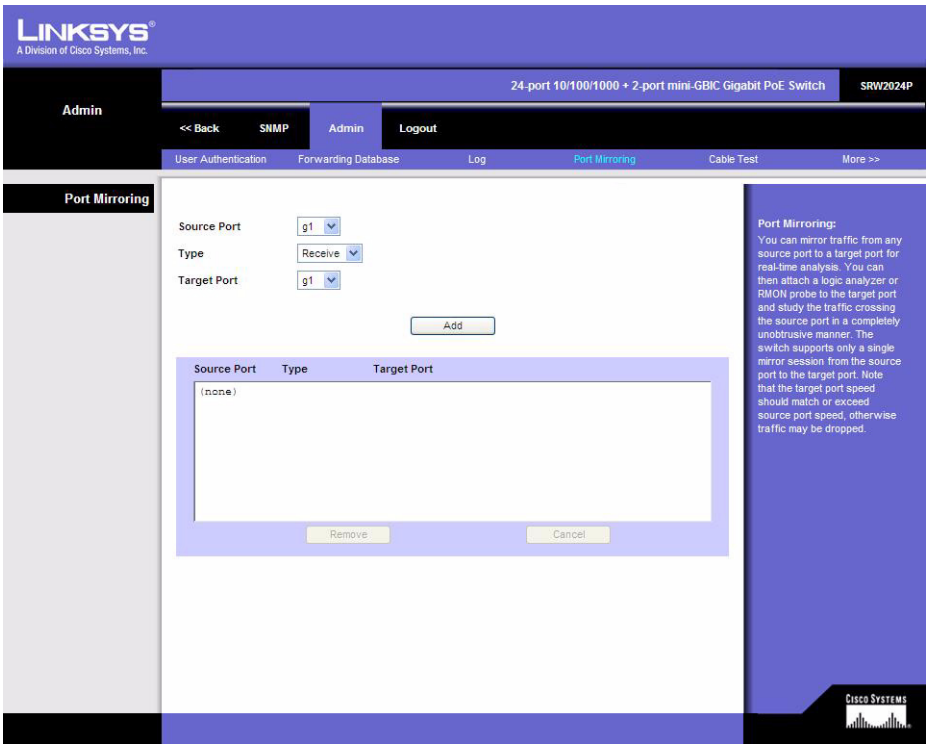
Source Email Address—Sets the email address used for the "From" field in alert messages. You may use a symbolic email address that identifies the switch, or the address of an administrator responsible for the switch.

Destination Email Address (1-5)—Specifies the email recipients of alert messages. You can specify up to five recipients.

Enable Admin Status, select the minimum severity level, and specify a source email address. Add at least one IP address to the SMTP server list and specify up to five email addresses to receive the alert messages. Click **Save Settings**.

Admin Tab - Port Mirroring

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.



The target port speed should match or exceed source port speed, otherwise traffic may be dropped from the monitor port. The switch supports only one mirror session. Set the following attributes for port mirroring using the Port Mirroring screen.

Source Port—Defines the port to which traffic is mirrored.

Type—Indicates the port mode configuration for port mirroring. The possible field values are:

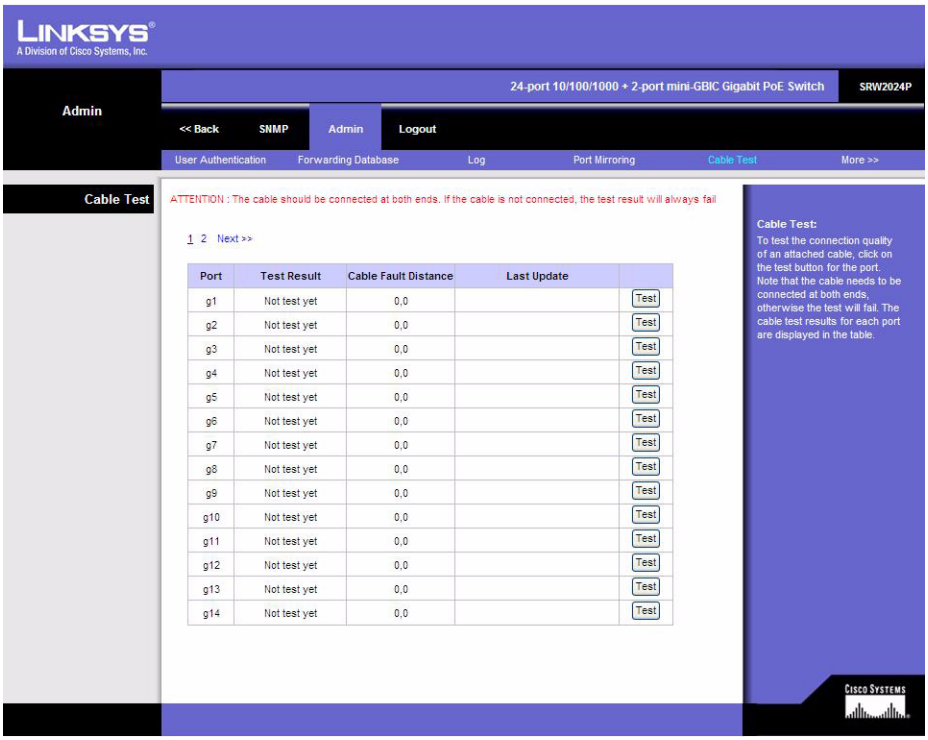
- **Receive**—Defines the port mirroring on receiving ports. This is the default value.
- **Transmit**—Defines the port mirroring on transmitting ports.
- **Both**—Defines the port mirroring on both receiving and transmitting ports.

Target Port—Defines the port from which traffic is mirrored.

Specify the source port, the traffic type to be mirrored, and the target port, then click **Add**. The mirror session is displayed in the text box.

Admin Tab - Cable Test

To test the connection quality of an attached cable, click on the **Test** button for the port. Note that the cable needs to be connected at both ends; otherwise the test will fail.



Port—This is the port to which the cable is connected.

Test Result—This is the test result. OK indicates that the cable passed the test. No Cable means there is no cable connected to the port. Open Cable means the cable is connected on only one side. Short Cable indicates that a short has occurred in the cable. Undefined indicates that the test could not be properly performed.

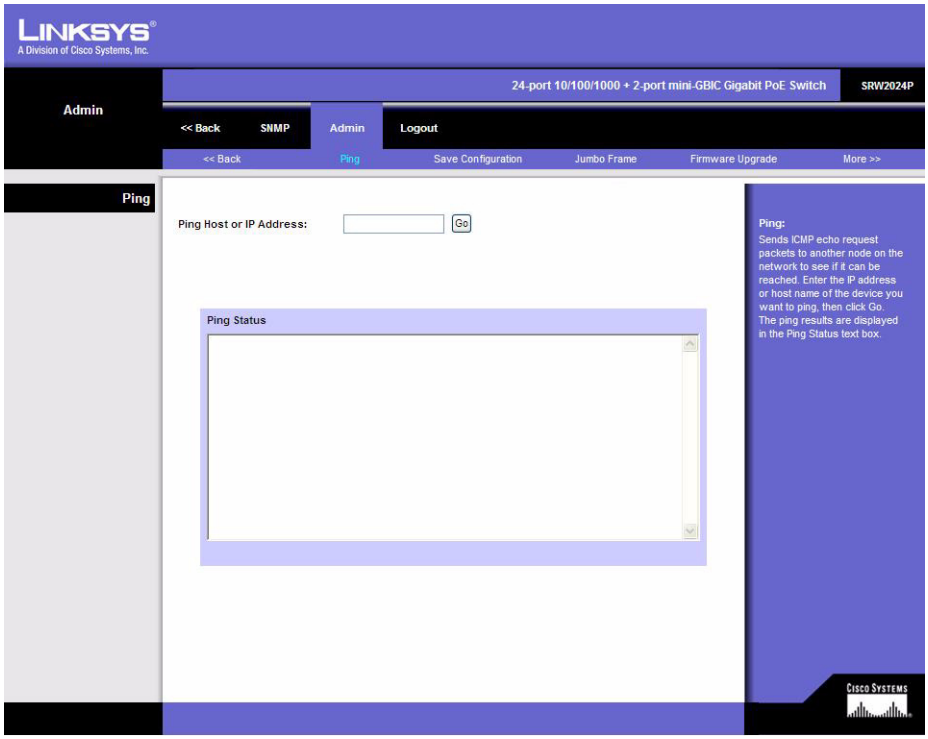
Cable Fault Distance—This is the distance from the port at which the cable error occurred.

Last Update—This is the last time the port was tested.

Test—Click the **Test** button to perform the test.

Admin Tab - Ping

You can use a ping to see if another site on the network can be reached. Ping sends ICMP echo request packets to another node on the network. Enter the IP address or host name of the device you want to ping, then click **Go**. The ping results are displayed in the Ping Status text box.

