



**USER GUIDE**

# 24- or 48-Port 10/100 + 4-Port Gigabit Switch with WebView and Power over Ethernet

**BUSINESS SERIES**

<b>Chapter 2: About This Guide . . . . .</b>	<b>4</b>
Icon Descriptions	4
Online Resources	4
Copyright and Trademarks	5
<b>Chapter 3: Introduction . . . . .</b>	<b>6</b>
<b>Chapter 4: Getting to Know the Switch . . . . .</b>	<b>8</b>
Front Panels	8
Ports	9
The Back Panel	9
The Side Panel	10
LAN Ports	10
The Gigabit Expansion Ports	10
The Console Port	11
<b>Chapter 5: Connecting the Switch . . . . .</b>	<b>12</b>
Overview	12
Before You Install the Switch...	13
Placement Options	13
Connecting the Switch	14
Uplinking the Switch	15
<b>Chapter 6: Using the Console Interface for Configuration . . . . .</b>	<b>16</b>
Overview	16
Configuring the HyperTerminal Application	16
Connecting to the Switch through a Telnet Session	17
Configuring the Switch through the Console Interface	18
<b>Chapter 7: Using the Web-based Utility for Configuration . . . . .</b>	<b>31</b>
Overview	31
Accessing the Web-based Utility	31
Setup Tab—Summary	32
Setup Tab—Network Settings	34
Setup Tab—Time	35
Port Management Tab—Port Settings	37
Port Management Tab—Link Aggregation	40
Port Management Tab—LACP	41
Port Management Tab -PVE Mapping	43
Port Management Tab—PoE Power Settings	43
VLAN Management Tab—Create VLAN	45
VLAN Management Tab—Port Settings	46
VLAN Management Tab—Ports to VLAN	47
VLAN Management Tab—VLAN to Ports	48
VLAN Management Tab—GVRP	49
Statistics Tab—RMON Statistics	51
Statistics Tab—RMON History	53
Statistics Tab—RMON Alarms	54
Statistics Tab—RMON Events	56
Statistics Tab—Port Utilization	58

Statistics Tab—802.1x Statistics	59
ACL Tab—IP Based ACL	60
ACL Tab—IPv6 Based ACL	63
ACL Tab—MAC Based ACL	64
ACL Tab—TCAM Utilization	65
Security Tab—ACL Binding	65
Security Tab—Authentication Servers	66
Security Tab—802.1x Settings	68
Security Tab—Port Security	70
Security Tab—HTTPS Settings	72
Security Tab—Management ACL	73
Security Tab—Dynamic VLAN	74
Security Tab—Network Access MAC Address	75
Security Tab—SSH Settings	76
Security Tab—SSH Host-Key Settings	77
QoS Tab	78
QoS Tab—CoS Settings	78
QoS Tab—Queue Settings	80
QoS Tab—DSCP Settings	81
QoS Tab—Diffserv Settings	82
QoS Tab—Diffserv Port Binding	85
Click Save Settings to save the changes.	86
QoS Tab—Bandwidth	86
Spanning Tree Tab	87
Spanning Tree Tab—STP Status	87
Spanning Tree Tab—Global STP	89
Spanning Tree Tab—STP Port Settings	90
Spanning Tree Tab—RSTP Port Settings	93
Spanning Tree Tab—MSTP Properties	95
Spanning Tree Tab—MSTP Instance Settings	95
Spanning Tree Tab—MSTP Interface Settings	97
Multicast Tab—Global Settings	99
Multicast Tab—Static Member Ports	100
Multicast Tab—Static Router Ports	100
Multicast Tab—Member Ports Query	102
Multicast Tab—Router Ports Query	103
SNMP Tab	103
SNMP Tab—Global Parameters	104
SNMP Tab—Views	106
SNMP Tab—Group Profile	107
SNMP Tab—Group Membership	107
SNMP Tab—Communities	109
SNMP Tab—Notification Recipient	110
Admin Tab—User Authentication	111
Admin Tab—Forwarding Database	113
Admin Tab—Log	115
Admin Tab—Port Mirroring	118
Admin Tab—Cable Test	119
Admin Tab—Ping	120
Admin Tab—Save Configuration	121
Admin Tab—Jumbo Frame	121