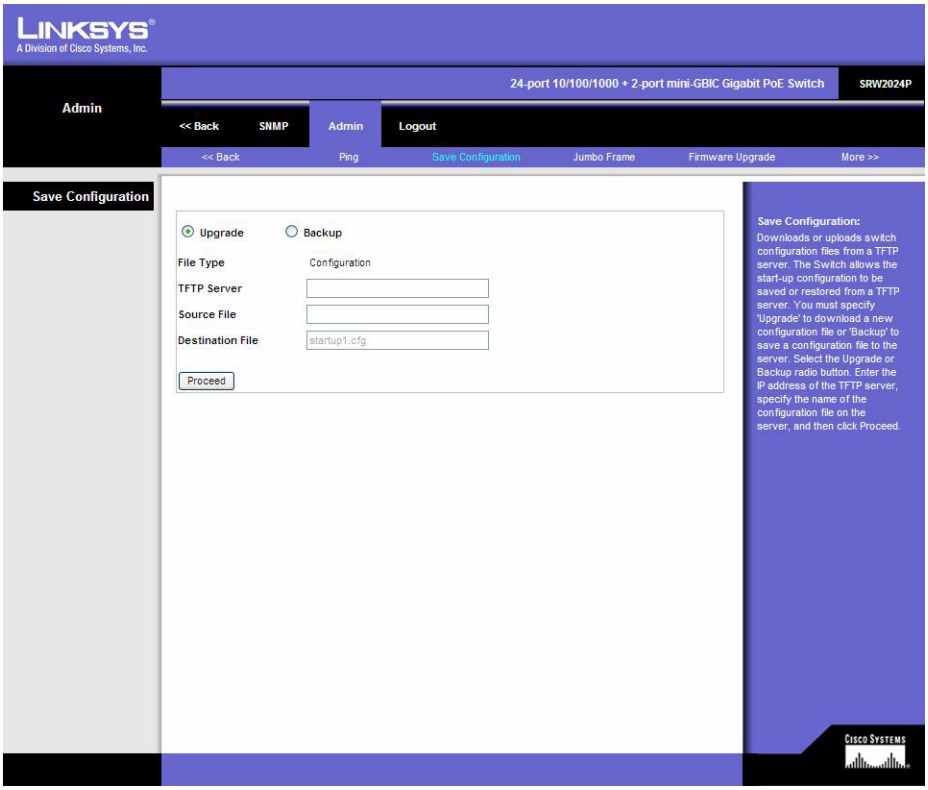


The following are some common displayed results of a ping:

- **Normal response**—The normal response occurs in one to ten seconds, depending on network traffic.
- **Destination does not respond**—If the host does not respond, a “timeout” appears in 10 seconds.
- **Destination unreachable**—The gateway for this destination indicates that the destination is unreachable.
- **Network or host unreachable**—The gateway found no corresponding entry in the route table

Admin Tab - Save Configuration

Downloads or uploads switch configuration files from a TFTP server. The switch allows the start-up configuration to be saved or restored from a TFTP server. You must specify “Upgrade” to download a new configuration file or “Backup” to save a configuration file to the server.

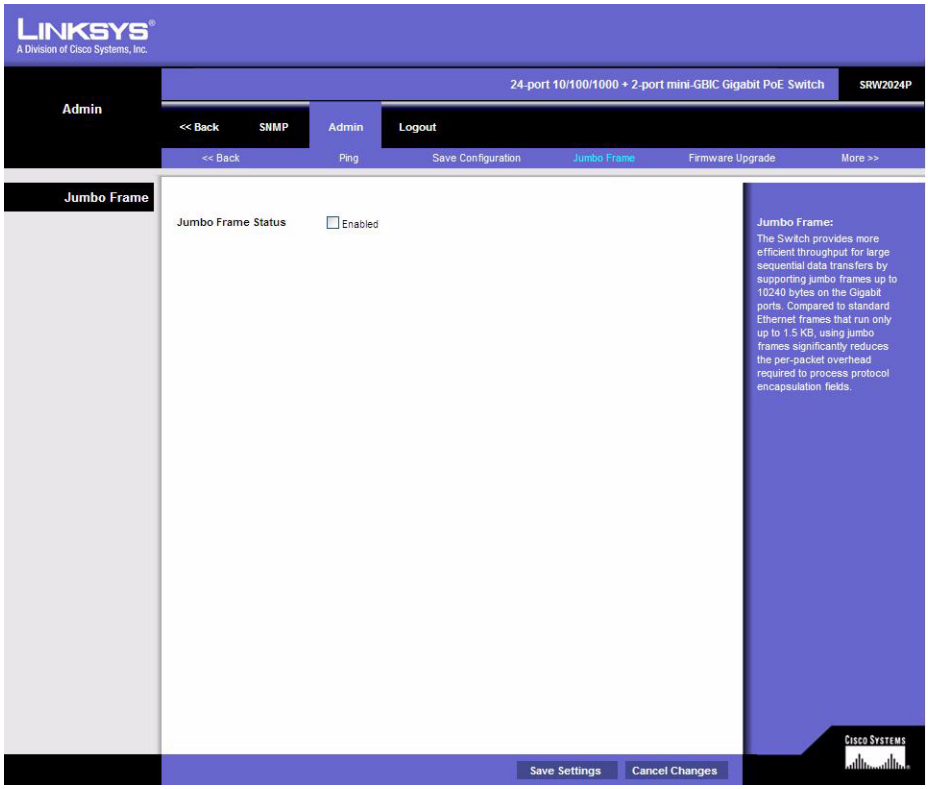


Select **Upgrade** or **Backup**. Enter the IP address of the TFTP server, specify the name of the configuration file on the server, and then click **Save Settings.**

Admin Tab - Jumbo Frame

The switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames up to 10240 bytes on the Gigabit ports and mini jumbo frames on the 10/100Mbps ports. Compared to standard Ethernet frames that run only up to 1.5 KB, using

jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.



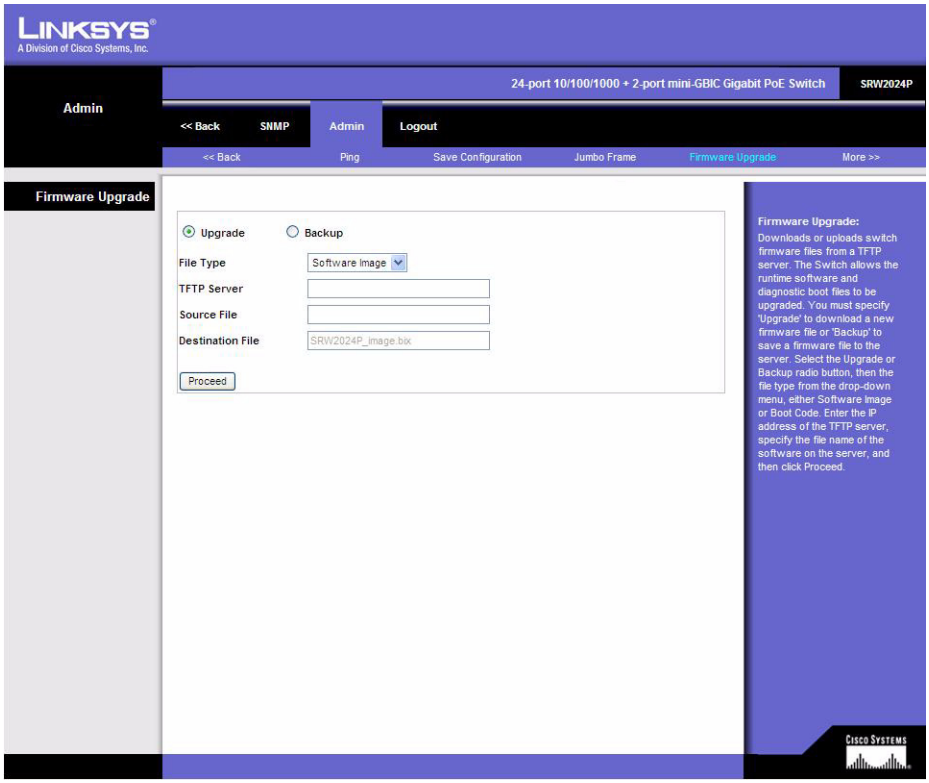
To use jumbo frames, both the source and destination end nodes (such as a computer or server) must support this feature. Also, when the connection is operating at full duplex, all switches in the network between the two end nodes must be able to accept the extended frame size. And for half-duplex connections, all devices in the collision domain would need to support jumbo frames.

Enabling jumbo frames limits the maximum threshold for broadcast storm control to 64 packets per second.

Admin Tab - Firmware Upgrade

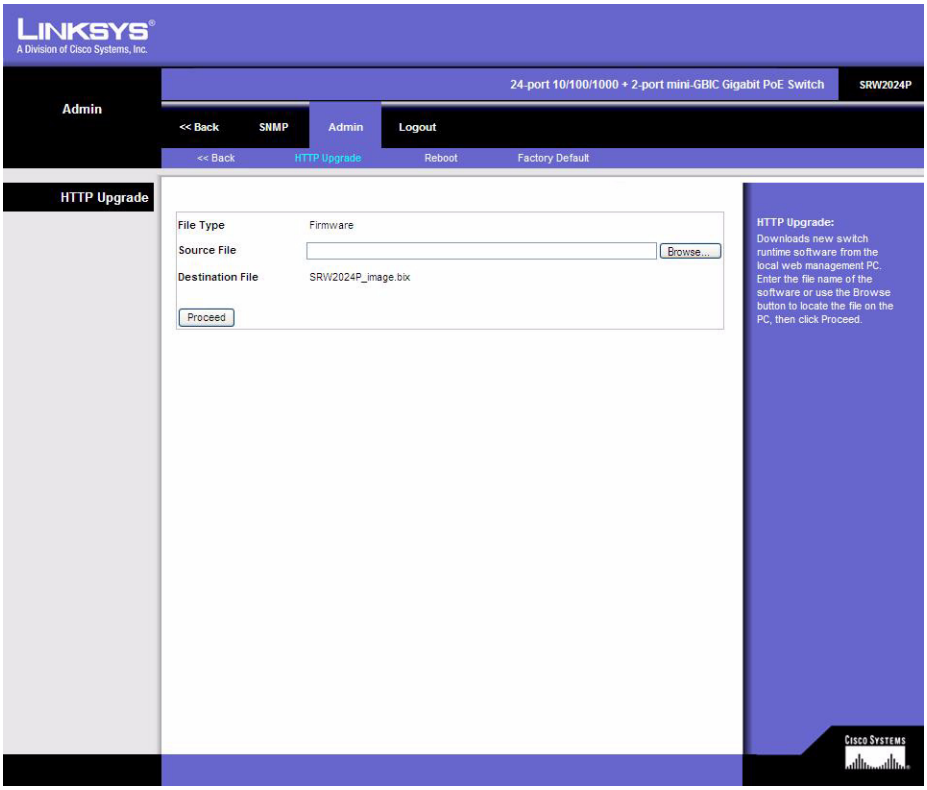
Go here to download or upload switch firmware files from a TFTP server. The switch allows the runtime software and diagnostic boot files to be upgraded. You must specify “Upgrade” to download a new firmware file or “Backup” to save a firmware file to the server. Select the **Upgrade** or **Backup** radio button, then the file type from the drop-down list, either Software

Image or Boot Code. Enter the IP address of the TFTP server, specify the file name of the software on the server, and then click **Save Settings**.