Admin Tab—Firmware Upgrade	123
Admin Tab—HTTP Upgrade	124
Admin Tab—Reboot	125
Admin Tab—Factory Default	126
<b>Appendix A: Specifications . . . . .</b>	<b>127</b>
<b>Appendix B: Warranty Information . . . . .</b>	<b>133</b>
Limited Warranty	133
Exclusions and Limitations	133
Obtaining Warranty Service	134
Technical Support	134
<b>Appendix C: Regulatory Information . . . . .</b>	<b>135</b>
Federal Communications Commission Interference Statement	135
Industry Canada Statement	135
Règlement d'Industry Canada	135
EC Declaration of Conformity (Europe)	136
User Information for Consumer Products Covered by EU Directive 2002/96/EC on Waste Electric and Electronic Equipment (WEEE)	136
<b>Appendix D: Safety Information . . . . .</b>	<b>143</b>
Meaning of the Warning Symbol	143
General Safety Information	143
Power Safety Information	144
<b>Appendix E: Software License Agreement . . . . .</b>	<b>146</b>
Software in Linksys Products:	146
Software Licenses:	146
Schedule 1 Linksys Software License Agreement	146
Schedule 2	148
Schedule 3	153
<b>Appendix F: Contacts. . . . .</b>	<b>156</b>
<b>Appendix G: Gigabit Ethernet and Fiber Optic Cabling . . . . .</b>	<b>157</b>
Gigabit Ethernet	157
Fiber Optic Cabling	157
<b>Appendix H: Windows Help. . . . .</b>	<b>158</b>
TCP/IP	158
Shared Resources	158
Network Neighborhood/My Network Places	158
<b>Appendix I: Downloading using Xmodem . . . . .</b>	<b>159</b>
Startup Menu Procedures	159
<b>Appendix J: Glossary . . . . .</b>	<b>162</b>

# About This Guide

## Icon Descriptions

While reading through the User Guide you may see various icons that call attention to specific items. Below is a description of these icons:



**NOTE:** This check mark indicates that there is a note of interest and is something that you should pay special attention to while using the product.



**WARNING:** This graphic means that there is a caution or warning and it is something that could damage your property or product.



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

## Online Resources

Resource	Website
Linksys	<a href="http://www.linksys.com">www.linksys.com</a>
Linksys International	<a href="http://www.linksys.com/international">www.linksys.com/international</a>
Glossary	<a href="http://www.linksys.com/glossary">www.linksys.com/glossary</a>
Network Security	<a href="http://www.linksys.com/security">www.linksys.com/security</a>

## Copyright and Trademarks

 <p><b>LINKSYS</b><sup>®</sup> A Division of Cisco</p> 	<p>Linksys is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. Copyright © 2008 Cisco Systems, Inc. All rights reserved. Other brands and product names are trademarks or registered trademarks of their respective holders.</p>
---	---

# 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 using 802.1x security using a RADIUS authentication mechanism and can also be controlled using MAC-based filtering.

Extensive QoS features makes the solution ideal for real-time applications like Voice and Video. The 4 priority queues together with the Weighted Round Robin and Strict Priority scheduling techniques facilitate efficient coexistence 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.

There are features that allow you to expand and grow your network of switches. Link aggregation allows multiple high-bandwidth trunks between switches to be setup. This also provides a level of reliability in that the system continues to operate if one of the links break. Spanning Tree (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.

What's in this User Guide?

- [Chapter 2, "About This Guide"](#)

This Chapter describes Icons you will see throughout the guide, as well as Online Resources that can help when using this product.

- [Chapter 3, "Introduction"](#)

The current Chapter, this is an introduction and where to find information.

- [Chapter 4, "Getting to Know the Switch"](#)

This chapter describes the physical features of the Switch.

- [Chapter 5, "Connecting the Switch"](#)

This chapter explains how to install and connect the Switch.

- [Chapter 6, "Using the Console Interface for Configuration"](#)

This chapter instructs you on how to use the Switch's console interface when you configure the Switch.

- [Chapter 7, "Using the Web-based Utility for Configuration"](#)

This chapter shows you how to configure the Switch using the Web-based Utility.

- [Appendix A, "Specifications"](#)

This appendix provides the Switch's technical specifications.

- [Appendix B, "Warranty Information"](#)

This appendix supplies the Switch's warranty information.

- [Appendix C, "Regulatory Information"](#)

This appendix supplies the Switch's regulatory information.

- [Appendix D, "Safety Information"](#)

This appendix describes the meaning of the various safety and warning symbols.

- [Appendix E, "Software License Agreement"](#)

This appendix describes the End User Software License Agreement.

- [Appendix F, "Contacts"](#)

This appendix provides contact information for a variety of Linksys resources, including Technical Support.

- [Appendix G, "Gigabit Ethernet and Fiber Optic Cabling"](#)

This appendix provides information about Fiber Optic cabling and Gigabit Ethernet requirements.

- [Appendix H, "Windows Help"](#)

This appendix describes how you can use Windows Help for instructions about networking, such as installing the TCP/IP protocol.