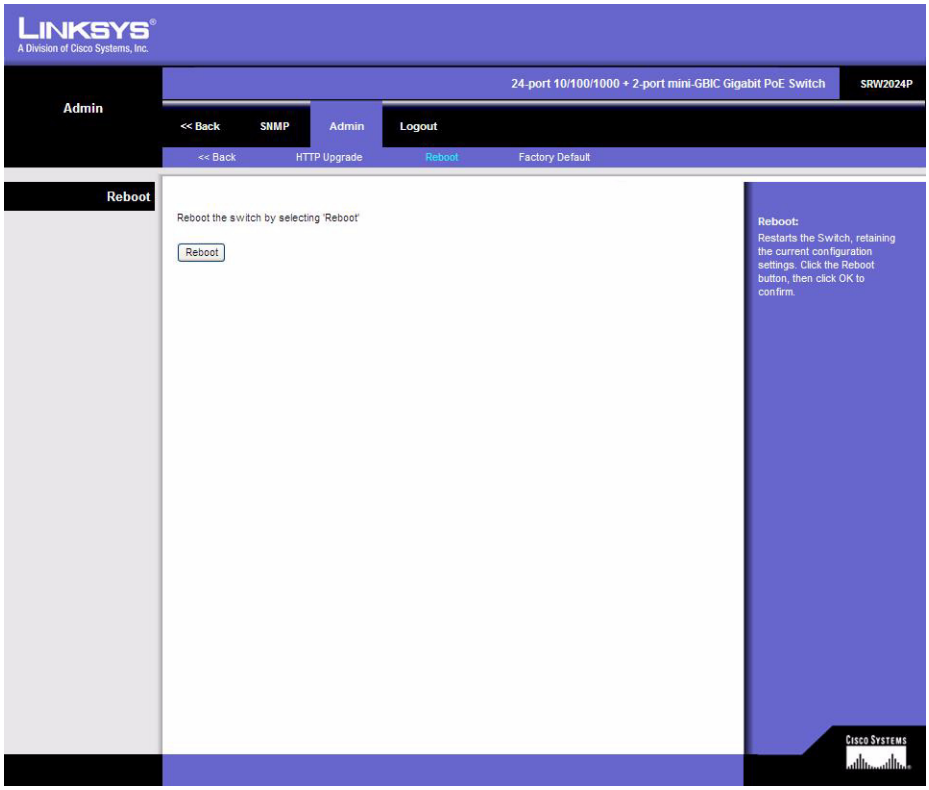
Admin Tab - HTTP Upgrade

Download new switch runtime software from the local web management PC. Enter the file name of the software or use the Browse button to locate the file on the PC, then click **Save Settings**.



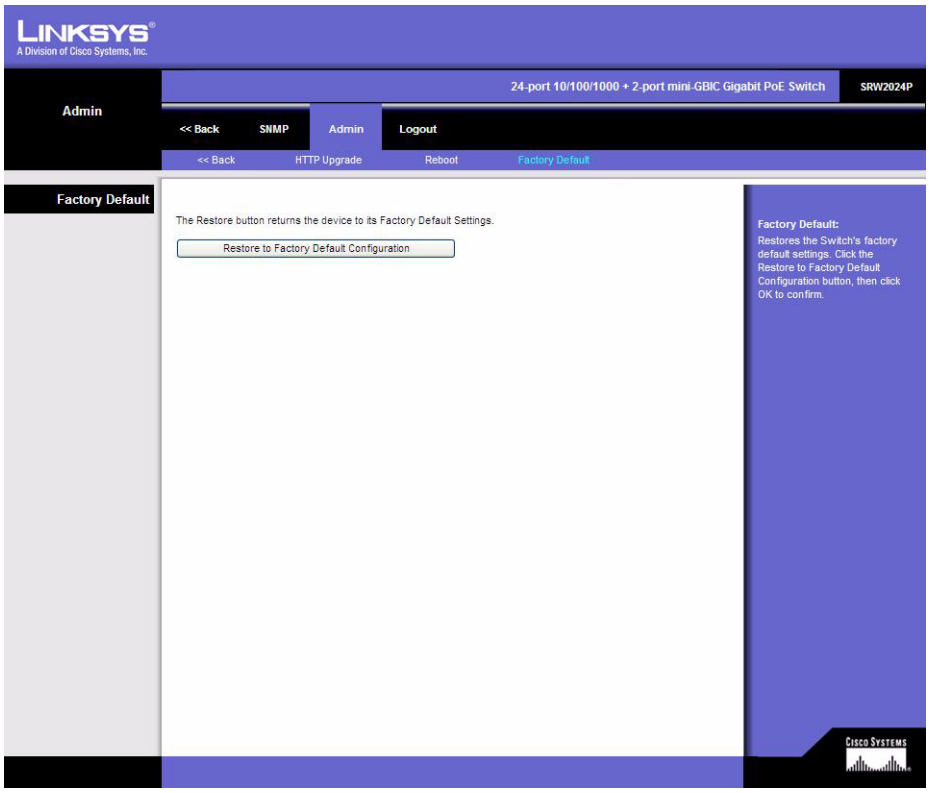
Admin Tab - Reboot

The *Reboot* screen resets the device. The device configuration is automatically saved before the device is rebooted.



Admin Tab - Factory Default

The *Factory Reset* screen restores the switch's factory default settings.



Click the **Reset to Factory Default Configuration** button, then click **OK** to confirm and restart the switch.

NOTE: Restoring the factory defaults will erase all configuration settings that you have made. You can save a backup of your current configuration settings from the Admin - Save Configuration screen.

Upon completion of modifying all of the configuration settings you need, be sure to log out of the web-based Interface.

About Gigabit Ethernet and Fiber Optic Cabling

Gigabit Ethernet

Gigabit Ethernet runs at speeds of 1Gbps (Gigabit per second), ten times faster than 100Mbps Fast Ethernet, but it still integrates seamlessly with 100Mbps Fast Ethernet hardware. Users can connect Gigabit Ethernet hardware with either fiber optic cabling or copper Category 5e cabling, with fiber optics more suited for network backbones. As the Gigabit standard gradually integrates into existing networks, current computer applications will enjoy faster access time for network data, hardware, and Internet connections.

Fiber Optic Cabling

Fiber optic cabling is made from flexible, optically efficient strands of glass and coated with a layer of rubber tubing, fiber optics use photons of light instead of electrons to send and receive data. Although fiber is physically capable of carrying terabits of data per second, the signaling hardware currently on the market can handle no more than a few gigabits of data per second.

Fiber cables come with two main connector types. The most commonly used fiber optic cable is multi-mode fiber cable (MMF), with a 62.5 micron fiber optic core. Single-mode fiber cabling is somewhat more efficient than multi-mode but far more expensive, due to its smaller optic core that helps retain the intensity of traveling light signals. A fiber connection always require two fiber cables: one transmits data, and the other receives it.

Each fiber optic cable is tipped with a connector that fits into a fiber port on a network adapter, hub, or switch. In the USA, most cables use a square SC connector that slides and locks into place when plugged into a port or connected to another cable. In Europe, the round ST connector is more prevalent.

You must use the Linksys MGBT1, MGBSX1, or MGBLH1 mini-GBIC modules with the Linksys Gigabit Switches. The MGBSX1 and the MGBLH1 require fiber cabling with LC connectors, and the MGBT1 requires a Category 5e Ethernet cable with an RJ-45 connector.

Windows Help

Almost all networking products require Microsoft Windows. Windows is the most used operating system in the world and comes with many features that help make networking easier. These features can be accessed through Windows Help and are described in this appendix.

TCP/IP

Before a computer can communicate within a network, TCP/IP must be enabled. TCP/IP is a set of instructions, or protocol, all PCs follow to communicate over a network. This is true for wireless networks as well. Your PCs will not be able to utilize wireless networking without having TCP/IP enabled. Windows Help provides complete instructions on enabling TCP/IP.

Shared Resources

If you wish to share printers, folder, or files over your network, Windows Help provides complete instructions on utilizing shared resources.

Network Neighborhood/My Network Places

Other PCs on your network appear under Network Neighborhood or My Network Places (depending upon the version of Windows you're running). Windows Help provides complete instructions on adding PCs to your network.