- [Appendix I, "Downloading using Xmodem"](#)

This appendix describes how you can download software into the Switch using Xmodem.

- [Appendix J, "Glossary"](#)

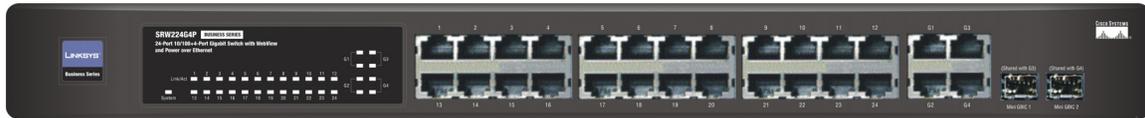
This appendix gives a brief glossary of terms frequently used in networking.

# Getting to Know the Switch

## Front Panels

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

**SRW224G4P—Front Panel**



**SRW248G4P—Front Panel**



## LEDs

LED	Description
System	Green. 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)	Green. The Link/Act LED lights up green to indicate a functional 10/100Mbps network link through the corresponding port with an attached device that does not use Power over Ethernet (PoE). Blinks green to indicate that the Switch is actively sending or receiving data over that port.
	Orange. The Link/Act LED lights up orange to indicate a functional 10/100Mbps network link through the corresponding port with an attached PoE device.
Link/Act (G1-G4)	Green. The Link/Act LED lights up green to indicate a functional 10/100Mbps network link through the corresponding port with an attached device. Blinks green to indicate that the Switch is actively sending or receiving data over that port.
	Orange. The Link/Act LED lights up orange to indicate a functional 1000Mbps network link through the corresponding port with an attached device.
PoE	Orange. The PoE LED lights orange to indicate a powered device is connected to the corresponding port (1 through 24).

LED	Description
	Flashes to indicate that the Switch is actively sending power over that port.

## Ports

Name	Description
SRW224G4P LAN (1-24) SRW248G4P LAN (1-48)	The LAN (Local Area Network) ports connect to Ethernet network devices, such as other switches or routers.
SRW224G4P MiniGBIC (G3) / MiniGBIC (G4) SRW248G4P MiniGBIC (G3) / MiniGBIC (G4)	<p>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. They link to high-speed network peripheral system or clients at speeds of 1000Mbps.</p> <p>Use the Linksys MGBT1, MGBSX1, or MGBLH1 miniGBIC modules with the Switch.</p> <p>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.</p>
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. Refer to 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.

### Back Panel



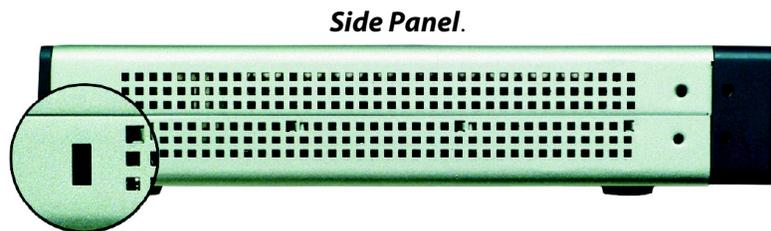
Label	Description
Power	The Power port is where you connect the power cord.



**NOTE:** If you need to reset the Switch, unplug 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.



Name	Description
Security	Slot The security slot is where you can attach a lock so the Switch will be protected from theft.

## LAN Ports

These Switches are equipped with twenty-four and forty-eight auto-sensing RJ-45 LAN ports. These RJ-45 ports support network speeds of either 10Mbps or 100Mbps, 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 or 100Mbps), and adjust its speed and duplex 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

These Switches are equipped with two miniGBIC ports that have shared Gigabit Ethernet ports (G3 on the SRW224G4P) and (G4 on the SRW248G4P) 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, refer to "[Appendix G, "Gigabit Ethernet and Fiber Optic Cabling"](#)".

### **The Console Port**

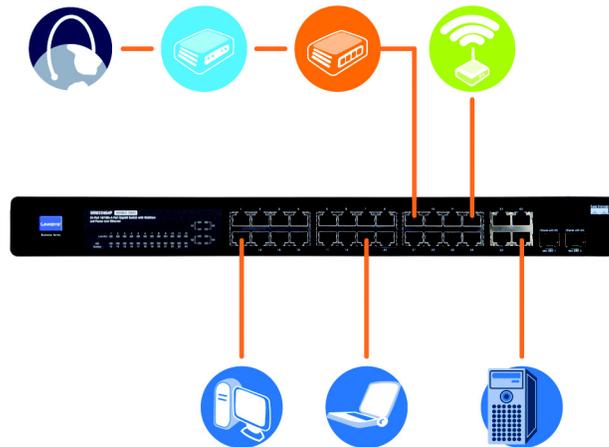
These Switches are equipped with a serial port labeled Console (located on the back of the switch) that allows you to connect to a computer's serial port (for configuration purposes) using the provided serial cable. You can use HyperTerminal to manage the Switch using the console port. With this and many other Linksys products, your networking options are limitless. Go to the Linksys website at [www.linksys.com](http://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. All explanations shown in this chapter, unless specifically identified, are applicable to both the SRW224G4P and the SRW248G4P switches. For an example of a typical network configuration, see the application diagram shown below.

### Typical Network Configuration for the SRW224G4P or SRW248G4P



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

**Table 1: Maximum Cabling Distances**

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)



**NOTE:** 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 rackmount placement.



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

## Desktop Placement

1. Attach the rubber feet to the recessed areas on the bottom of the Switch.

### Add Feet



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 to the section, **\*\*\*“Connecting the Switch.”**

## Rack-Mount Placement

To mount the SRW224G4P or the SRW248G4P Switch in any standard-sized, 19-inch wide, 1U high rack, follow these instructions:

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.

### *Attach the Brackets to the Switch*



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.

### *Mount the Switch in the Rack*



5. Proceed to the section, "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.)



**IMPORTANT:** 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.



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

## 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 6, "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 7, "Using the Web-based Utility for Configuration."](#)

# Using the Console Interface for Configuration

## Overview

The SRW224G4P and the SRW248G4P Switches feature a menu-driven console interface for basic configuration of the Switch and management of your network. The Switches 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.

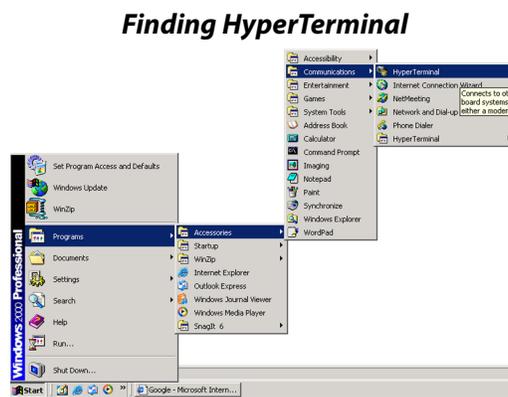
## Configuring the HyperTerminal Application

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 SRW224G4P. 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**.

## Connect To



4. Set the serial port settings as follows:

Bits per second: **38400**

Data bits: **8**

Parity: **None**

Stop bits: **1**

Flow control: **None**

Then, click the **OK** button.

## COM1 Properties



## 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 will now appear. The first time you open the CLI interface, select **Edit** and press **Enter**. Enter **admin** in the User Name field. Leave the Password field blank.

Press the **Esc** button and you will return to the *Login* screen. Use the right arrow button to navigate to **Execute** and press the **Enter** button to enter the CLI interface.

## Telnet Login Screen



## 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 Menu
2. Port Status
3. Port Configuration
4. PoE Configuration
5. Help
0. Logout

### Switch Main Menu



## System Configuration Menu

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

1. System Configuration
2. Management Settings
3. User & Password Settings
4. IP Configuration
5. File Management
6. Restore System Default Settings
7. Reboot System
0. Back to Main Menu

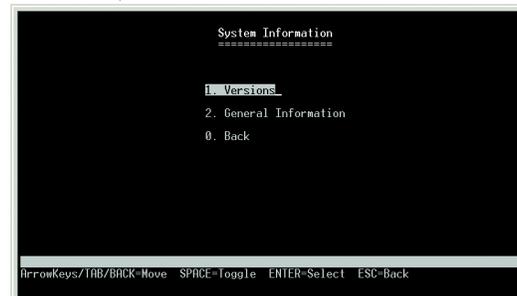
### **System Configuration Menu**



## System Information

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

### **System Information Menu**



## Versions

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

```

Versions
-----
Boot Version:      1.0.2
Software Version:  1.0.3
Loader Version:    1.0.2
Hardware Version:  R01

Action-> Quit
ArrowKeys/TAB/BACK-Move SPACE=Toggle ENTER=Select ESC=Back

```

## 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.

```

General System Information
-----
System Description: SRH2024P
System Up Time:    0, 0:26:13 <day, hour:min:sec>
System Mac Address: 00-16-B6-F0-3C-F8
System Contact:
System Name:
System Location:

Action-> Quit Edit Save
ArrowKeys/TAB/BACK-Move SPACE=Toggle ENTER=Select ESC=Back

```

## Management Settings

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

```

Management Settings Menu
-----
1. Serial Port Configuration
2. Protocol Configuration
0. Back

ArrowKeys/TAB/BACK-Move SPACE=Toggle ENTER=Select ESC=Back

```

## 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.

### Serial Port Configuration

```
Serial Port Configuration
=====
Baud Rate:      38400  bps

Action-> Quit Edit Save
ArrowKeys/TAB/BACK-Move SPACE=Toggle ENTER=Select ESC=Back
```

## Protocol Configuration

On the *Protocol Configuration* screen, you can enable or disable LLDP or UPnP.