Downloading with Xmodem

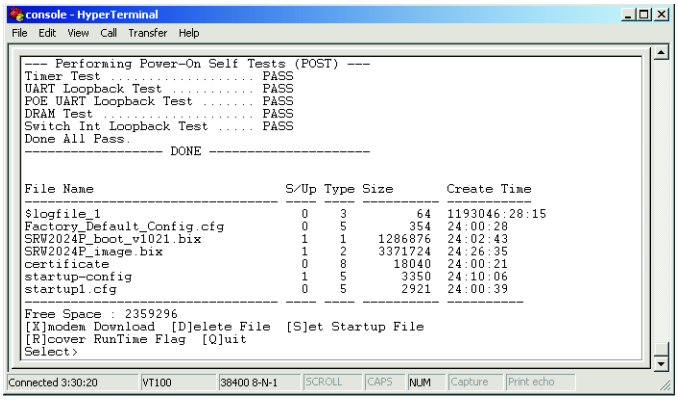
Startup Menu Procedures

The Startup menu can be entered when booting the device. There is a two-second window of time to enter the Startup Menu immediately after the POST test. The menu can be accessed directly from a terminal connected to the console port. The Startup menu procedures can be done using the ASCII terminal or Windows HyperTerminal.

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

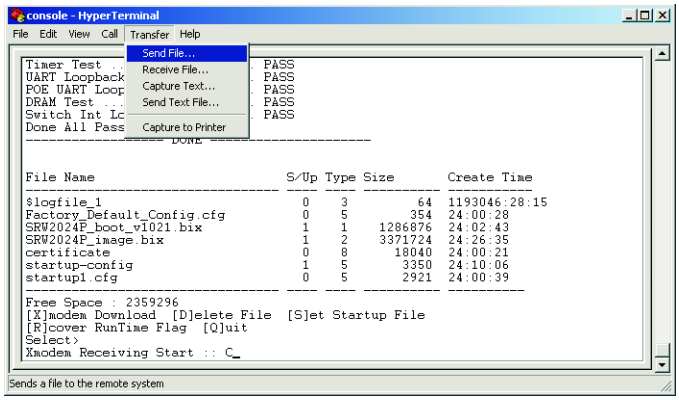
To enter the Startup menu:

1. Power off your computer and switch.
2. Connect the provided null modem cable from the COM port on your computer to the Console port on the switch.
3. Power on your computer and launch HyperTerminal, follow the instructions in Chapter 5, "Using the Console Interface for Configuration" to configure HyperTerminal to connect to the switch.



4. Power on the switch and watch for the POST done message: *Done All Pass*.
5. When the DONE message appears, press and hold **Ctrl-U** to access the Xmodem interface.
6. Check that the switch has sufficient flash memory space for the new code file before starting the download. You can store a maximum of only two runtime and two diagnostic code files in the switch's flash memory. Use the [D]elete File command to remove a runtime or diagnostic file.
7. Press **X** to start to download the new code file. If using Windows HyperTerminal, click the **Transfer** button, and then click **Send File**. Select the XModem Protocol and then use the **Browse** button to select the required firmware code file from your PC system. The *Xmodem*

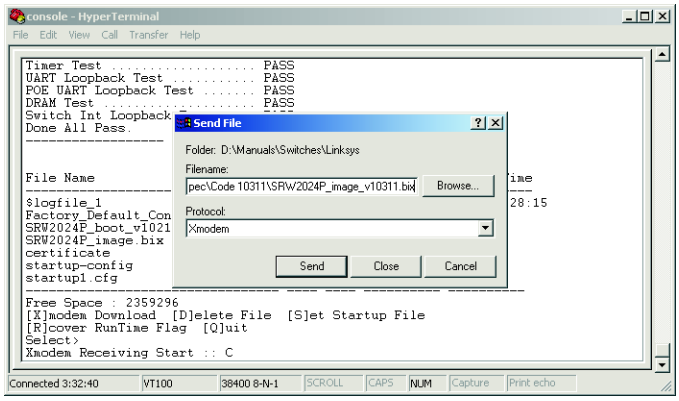
file send window displays the progress of the download procedure. Note: The download file must be a valid binary software file from Linksys for the target switch.



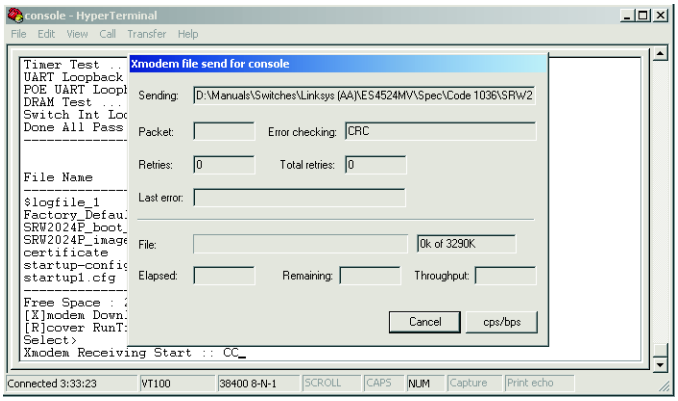
8. After the file has been downloaded, you are prompted with *Update Image File:* to specify the type of code file. Press **R** for runtime code, **D** for diagnostic code, or, **L** for loader code.

   Caution: If you select <L> for loader code, be sure the file is a valid loader code file for the switch. If you download an invalid file, the switch will not be able to boot. Unless absolutely necessary, do not attempt to download loader code files. Press **Send** and the software is downloaded.

9. Specify a name for the downloaded code file. File names are case-sensitive, should be from 1 to 31 characters, not contain slashes (\ or /), and the leading letter of the file name should not be a period (.). (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)



10. To set the new downloaded file as the startup file, use the [S]et Startup File menu option.



11. Press **Q** to quit the firmware-download mode and boot the switch.

    After quitting, the device reboots automatically.

Glossary

This glossary contains some basic networking terms you may come across when using this product. For more advanced terms, see the complete Linksys glossary at http://www.linksys.com/glossary.

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

Access Point - A device that allows wireless-equipped computers and other devices to communicate with a wired network. Also used to expand the range of a wireless network.

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

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

ACE - Filters in Access Control Lists (ACL) that determine which network traffic is forwarded. An ACE is based on the following criteria:

- Protocol
- Protocol ID
- Source Port
- Destination Port
- Wildcard Mask
- Source IP Address
- Destination IP Address

ACL (Access **C**ontrol **L**ist**)** - Access Control Lists are used to grant, deny, or limit access devices, features, or applications.

Auto-negotiation - Allows 10/100 Mbps or 10/100/1000 Mbps Ethernet ports to automatically establish the optimal duplex mode, flow control, and speed.

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

Bandwidth - The transmission capacity of a given device or network.

Bandwidth Assignments - Indicates the amount of bandwidth assigned to a specific application, user, and/or interface.

Baud - Indicates the number of signaling elements transmitted each second.

Best Effort - Indicates that traffic is assigned to the lowest priority queue, and packet delivery is not guaranteed.

Bit - A binary digit.

Boot - To start a device and cause it to start executing instructions.

Browser - An application program that provides a way to look at and interact with all the information on the World Wide web.

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

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

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

Burst - A packet transmission at faster than normal rates. Bursts are limited in time and only occur under specific conditions.

Byte - A unit of data that is usually eight bits long

Cable Modem - A device that connects a computer to the cable television network, which in turn connects to the Internet.

CBS (**C**ommitted **B**urst **S**ize) - The maximum number of data bits transmitted within a specific time interval.

CIR (**C**ommitted **I**nformation **R**ate) - The data rate is averaged over a minimum time increment.

Class Maps - An aspect of Quality of Service system that is comprised of an IP ACL and/or a MAC ACL. Class maps are configured to match packet criteria, and are matched to packets in a first-fit fashion.

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

Communities - A group of users that have the same system access rights.

CoS (**C**lass **o**f **S**ervice) - The 802.1p priority scheme. CoS provides a method for tagging packets with priority information. A CoS value between 0-7 is added to the Layer II header of packets, where zero is the lowest priority and seven is the highest.

DDNS (**D**ynamic **D**omain **N**ame **S**ystem) - Allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (e.g., www.xyz.com) and a dynamic IP address.

Default Gateway - A device that forwards Internet traffic from your local area network.

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) - A networking protocol that allows administrators to assign temporary IP addresses to network computers by "leasing" an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

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

DHCP Server - An Internet host that returns configuration parameters to DHCP clients.

DNS (**D**omain **N**ame **S**erver) - The IP address of your ISP's server, which translates the names of websites into IP addresses.

Domain - A specific name for a network of computers.

Download - To receive a file transmitted over a network.

DSL (**D**igital **S**ubscriber **L**ine) - An always-on broadband connection over traditional phone lines.

DSCP (**D**iff**S**erve **C**ode **P**oint) provides a method of tagging IP packets with QoS priority information.

Dynamic IP Address - A temporary IP address assigned by a DHCP server.

EIGRP (**E**nhanced **I**nterior **G**ateway **R**outing **P**rotocol) - Provides fast convergence, support for variable-length subnet mask, and supports multiple network layer protocols.

Encryption - Encoding data transmitted in a network.

Ethernet - IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium.

Firmware - The programming code that runs a networking device.

Flow Control - Enables lower speed devices to communicate with higher speed devices. This feature is implemented by the higher speed device refraining from sending packets.

FTP (**F**ile **T**ransfer **P**rotocol) - A protocol used to transfer files over a TCP/IP network.

Full Duplex - The ability of a networking device to receive and transmit data simultaneously.

GARP (**G**eneral **A**ttributes **R**egistration **P**rotocol) - Registers client stations into a multicast domain.

Gateway - A device that interconnects networks with different, incompatible communications protocols.

GBIC (**G**iga**B**it **I**nterface **C**onverter) - A hardware module used to attach network devices to fiber-based transmission systems. GBIC converts the serial electrical signals to serial optical signals and vice versa.

GVRP (**G**ARP **V**LAN **R**egistration **P**rotocol) - Registers client stations into a VLANs.

Half Duplex - Data transmission that can occur in two directions over a single line, but only one direction at a time.

HTTP (**H**yper**T**ext **T**ransport **P**rotocol) - The communications protocol used to connect to servers on the World Wide web.