Select **Edit**, use the **Tab** key to highlight LLDP or UPnP, and press the **Enter** key to make changes. Toggle the protocol state to **enabled** or **disabled** 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.

### Protocol Configuration

```
Protocol Configuration
=====
LLDP Status      Enable
Upnp Status       Enable

Action-> Quit Edit Save
ArrowKeys/TAB/BACK-Move SPACE=Toggle ENTER=Select ESC=Back
```

## 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.

## User & Password Settings

```
User & Password Settings
=====
Username      Password      Again Password
-----
1. admin      *****      *****
2.
3.
4.
5.
Action-> Quit Edit Save
ArrowKeys/TAB/BACK=Move SPACE=Toggle ENTER=Select ESC=Back
```



**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 Configuration Menu

```
IP Configuration
=====
1. IP Address Settings
2. HTTP/HTTPS
3. SNMP
4. Network Diagnostics
0. Back
ArrowKeys/TAB/BACK=Move SPACE=Toggle ENTER=Select ESC=Back
```

## IP Address Configuration

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.

## IP Address Configuration

```
IP Address Configuration
*****
IP Address      192.168.1.254
Subnet Mask     255.255.255.0
Default Gateway 0.0.0.0
Management VLAN 1
IP Mode         User Define

Action-> Quit Edit Save
ArrowKeys/TAB/BACK=Move SPACE=Toggle ENTER=Select ESC=Back
```

## 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.

## HTTP/HTTPS

```
HTTP/HTTPS
*****
HTTP Server     ENABLE
HTTP Server port 80
HTTPS Server    ENABLE
HTTPS Server port 443

Action-> Quit Edit Save
ArrowKeys/TAB/BACK=Move SPACE=Toggle ENTER=Select ESC=Back
```

## SNMP

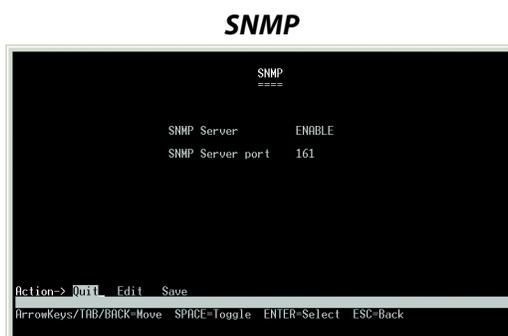
The *SNMP* screen allows you to set the Switch's SNMP settings.

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 Diagnostics Menu displays two choices: Ping and Traceroute.



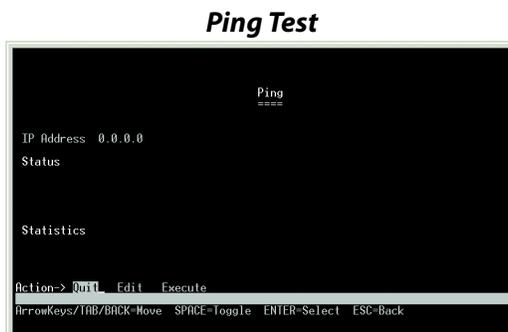
## Ping

The *Ping* 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.



## Traceroute

The *Traceroute* Screen allows you to display the route taken to reach another network device. The *Traceroute* screen displays the IP address of the location you want to reach.

Select **Edit** to change the IP address, and select **Execute** to begin the trace route function.

The trace route function first sends probe datagrams with the TTL value set at one. This causes the first router to discard the datagram and return an error message. The trace function then sends several probe messages at each subsequent TTL level and displays the round-trip time for each message. If the timer goes off before a response is returned, the trace function prints a series of asterisks.

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.

## Traceroute Test

```
Traceroute
*****
IP Address: 0.0.0.0
Status
Results

Action-> Quit Edit Execute
ArrowKeys/TAB/BACK=Move SPACE=Toggle ENTER=Select ESC=Back
```

## 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.

## File Management

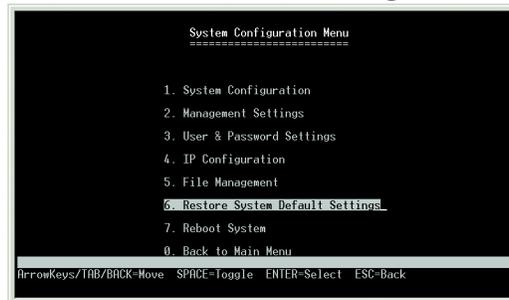
```
File Management
*****
Source File:      tftp
Destination File: image
File Name:
IP Address:      0.0.0.0

Action-> Quit Edit Execute
ArrowKeys/TAB/BACK=Move SPACE=Toggle ENTER=Select ESC=Back
```

## 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.

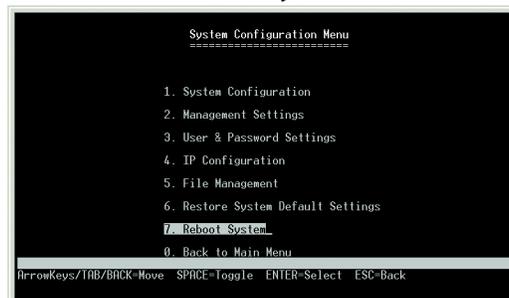
## Restore Default Settings



## 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.

## Reboot System



## 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.

## Back to Main Menu



## 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 Status

```

Port Status
=====
Port  Enable  Link  Spd  Flow  Port  Enable  Link  Spd  Flow
Dplx Ctrl                                     Dplx Ctrl
-----
Giga1  Enable  Up    1000F  None  Giga13  Enable  Down
Giga2  Enable  Down  -----  Giga14  Enable  Down
Giga3  Enable  Down  -----  Giga15  Enable  Down
Giga4  Enable  Down  -----  Giga16  Enable  Down
Giga5  Enable  Down  -----  Giga17  Enable  Down
Giga6  Enable  Down  -----  Giga18  Enable  Down
Giga7  Enable  Down  -----  Giga19  Enable  Down
Giga8  Enable  Down  -----  Giga20  Enable  Down
Giga9  Enable  Down  -----  Giga21  Enable  Down
Giga10  Enable  Down  -----  Giga22  Enable  Down
Giga11  Enable  Down  -----  Giga23  Enable  Down
Giga12  Enable  Down  -----  Giga24  Enable  Down

Action-> Quit Refresh
ArrowKeys/TAB/BACK=Move SPACE=Toggle ENTER=Select ESC=Back
    
```

## 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.

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, when 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

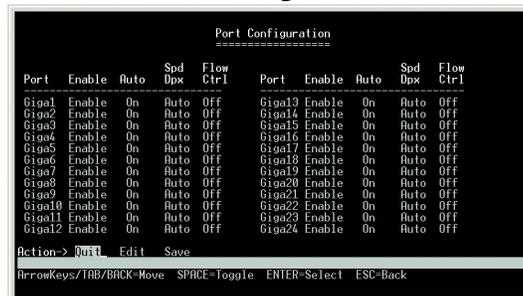
(Default: Auto-negotiation enabled; Advertised capabilities for 100Base-TX – 10half, 10full, 100half, 100full; 1000Base-T – 10half, 10full, 100half, 100full, 1000full; 1000Base-SX/LX/LH (SFP) – 1000full;

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.

## Port Configuration



```
Port Configuration
=====
Port  Enable  Auto  Spd  Flow  Port  Enable  Auto  Spd  Flow
      Dplx  Ctrl                                Dplx  Ctrl
-----
Giga1  Enable  On    Auto Off    Giga13 Enable  On    Auto Off
Giga2  Enable  On    Auto Off    Giga14 Enable  On    Auto Off
Giga3  Enable  On    Auto Off    Giga15 Enable  On    Auto Off
Giga4  Enable  On    Auto Off    Giga16 Enable  On    Auto Off
Giga5  Enable  On    Auto Off    Giga17 Enable  On    Auto Off
Giga6  Enable  On    Auto Off    Giga18 Enable  On    Auto Off
Giga7  Enable  On    Auto Off    Giga19 Enable  On    Auto Off
Giga8  Enable  On    Auto Off    Giga20 Enable  On    Auto Off
Giga9  Enable  On    Auto Off    Giga21 Enable  On    Auto Off
Giga10 Enable  On    Auto Off   Giga22 Enable  On    Auto Off
Giga11 Enable  On    Auto Off   Giga23 Enable  On    Auto Off
Giga12 Enable  On    Auto Off   Giga24 Enable  On    Auto Off

Action-> Quit Edit Save
ArrowKeys/TAB/BACK-Move SPACE=Toggle ENTER=Select ESC=Back
```

## 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 Configuration



```
PoE Main Menu
=====
1. System PoE Configuration
2. Port PoE Status
3. Port PoE Configuration
0. Back

ArrowKeys/TAB/BACK-Move SPACE=Toggle ENTER=Select ESC=Back
```