HTTPS (**H**yper**T**ext **T**ransport **P**rotocol **S**ecure) - An extension to the standard HTTP protocol that provides confidentiality by encrypting the traffic from the website. By default this protocol uses TCP port 443.

ICMP (Internet **C**ontrol **M**essage **P**rotocol) - Allows the gateway or destination host to communicate with the source host. For example, to report a processing error.

IGMP (**I**nternet **G**roup **M**anagement **P**rotocol) - Allows hosts to notify their local switch or router that they want to receive transmissions assigned to a specific multicast group.

IP (**I**nternet **P**rotocol) - A protocol used to send data over a network.

IP Address - The address used to identify a computer or device on a network.

IPCONFIG - A Windows 2000 and XP utility that displays the IP address for a particular networking device.

IPSec (**I**nternet **P**rotocol **Sec**urity) - A VPN protocol used to implement secure exchange of packets at the IP layer.

ISP (**I**nternet **S**ervice **P**rovider) - A company that provides access to the Internet.

Jumbo Frames - Enable transporting identical data in fewer frames. Jumbo Frames reduce overhead, lower processing time, and ensure fewer interrupts.

LAG (**L**ink **A**ggregated **G**roup) - Aggregates ports or VLANs into a single virtual port or VLAN.

LAN - The computers and networking products that make up your local network.

MAC (**M**edia **A**ccess **C**ontrol) **Address** - The unique address that a manufacturer assigns to each networking device.

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

Mbps (**M**ega**B**its **P**er **S**econd) - One million bits per second; a unit of measurement for data transmission.

MD5 (**M**essage **D**igest **5**) - An algorithm that produces a 128-bit hash. MD5 is a variation of MD4, and increases MD4 security. MD5 verifies the integrity of the communication and authenticates the origin of the communication.

MDI (**M**edia **D**ependent **I**nterface) A cable used for end stations.

MDIX (**M**edia **D**ependent **I**nterface with Crossover) - A cable used for hubs and switches.

MIB (**M**anagement **I**nformation **B**ase) - MIBs contain information describing specific aspects of network components.

Multicast - Transmits copies of a single packet to multiple ports.

Network - A series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users.

NMS (**N**etwork **M**anagement **S**ystem) - An interface that provides a method of managing a system.

OID (**O**bject **Id**entifier) - Used by SNMP to identify managed objects. In the SNMP Manager/Agent network management paradigm, each managed object must have an OID to identify it.

Packet - A unit of data sent over a network.

Ping (**P**acket **IN**ternet **G**roper) - An Internet utility used to determine whether a particular IP address is online.

Policing - Determines if traffic levels are within a specified profile. Policing manages the maximum traffic rate used to send or receive packets on an interface.

Port - The connection point on a computer or networking device used for plugging in cables or adapters.

Port Mirroring - Monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from one port to a monitoring port.

Power **o**ver **E**thernet (**PoE**) - A technology enabling an Ethernet network cable to deliver both data and power.

QoS (**Q**uality **o**f **S**ervice) -Provides policies that contain sets of filters (rules). QoS allows network managers to decide how and what network traffic is forwarded according to priorities, application types, and source and destination addresses.

RADIUS (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice) - A protocol that uses an authentication server to control network access.

RJ-45 (**R**egistered **J**ack-**45**) - An Ethernet connector that holds up to eight wires.

RMON (**R**emote **Mon**itoring) - Provides network information to be collected from a single workstation.

Router - A networking device that connects multiple networks together.

RSTP (**R**apid **S**panning **T**ree **P**rotocol) - Detects and uses network topologies that allow a faster convergence of the spanning tree, without creating forwarding loops.

Server - Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

SMTP (**S**imple **M**ail **T**ransfer **P**rotocol) - The standard e-mail protocol on the Internet.

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) - A widely used network monitoring and control protocol.

SSH - Secure Shell. A utility that uses strong authentication and secure communications to log in to another computer over a network.

SSL (**S**ecure **S**ocket **L**ayer) - Encryption technology for the Internet used to provide secure transactions, such as the transmission of credit card numbers for e-commerce.

Static IP Address - A fixed address assigned to a computer or device that is connected to a network.

STP (**S**panning **T**ree **P**rotocol) - Prevents loops in network traffic. The Spanning Tree Protocol (STP) provides tree topography for any arrangement of bridges. STP provides one path between end stations on a network, eliminating loops.

Subnet (**Sub**-**net**work) - Subnets are portions of a network that share a common address component. In TCP/IP networks, devices that share a prefix are part of the same subnet. For example, all devices with a prefix of 157.100.100.100 are part of the same subnet.

Subnet Mask - An address code that determines the size of the network.

Switch - Filters and forwards packets between LAN segments. Switches support any packet protocol type.

TACACS+ (**T**erminal **A**ccess **C**ontroller **A**ccess **C**ontrol **S**ystem **Plus**) - Proprietary Cisco enhancement to Terminal Access Controller Access Control System (TACACS). Provides additional support for authentication, authorization, and accounting.

TCP (**T**ransmission **C**ontrol **P**rotocol) - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) - A set of instructions PCs use to communicate over a network.

Telnet - A user command and TCP/IP protocol used for accessing remote PCs.

TFTP (**T**rivial **F**ile **T**ransfer **P**rotocol) - A version of the TCP/IP FTP protocol that has no directory or password capability.

Throughput - The amount of data moved successfully from one node to another in a given time period.

Trunking - Link Aggregation. Optimizes port usage by linking a group of ports together to form a single trunk (aggregated groups).

TX Rate - Transmission Rate.

UDP (**U**ser **D**ata **P**rotocol) - Communication protocol that transmits packets but does not guarantee their delivery.

Upgrade - To replace existing software or firmware with a newer version.

Upload - To transmit a file over a network.

URL (**U**niform **R**esource **L**ocator) - The address of a file located on the Internet.

VLAN (**V**irtual **L**ocal **A**rea **N**etworks) - Logical subgroups that constitute a Local Area Network (LAN). This is done in software rather than defining a hardware solution.

WAN (**W**ide **A**rea **N**etwork) - Networks that cover a large geographical area.

Wildcard Mask - Specifies which IP address bits are used, and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all the bits are important. For example, if the destination IP address is 149.36.184.198 and the wildcard mask is 255.36.184.00, the first two bits of the IP address are used, while the last two bits are ignored.

Warranty Information

LIMITED WARRANTY

Linksys warrants this Linksys hardware product against defects in materials and workmanship under normal use for the Warranty Period, which begins on the date of purchase by the original end-user purchaser and lasts for the period specified for this product at www.linksys.com/warranty. The internet URL address and the web pages referred to herein may be updated by Linksys from time to time; the version in effect at the date of purchase shall apply.

This limited warranty is non-transferable and extends only to the original end-user purchaser. Your exclusive remedy and Linksys entire liability under this limited warranty will be for Linksys, at its option, to (a) repair the product with new or refurbished parts, (b) replace the product with a reasonably available equivalent new or refurbished Linksys product, or (c) refund the purchase price of the product less any rebates. Any repaired or replacement products will be warranted for the remainder of the original Warranty Period or thirty (30) days, whichever is longer. All products and parts that are replaced become the property of Linksys.

Exclusions and Limitations

This limited warranty does not apply if: (a) the product assembly seal has been removed or damaged, (b) the product has been altered or modified, except by Linksys, (c) the product damage was caused by use with non.Linksys products, (d) the product has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Linksys, (e) the product has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident, (f) the serial number on the Product has been altered, defaced, or removed, or (g) the product is supplied or licensed for beta, evaluation, testing or demonstration purposes for which Linksys does not charge a purchase price or license fee.

ALL SOFTWARE PROVIDED BY LINKSYS WITH THE PRODUCT, WHETHER FACTORY LOADED ON THE PRODUCT OR CONTAINED ON MEDIA ACCOMPANYING THE PRODUCT, IS PROVIDED AS IS WITHOUT WARRANTY OF ANY KIND. Without limiting the foregoing, Linksys does not warrant that the operation of the product or software will be uninterrupted or error free. Also, due to the continual development of new techniques for intruding upon and attacking networks, Linksys does not warrant that the product, software or any equipment, system or network on which the product or software is used will be free of vulnerability to intrusion or attack. The product may include or be bundled with third party software or service offerings. This limited warranty shall not apply to such third party software or service offerings. This limited warranty does not guarantee any continued availability of a third party's service for which this product's use or operation may require.

TO THE EXTENT NOT PROHIBITED BY LAW, ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY OR FITNESS FOR A PARTICULAR PURPOSE ARE LIMITED TO THE DURATION OF THE WARRANTY PERIOD. ALL OTHER EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF NON-INFRINGEMENT, ARE DISCLAIMED. Some jurisdictions do not allow limitations on how long an implied warranty lasts, so the above limitation may not apply to you. This limited warranty gives you specific legal rights, and you may also have other rights which vary by jurisdiction.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL LINKSYS BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, REGARDLESS OF THE THEORY OF LIABILITY (INCLUDING NEGLIGENCE), ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE PRODUCT (INCLUDING ANY SOFTWARE), EVEN IF LINKSYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL LINKSYS' LIABILITY EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT. The foregoing limitations will apply even if any warranty or remedy provided under this limited warranty fails of its essential purpose. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Obtaining Warranty Service

If you have a question about your product or experience a problem with it, please go to www.linksys.com/support where you will find a variety of online support tools and information to assist you with your product. If the product proves defective during the Warranty Period, contact the Value Added Reseller (VAR) from whom you purchased the product or Linksys Technical Support for instructions on how to obtain warranty service. The telephone number for Linksys Technical Support in your area can be found in the product User Guide and at www.linksys.com. Have your product serial number and proof of purchase on hand when calling. A DATED PROOF OF ORIGINAL PURCHASE IS REQUIRED TO PROCESS WARRANTY CLAIMS. If you are requested to return your product, you will be given a Return Materials Authorization (RMA) number. You are responsible for properly packaging and shipping your product to Linksys at your cost and risk. You must include the RMA number and a copy of your dated proof of original purchase when returning your product. Products received without a RMA number and dated proof of original purchase will be rejected. Do not include any other items with the product you are returning to Linksys. Defective product covered by this limited warranty will be repaired or replaced and returned to you without charge. Customers outside of the United States of America and Canada are responsible for all shipping and handling charges, custom duties, VAT and other associated taxes and charges. Repairs or replacements not covered under this limited warranty will be subject to charge at Linksys' then-current rates.