## 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.

## Power Configuration

```

Power Configuration
=====
Power Allocation(37-180) 180

Action-> Quit Edit Save
ArrowKeys/TAB/BACK=Move SPACE=Toggle ENTER=Select ESC=Back
    
```

## 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.

## Power Port Status

```

Power Port Status
=====
Port  Admin  Pri-  Allo-  Cons-  Port  Admin  Pri-  Allo-  Cons-
Status mode ority cation umption Status mode ority cation umption
1  Enable Off Low 15400 0 13 Enable Off Low 15400 0
2  Enable Off Low 15400 0 14 Enable Off Low 15400 0
3  Enable Off Low 15400 0 15 Enable Off Low 15400 0
4  Enable Off Low 15400 0 16 Enable Off Low 15400 0
5  Enable Off Low 15400 0 17 Enable Off Low 15400 0
6  Enable Off Low 15400 0 18 Enable Off Low 15400 0
7  Enable Off Low 15400 0 19 Enable Off Low 15400 0
8  Enable Off Low 15400 0 20 Enable Off Low 15400 0
9  Enable Off Low 15400 0 21 Enable Off Low 15400 0
10 Enable Off Low 15400 0 22 Enable Off Low 15400 0
11 Enable Off Low 15400 0 23 Enable Off Low 15400 0
12 Enable Off Low 15400 0 24 Enable Off Low 15400 0

Action-> Quit Refresh
ArrowKeys/TAB/BACK=Move SPACE=Toggle ENTER=Select ESC=Back
    
```

## 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 and up-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.

## Power Port Configuration

```
Power Port Configuration
=====
Port  Admin Status Priority Power Allocation  Port  Admin Status Priority Power Allocation
-----
1  Enable Low 15400 13 Enable Low 15400
2  Enable Low 15400 14 Enable Low 15400
3  Enable Low 15400 15 Enable Low 15400
4  Enable Low 15400 16 Enable Low 15400
5  Enable Low 15400 17 Enable Low 15400
6  Enable Low 15400 18 Enable Low 15400
7  Enable Low 15400 19 Enable Low 15400
8  Enable Low 15400 20 Enable Low 15400
9  Enable Low 15400 21 Enable Low 15400
10 Enable Low 15400 22 Enable Low 15400
11 Enable Low 15400 23 Enable Low 15400
12 Enable Low 15400 24 Enable Low 15400
Action-> Quit Edit Save
ArrowKeys/TAB/BACK=Move SPACE=Toggle ENTER=Select ESC=Back
```

## 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.

## Help

```
Help
====
The device screens consist of a series
of menus. Each menu has several options,
which are listed vertically. To select
an option, highlight the option and press
<Enter>. The highlighted option is activated.
Action-> Quit
ArrowKeys/TAB/BACK=Move SPACE=Toggle ENTER=Select ESC=Back
```

## Log Out

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

## Log Out

```
Switch Main Menu
=====
1. System Configuration Menu
2. Port Status
3. Port Configuration
4. PoE Configuration
5. Help
0. Log Out
ArrowKeys/TAB/BACK=Move SPACE=Toggle ENTER=Select ESC=Back
```

# 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

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

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.



**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 management station used to configure the device.

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.

The LEDs on the *Setup Summary* screen display status information about their corresponding ports. A green LED indicates a connection, while 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. The front panel LEDs display different status information, which is described in Chapter 2: Getting to Know the Switch.

### Login Screen

## Setup Tab—Summary

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

Category	Parameter	Value
Device Information	System Name	
	IP Address	192.168.1.254
	Subnet Mask	255.255.255.0
	DNS Servers	
	Default Gateway	0.0.0.0
	Address Mode	Static
System Information	Base MAC Address	00-1C-10-EC-D5-6D
	Serial Number	WQ200GB01821
	Model Name	SRW224G4P
	Hardware Version	R01
	Boot Version	1.0.1 Dec 1 2006
	Firmware Version	1.2.4 Aug 27 2008
PoE Information	System Location	
	System Contact	
	System Uptime	0 days, 0 hours, 15 minutes, and 31.24 seconds
	Current Time	00:16:14 Jan 1 2001
PoE Information	Maximum Available Power	180 watts
	System Operation Status	on
	Main Power Consumption	0 watts

### Device Information

**System Name**—Displays the name for the Switch, if one has been entered on the Setup-Network Settings tab.

**IP Address**—The IP address of the Switch is displayed here (configurable from Setup—Network Settings tab).

**Subnet Mask**—The Subnet Mask of the Switch is displayed here (configurable from Setup—Network Settings tab).

**DNS Servers**—The DNS Servers are displayed here (configurable from Setup—Network Settings tab).

**Default Gateway**—The Default Gateway is displayed here (configurable from Setup—Network Settings tab).

**Address Mode**—Indicates whether the Switch is configured with a Static or Dynamic IP address (configurable from Setup—Network Settings tab).