Technical Support

This limited warranty is neither a service nor a support contract. Information about Linksys' current technical support offerings and policies (including any fees for support services) can be found at: www.linksys.com/support. This limited warranty is governed by the laws of the jurisdiction in which the Product was purchased by you. Please direct all inquiries to: Linksys, P.O. Box 18558, Irvine, CA 92623

Regulatory Information

FCC Statement

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution

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

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. To maintain compliance with FCC RF exposure compliance requirements, please avoid direct contact to the transmitting antenna during transmitting.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

We declare that the product is limited in CH1~CH11 by specified firmware controlled in the USA.

Generic Discussion on RF Exposure

The Cisco products are designed to comply with the following national and international standards on Human Exposure to Radio Frequencies.

US 47 Code of Federal Regulations Part 2 Subpart J

American National Standards Institute (ANSI) / Institute of Electrical and Electronic Engineers / IEEE C 95.1 (92)

International Commission on Non Ionizing Radiation Protection (ICNIRP) 98

Ministry of Health (Canada) Safety Code 6. Limits on Human Exposure to Radio Frequency Fields in the range from 3kHz to 300 GHz

Australia Radiation Protection Standard

To ensure compliance with various national and international Electromagnetic Field (EMF) standards, the system should only be operated with Cisco approved antennas and accessories.

US

This system has been evaluated for RF exposure for Humans in reference to ANSI C 95.1 (American National Standards Institute) limits. The evaluation was based on evaluation per ANI C 95.1 and FCC OET Bulletin 65C rev 01.01. The minimum separation distance from the antenna to general bystander is 7.9 inches (20cm) to maintain compliance.

Canada

This system has been evaluated for RF exposure for Humans in reference to ANSI C 95.1 (American National Standards Institute) limits. The evaluation was based on evaluation per RSS-102 Rev 2. The minimum separation distance from the antenna to general bystander is 7.9 inches (20cm) to maintain compliance.

EU

This system has been evaluated for RF exposure for Humans in reference to the ICNIRP (International Commission on Non-Ionizing Radiation Protection) limits. The evaluation was based on the EN 50385 Product Standard to Demonstrate Compliance of Radio Base stations and Fixed Terminals for Wireless Telecommunications Systems with basic restrictions or reference levels related to Human Exposure to Radio Frequency Electromagnetic Fields from 300 MHz to 40 GHz. The minimum separation distance from the antenna to general bystander is 20cm (7.9 inches).

Australia

This system has been evaluated for RF exposure for Humans as referenced in the Australian Radiation Protection standard and has been evaluated to the ICNIRP (International Commission on Non-Ionizing Radiation Protection) limits. The minimum separation distance from the antenna to general bystander is 20cm (7.9 inches).

ANSI C 95.1 (99)

This system has been evaluated for RF exposure for Humans in reference to the ANSI (American National Standards Institute) limits as referenced in C 95.1 (99). The minimum separation distance from the antenna to the user is 7.9 inches (20cm).

ICNIRP Limits

This system has been evaluated for RF exposure for Humans in reference to the ICNIRP (International Commission on Non-Ionizing Radiation Protection) limits. The minimum separation distance from the antenna to the user is 20cm (7.9 inches).

Explosive Environment, Medical and FAA Device Information

Use on Board Aircraft

The use of wireless on board aircraft is restricted by certain regulations and airline policy. Unless otherwise instructed by the airlines wireless devices should be turned off while on board aircraft.

Interference to Implanted Medical Devices

A minimum separation distance of 6 inches (15cm) is recommended between portable devices and implanted pacemakers to avoid possible interference. Please consult your physician or medical device maker for further details.

Medical Device use

Cisco products unless otherwise specified are not registered or listed as a FDA medical device. Therefore specific use in some unique medical applications may require additional approvals. Please contact your Cisco sales person for further details

Safety Notices

Do not use this product near water, for example, in a wet basement or near a swimming pool.

Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightning.

Industry Canada (Canada)

Operation is subject to the following two conditions:

1. This device may not cause interference and

2. This device must accept any interference, including interference that may cause undesired operation of the device.

This device has been designed to operate with an antenna having a maximum gain of 3.3 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

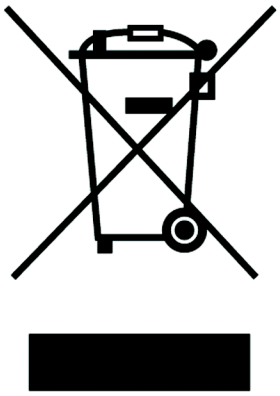
This device complies with Canadian ICES-003 and RSS210 rules.

Cet appareil est conforme aux normes NMB-003 et RSS210 d'Industry Canada.

User Information for Consumer Products Covered by EU Directive 2002/96/EC on Waste Electric and Electronic Equipment (WEEE)

WARNING: Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.

This document contains important information for users with regards to the proper disposal and recycling of Linksys products. Consumers are required to comply with this notice for all electronic products bearing the following symbol:



English

Environmental Information for Customers in the European Union

European Directive 2002/96/EC requires that the equipment bearing this symbol on the product and/or its packaging must not be disposed of with unsorted municipal waste. The symbol indicates that this product should be disposed of separately from regular household waste streams. It is your responsibility to dispose of this and other electric and electronic equipment via designated collection facilities appointed by the government or local authorities. Correct disposal and recycling will help prevent potential negative consequences to the environment and human health. For more detailed information about the disposal of your old equipment, please contact your local authorities, waste disposal service, or the shop where you purchased the product.

Ceština/Czech

Informace o ochraně životního prostředí pro zákazníky v zemích Evropské unie

Evropská směrnice 2002/96/ES zakazuje, aby zařízení označené tímto symbolem na produktu anebo na obalu bylo likvidováno s netříděným komunálním odpadem. Tento symbol udává, že daný produkt musí být likvidován odděleně od běžného komunálního odpadu. Odpovídáte za likvidaci tohoto produktu a dalších elektrických a elektronických zařízení prostřednictvím určených sběrných míst stanovených vládou nebo místními úřady. Správná likvidace a recyklace pomáhá předcházet potenciálním negativním dopadům na životní prostředí a lidské zdraví. Podrobnější informace o likvidaci starého vybavení si laskavě vyžádejte od místních úřadů, podniku zabývajícího se likvidací komunálních odpadů nebo obchodu, kde jste produkt zakoupili.

Dansk/Danish

Miljøinformation for kunder i EU

EU-direktiv 2002/96/EF kræver, at udstyr der bærer dette symbol på produktet og/eller emballagen ikke må bortskaffes som usorteret kommunalt affald. Symbolet betyder, at dette produkt skal bortskaffes adskilt fra det almindelige husholdningsaffald. Det er dit ansvar at bortskaffe dette og andet elektrisk og elektronisk udstyr via bestemte indsamlingssteder udpeget af staten eller de lokale myndigheder. Korrekt bortskaffelse og genvinding vil hjælpe med til at undgå mulige skader for miljøet og menneskers sundhed. Kontakt venligst de lokale myndigheder, renovationstjenesten eller den butik, hvor du har købt produktet, angående mere detaljeret information om bortskaffelse af dit gamle udstyr.

Nederlands/Dutch

Milieu-informatie voor klanten in de Europese Unie

De Europese Richtlijn 2002/96/EC schrijft voor dat apparatuur die is voorzien van dit symbool op het product of de verpakking, niet mag worden ingezameld met niet-gescheiden huishoudelijk afval. Dit symbool geeft aan dat het product apart moet worden ingezameld. U bent zelf verantwoordelijk voor de vernietiging van deze en andere elektrische en elektronische apparatuur via de daarvoor door de landelijke of plaatselijke overheid aangewezen inzamelingskanalen. De juiste vernietiging en recycling van deze apparatuur voorkomt mogelijke negatieve gevolgen voor het milieu en de gezondheid. Voor meer informatie over het vernietigen van uw oude apparatuur neemt u contact op met de plaatselijke autoriteiten of afvalverwerkingsdienst, of met de winkel waar u het product hebt aangeschaft.

Eesti/Estonian

Keskkonnaalane informatsioon Euroopa Liidus asuvatele klientidele

Euroopa Liidu direktiivi 2002/96/EÜ nõuete kohaselt on seadmeid, millel on tootel või pakendil käesolev sümbol, keelatud kõrvaldada koos sorteerimata olmejäätmetega. See sümbol näitab, et toode tuleks kõrvaldada eraldi tavalistest olmejäätmevoogudest. Olete kohustatud kõrvaldama käesoleva ja ka muud elektri- ja elektroonikaseadmed riigi või kohalike ametiasutuste poolt ette nähtud kogumispunktide kaudu. Seadmete korrektne kõrvaldamine ja ringlussevõtt aitab vältida võimalikke negatiivseid tagajärgi keskkonnale ning inimeste tervisele. Vanade seadmete kõrvaldamise kohta täpsema informatsiooni saamiseks võtke palun ühendust kohalike ametiasutustega, jäätmekäitlusfirmaga või kauplusega, kust te toote ostsite.

Suomi/Finnish

Ympäristöä koskevia tietoja EU-alueen asiakkaille

EU-direktiivi 2002/96/EY edellyttää, että jos laitteistossa on tämä symboli itse tuotteessa ja/tai sen pakkauksessa, laitteistoa ei saa hävittää lajittelemattoman yhdyskuntajätteen mukana. Symboli merkitsee sitä, että tämä tuote on hävitettävä erillään tavallisesta kotitalousjätteestä. Sinun vastuullasi on hävittää tämä elektroniikkatuote ja muut vastaavat elektroniikkatuotteet viemällä tuote tai tuotteet viranomaisten määräämään keräyspisteeseen. Laitteiston oikea hävittäminen estää mahdolliset kielteiset vaikutukset ympäristöön ja ihmisten terveyteen. Lisätietoja vanhan laitteiston oikeasta hävitystavasta saa paikallisilta viranomaisilta, jätteenhävityspalvelusta tai siitä myymälästä, josta ostit tuotteen.

Français/French

Informations environnementales pour les clients de l'Union européenne

La directive européenne 2002/96/CE exige que l'équipement sur lequel est apposé ce symbole sur le produit et/ou son emballage ne soit pas jeté avec les autres ordures ménagères. Ce symbole indique que le produit doit être éliminé dans un circuit distinct de celui pour les déchets des ménages. Il est de votre responsabilité de jeter ce matériel ainsi que tout autre matériel électrique ou électronique par les moyens de collecte indiqués par le gouvernement et les pouvoirs publics des collectivités territoriales. L'élimination et le recyclage en bonne et due forme ont pour but de lutter contre l'impact néfaste potentiel de ce type de produits sur l'environnement et la santé publique. Pour plus d'informations sur le mode d'élimination de votre ancien équipement, veuillez prendre contact avec les pouvoirs publics locaux, le service de traitement des déchets, ou l'endroit où vous avez acheté le produit.

Deutsch/German

Umweltinformation für Kunden innerhalb der Europäischen Union

Die Europäische Richtlinie 2002/96/EC verlangt, dass technische Ausrüstung, die direkt am Gerät und/oder an der Verpackung mit diesem Symbol versehen ist nicht zusammen mit unsortiertem Gemeindeabfall entsorgt werden darf. Das Symbol weist darauf hin, dass das Produkt von regulärem Haushaltmüll getrennt entsorgt werden sollte. Es liegt in Ihrer Verantwortung, dieses Gerät und andere elektrische und elektronische Geräte über die dafür zuständigen und von der Regierung oder örtlichen Behörden dazu bestimmten Sammelstellen zu entsorgen. Ordnungsgemäßes Entsorgen und Recyceln trägt dazu bei, potentielle negative Folgen für Umwelt und die menschliche Gesundheit zu vermeiden. Wenn Sie weitere Informationen zur Entsorgung Ihrer Altgeräte benötigen, wenden Sie sich bitte an die örtlichen Behörden oder städtischen Entsorgungsdienste oder an den Händler, bei dem Sie das Produkt erworben haben.

Ξλληνικά/Greek

Στοιχεία περιβαλλοντικής προστασίας για πελάτες εντός της Ευρωπαϊκής Ένωσης

Η Κοινοτική Οδηγία 2002/96/EC απαιτεί ότι ο εξοπλισμός ο οποίος φέρει αυτό το σύμβολο στο προϊόν και/ή στη συσκευασία του δεν πρέπει να απορρίπτεται μαζί με τα μικτά κοινοτικά απορρίμματα. Το σύμβολο υποδεικνύει ότι αυτό το προϊόν θα πρέπει να απορρίπτεται ξεχωριστά από τα συνήθη οικιακά απορρίμματα. Είστε υπεύθυνος για την απόρριψη του παρόντος και άλλου ηλεκτρικού και ηλεκτρονικού εξοπλισμού μέσω των καθορισμένων εγκαταστάσεων συγκέντρωσης απορριμμάτων οι οποίες παρέχονται από το κράτος ή τις αρμόδιες τοπικές αρχές. Η σωστή απόρριψη και ανακύκλωση συμβάλλει στην πρόληψη πιθανών αρνητικών συνεπειών για το περιβάλλον και την υγεία. Για περισσότερες πληροφορίες σχετικά με την απόρριψη του παλιού σας εξοπλισμού, παρακαλώ επικοινωνήστε με τις τοπικές αρχές, τις υπηρεσίες απόρριψης ή το κατάστημα από το οποίο αγοράσατε το προϊόν.

Magyar/Hungarian

Környezetvédelmi információ az európai uniós vásárlók számára

A 2002/96/EC számú európai uniós irányelv megkívánja, hogy azokat a termékeket, amelyeken, és/vagy amelyek csomagolásán az alábbi címke megjelenik, tilos a többi szelektálatlan lakossági hulladékkal együtt kidobni. A címke azt jelöli, hogy az adott termék kidobásakor a szokványos háztartási hulladékelszállítási rendszerektõl elkülönített eljárást kell alkalmazni. Az Ön felelõssége, hogy ezt, és más elektromos és elektronikus berendezéseit a kormányzati vagy a helyi hatóságok által kijelölt gyűjtőredszereken keresztül számolja fel. A megfelelõ hulladékfeldolgozás segít a környezetre és az emberi egészségre potenciálisan ártalmas negatív hatások megelõzésében. Ha elavult berendezéseinek felszámolásához további részletes információra van szüksége, kérjük, lépjen kapcsolatba a helyi hatóságokkal, a hulladékfeldolgozási szolgálattal, vagy azzal üzlettel, ahol a terméket vásárolta.

Italiano/Italian

Informazioni relative all'ambiente per i clienti residenti nell'Unione Europea

La direttiva europea 2002/96/EC richiede che le apparecchiature contrassegnate con questo simbolo sul prodotto e/o sull'imballaggio non siano smaltite insieme ai rifiuti urbani non differenziati. Il simbolo indica che questo prodotto non deve essere smaltito insieme ai normali rifiuti domestici. È responsabilità del proprietario smaltire sia questi prodotti sia le altre apparecchiature elettriche ed elettroniche mediante le specifiche strutture di raccolta indicate dal governo o dagli enti pubblici locali. Il corretto smaltimento ed il riciclaggio aiuteranno a prevenire conseguenze potenzialmente negative per l'ambiente e per la salute dell'essere umano. Per ricevere informazioni più dettagliate circa lo smaltimento delle vecchie apparecchiature in Vostro possesso, Vi invitiamo a contattare gli enti pubblici di competenza, il servizio di smaltimento rifiuti o il negozio nel quale avete acquistato il prodotto.

Latviešu valoda/Latvian

Ekoloģiska informācija klientiem Eiropas Savienības jurisdikcijā

Direktīvā 2002/96/EK ir prasība, ka aprīkojumu, kam pievienota zīme uz paša izstrādājuma vai uz tā iesaiņojuma, nedrīkst izmest nešķirotā veidā kopā ar komunālajiem atkritumiem (tiem, ko rada vietēji iedzīvotāji un uzņēmumi). Šī zīme nozīmē to, ka šī ierīce ir jāizmet atkritumos tā, lai tā nenonāktu kopā ar parastiem mājsaimniecības atkritumiem. Jūsu pienākums ir šo un citas elektriskas un elektroniskas ierīces izmest atkritumos, izmantojot īpašus atkritumu savākšanas veidus un līdzekļus, ko nodrošina valsts un pašvaldību iestādes. Ja izmešana atkritumos un pārstrāde tiek veikta pareizi, tad mazinās iespējamais kaitējums dabai un cilvēku veselībai. Sīkākas ziņas par novecojuša aprīkojuma izmešanu atkritumos jūs varat saņemt vietējā pašvaldībā, atkritumu savākšanas dienestā, kā arī veikalā, kur iegādājāties šo izstrādājumu.

Lietuvškai/Lithuanian

Aplinkosaugos informacija, skirta Europos Sąjungos vartotojams

Europos direktyva 2002/96/EC numato, kad įrangos, kuri ir (arba) kurios pakuotė yra pažymėta šiuo simboliu, negalima šalinti kartu su nerūšiuotomis komunalinėmis atliekomis. Šis simbolis rodo, kad gaminį reikia šalinti atskirai nuo bendro buitinių atliekų srauto. Jūs privalote užtikrinti, kad ši ir kita elektros ar elektroninė įranga būtų šalinama per tam tikras nacionalinės ar vietinės valdžios nustatytas atliekų rinkimo sistemas. Tinkamai šalinant ir perdirbant atliekas, bus išvengta galimos žalos aplinkai ir žmonių sveikatai. Daugiau informacijos apie jūsų senos įrangos šalinimą gali pateikti vietinės valdžios institucijos, atliekų šalinimo tarnybos arba parduotuvės, kuriose įsigijote tą gaminį.

Malti/Maltese

Informazzjoni Ambjentali għal Klijenti fl-Unjoni Ewropea

Id-Direttiva Ewropea 2002/96/KE titlob li t-tagħmir li jkun fih is-simbolu fuq il-prodott u/jew fuq l-ippakkjar ma jistax jintrema ma' skart muniċipali li ma ġiex isseparat. Is-simbolu jindika li dan il-prodott għandu jintrema separatament minn ma' l-iskart domestiku regolari. Hija responsabbiltà tiegħek li tarmi dan it-tagħmir u kull tagħmir ieħor ta' l-elettriku u elettroniku permezz ta' faċilitajiet ta' ġbir appuntati apposta mill-gvern jew mill-awtoritajiet lokali. Ir-rimi b'mod korrett u r-riċiklaġġ jgħin jipprevjeni konsegwenzi negattivi potenzjali għall-ambjent u għas-saħħa tal-bniedem. Għal aktar informazzjoni dettaljata dwar ir-rimi tat-tagħmir antik tiegħek, jekk jogħġbok ikkuntattja lill-awtoritajiet lokali tiegħek, is-servizzi għar-rimi ta' l-iskart, jew il-ħanut minn fejn xtrajt il-prodott.

Norsk/Norwegian

Miljøinformasjon for kunder i EU

EU-direktiv 2002/96/EF krever at utstyr med følgende symbol avbildet på produktet og/eller pakningen, ikke må kastes sammen med usortert avfall. Symbolet indikerer at dette produktet skal håndteres atskilt fra ordinær avfallsinnsamling for husholdningsavfall. Det er ditt ansvar å kvitte deg med dette produktet og annet elektrisk og elektronisk avfall via egne innsamlingsordninger slik myndighetene eller kommunene bestemmer. Korrekt avfallshåndtering og gjenvinning vil være med på å forhindre mulige negative konsekvenser for miljø og helse. For nærmere informasjon om håndtering av det kasserte utstyret ditt, kan du ta kontakt med kommunen, en innsamlingsstasjon for avfall eller butikken der du kjøpte produktet.

Polski/Polish

Informacja dla klientów w Unii Europejskiej o przepisach dotyczących ochrony środowiska

Dyrektywa Europejska 2002/96/EC wymaga, aby sprzęt oznaczony symbolem znajdującym się na produkcie i/lub jego opakowaniu nie był wyrzucany razem z innymi niesortowanymi odpadami komunalnymi. Symbol ten wskazuje, że produkt nie powinien być usuwany razem ze zwykłymi odpadami z gospodarstw domowych. Na Państwu spoczywa obowiązek wyrzucania tego i innych urządzeń elektrycznych oraz elektronicznych w punktach odbioru wyznaczonych przez władze krajowe lub lokalne. Pozbywanie się sprzętu we właściwy sposób i jego recykling pomogą zapobiec potencjalnie negatywnym konsekwencjom dla środowiska i zdrowia ludzkiego. W celu uzyskania szczegółowych informacji o usuwaniu starego sprzętu, prosimy zwrócić się do lokalnych władz, służb oczyszczania miasta lub sklepu, w którym produkt został nabyty.

Português/Portuguese

Informação ambiental para clientes da União Europeia

A Directiva Europeia 2002/96/CE exige que o equipamento que exibe este símbolo no produto e/ou na sua embalagem não seja eliminado junto com os resíduos municipais não separados. O símbolo indica que este produto deve ser eliminado separadamente dos resíduos domésticos regulares. É da sua responsabilidade eliminar este e qualquer outro equipamento eléctrico e electrónico através dos instalações de recolha designadas pelas autoridades governamentais ou locais. A eliminação e reciclagem correctas ajudarão a prevenir as consequências negativas para o ambiente e para a saúde humana. Para obter informações mais detalhadas sobre a forma de eliminar o seu equipamento antigo, contacte as autoridades locais, os serviços de eliminação de resíduos ou o estabelecimento comercial onde adquiriu o produto.

Slovenčina/Slovak

Informácie o ochrane životného prostredia pre zákazníkov v Európskej únii

Podľa európskej smernice 2002/96/ES zariadenie s týmto symbolom na produkte a/alebo jeho balení nesmie byť likvidované spolu s netriedeným komunálnym odpadom. Symbol znamená, že produkt by sa mal likvidovať oddelene od bežného odpadu z domácností. Je vašou povinnosťou likvidovať toto i ostatné elektrické a elektronické zariadenia prostredníctvom špecializovaných zberných zariadení určených vládou alebo miestnymi orgánmi. Správna likvidácia a recyklácia pomôže zabrániť prípadným negatívnym dopadom na životné prostredie a zdravie ľudí. Ak máte záujem o podrobnejšie informácie o likvidácii starého zariadenia, obráťte sa, prosím, na miestne orgány, organizácie zaoberajúce sa likvidáciou odpadov alebo obchod, v ktorom ste si produkt zakúpili.

Slovenčina/Slovene

Okoljske informacije za stranke v Evropski uniji

Evropska direktiva 2002/96/EC prepoveduje odlaganje opreme, označene s tem simbolom – na izdelku in/ali na embalaži – med običajne, nerazvrščene odpadke. Ta simbol opozarja, da je treba izdelek odvreči ločeno od preostalih gospodinjskih odpadkov. Vaša odgovornost je, da to in preostalo električno in elektronsko opremo odnesete na posebna zbirališča, ki jih določijo državne ustanove ali lokalna uprava. S pravilnim odlaganjem in recikliranjem boste preprečili morebitne škodljive vplive na okolje in zdravje ljudi. Če želite izvedeti več o odlaganju stare opreme, se obrnite na lokalno upravo, odpad ali trgovino, kjer ste izdelek kupili.

Español/Spanish

Información medioambiental para clientes de la Unión Europea

La Directiva 2002/96/CE de la UE exige que los equipos que lleven este símbolo en el propio aparato y/o en su embalaje no deben eliminarse junto con otros residuos urbanos no seleccionados. El símbolo indica que el producto en cuestión debe separarse de los residuos domésticos convencionales con vistas a su eliminación. Es responsabilidad suya desechar este y cualesquiera otros aparatos eléctricos y electrónicos a través de los puntos de recogida que ponen a su disposición el gobierno y las autoridades locales. Al desechar y reciclar correctamente estos aparatos estará contribuyendo a evitar posibles consecuencias negativas para el medio ambiente y la salud de las personas. Si desea obtener información más detallada sobre la eliminación segura de su aparato usado, consulte a las autoridades locales, al servicio de recogida y eliminación de residuos de su zona o pregunte en la tienda donde adquirió el producto.

Svenska/Swedish

Miljöinformation för kunder i Europeiska unionen

Det europeiska direktivet 2002/96/EC kräver att utrustning med denna symbol på produkten och/eller förpackningen inte får kastas med osorterat kommunalt avfall Symbolen visar att denna produkt bör kastas efter att den avskiljts från vanligt hushållsavfall. Det faller på ditt ansvar att kasta denna och annan elektrisk och elektronisk utrustning på fastställda insamlingsplatser utsedda av regeringen eller lokala myndigheter. Korrekt kassering och återvinning skyddar mot eventuella negativa konsekvenser för miljön och personhälsa. För mer detaljerad information om kassering av din gamla utrustning kontaktar du dina lokala myndigheter, avfallshanteringen eller butiken där du köpte produkten.

For more information, visit www.linksys.com.

Specifications

SRW2024 Specifications

Model	SRW2024
Ports	24 RJ-45 connectors for 10BASE-T, 100BASE-TX and 1000BASE-T with 4 shared SFP slots
Cabling Type	UTP CAT 5 or better for 10BASE-T/100BASE-TX, UTP CAT 5e or better for 1000BASE-T
LEDs	System, Link/Act, PoE
Switching Capacity	48 Gbps, non-blocking
Web User Interface	Built-in web UI for easy browser-based configuration (HTTP/HTTPS)
SNMP	SNMP version v1, v2c with support for traps
SNMP MIBs	RFC1213 MIB-2, RFC2863 Interface MIB, RFC2665 Ether-like MIB, RFC1493 Bridge MIB, RFC2674 Extended Bridge MIB (P-bridge, Q-bridge), RFC2819 RMON MIB (groups 1,2,3,9 only), RFC2737 Entity MIB, RFC 2618 RADIUS Client MIB
Port Mirroring	Traffic on a port can be mirrored to another port for analysis with a network analyzer or RMON probe
Other Management	RFC854 Telnet (Menu-driven configuration) Secure Shell (SSH) and Telnet Management Telnet Client SSL security for web UI Switch Audit Log DHCP Client BootP SNTP Xmodem upgrade Cable Diagnostics PING
F/W Upgrade	web browser upgrade (HTTP)
RMON	Embedded Remote Monitoring (RMON) software agent supports four RMON groups (history, statistics, alarms, and events) for enhanced traffic management, monitoring, and analysis
MAC Table Size	8K
IEEE 802.1X	802.1x - RADIUS Authentication. MD5 Encryption
Link Aggregation	Link Aggregation using IEEE 802.3ad LACP, Up to 8 ports in up to 8 LAGs.

SRW2024 Specifications

Storm Control	Broadcast, Multicast, and Unknown Unicast
Spanning Tree	EEE 802.1d Spanning Tree, IEEE 802.1w Rapid Spanning Tree
IGMP Snooping	IGMP (v1/v2) snooping provides for fast client joins and leaves of multicast streams and limits bandwidth-intensive video traffic to only the requestors
Priority Levels	4 Hardware queues
Scheduling	Priority Queueing and Weighted Round Robin (WRR)
Class of Service	Port-based 802.1p VLAN priority based IP TOS/DSCP based CoS IPv6 Traffic Class based CoS
Number of VLANs	256
VLAN	Port-based and 802.1q based VLANs Management VLAN
HOL Blocking	Head of line blocking prevention
Jumbo frame	Supports frames up to 10K byte frames
Standards	IEEE 802.3-2005 Ethernet, IEEE 802.3u Fast Ethernet, IEEE 802.3z Gigabit Ethernet, IEEE 802.ab Gigabit Ethernet, Flow Control
Power	Internal switching power
Certification	FCC Part 15 Class A, CE Class A, UL, cUL, CE mark, CB
Dimensions	16.93" x 1.75" x 13.78" (430 x 44.45 x 350 mm)
Unit Weight	8.60 lb. (4.47 kg)
Operating Temperature	32 to 104°F (0 to 50°C)
Storage Temperature	-4 to 158°F (-20 to 70°C)
Operating Humidity	10% to 90%
Storage Humidity	10% to 95%