**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**—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 (configurable from Setup—Network Settings tab).

**System Contact**—The contact person for this Switch is displayed here (configurable from Setup—Network Settings tab).

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

**Current Time**—The system time is displayed here (configurable from Setup—Time tab).

### PoE Information

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

**System Operation Status**—Displays whether the Switch can provide PoE power or not.

**Main power Consumption**—Displays 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.

The screenshot displays the Linksys web-based utility interface for configuring a 24-port 10/100 PoE Switch. The main navigation bar includes 'Setup', 'Port Management', 'VLAN Management', 'Statistics', 'ACL', 'Security', 'QoS', 'Spanning Tree', 'Multicast', and 'More >>'. The 'Network Settings' section is active, showing fields for Identification (System Name, System Location, System Contact, Object ID, Base MAC address) and IP Configuration (Management VLAN, IP Address Mode, Host Name, IP Address, Subnet Mask, Default Gateway, DNS Server). A 'Restart DHCP' button is also present. A help sidebar on the right explains the IP Configuration tab. At the bottom, there are 'Save Settings' and 'Cancel Changes' buttons.

### Identification

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

**System Location**—This field is used for entering 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 allows you to select the Management VLAN.

**IP Address Mode**—This drop-down 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 will only record 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 will attempt 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 menu.

**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 non-US and European countries, specify the amount of time for daylight savings. The default is 60 minutes. You may enter 1-1440 minutes.

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

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

**Recurring**—If you selected **Other** 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 primary SNTP server here.

**Server2**—Enter a secondary SNTP server here.

**Polling Interval**—The value defined here determines the amount of time (in seconds) before the Switch polls the SNTP server. The default value is every 1024 seconds (approx. 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.

**LINKSYS**  
A Division of Cisco Systems, Inc.

24-port 10/100 PoE Switch w/4 gigabit ports SRW224G4P

Port Management

Setup Port Management VLAN Management Statistics ACL Security QoS Spanning Tree Multicast More >>

Port Settings Link Aggregation LACP PVE Mapping PoE Power Settings

Port Settings

1 2 Next >>

Port	Description	Administrative Status	Link Status	Speed	Duplex	MDI/MDIX	Flow Control	Type	LAG	Detail
e1		Enabled	Up	100	Full	MDIX	None	100Base-TX		Detail
e2		Enabled	Down	10	Half	MDI	None	100Base-TX		Detail
e3		Enabled	Down	10	Half	MDI	None	100Base-TX		Detail
e4		Enabled	Down	10	Half	MDIX	None	100Base-TX		Detail
e5		Enabled	Down	10	Half	MDI	None	100Base-TX		Detail
e6		Enabled	Down	10	Half	MDI	None	100Base-TX		Detail
e7		Enabled	Down	10	Half	MDIX	None	100Base-TX		Detail
e8		Enabled	Down	10	Half	MDIX	None	100Base-TX		Detail
e9		Enabled	Down	10	Half	MDIX	None	100Base-TX		Detail
e10		Enabled	Down	10	Half	MDIX	None	100Base-TX		Detail
e11		Enabled	Down	10	Half	MDIX	None	100Base-TX		Detail
e12		Enabled	Down	10	Half	MDI	None	100Base-TX		Detail
e13		Enabled	Down	10	Half	MDI	None	100Base-TX		Detail
e14		Enabled	Down	10	Half	MDIX	None	100Base-TX		Detail

Port Management  
Configures ports, trunking, and PoE for the switch system.

Port Settings:  
You can use the Port Settings 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.  
Note that auto-negotiation must be disabled before you can configure or force an interface to use the Speed/Duplex Mode or Flow Control options.

Save Settings Cancel Changes

CISCO SYSTEMS

**Port**—The number of the port. To use an SFP module, click on the **Detail** button of the appropriate port (g1, g2, g3, g4).

**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 menu.

## Port Configuration

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

**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 item to transmit and receive pause frames, or clear it to auto-negotiate the sender and receiver for asymmetric pause frames. (The current switch chip only supports 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 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 Storm Control

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

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

**Mode**—Select the type of traffic storm to control.

**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**.

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

## Port Management Tab—Link Aggregation

The *Port management - Link Aggregation* Screen allows you to create multiple links between switches that work as one, virtual aggregate link.

**Link Aggregation**  
Create Port Channel

LAG	Description	Administrative Status	Type	Link Status	Speed	Duplex	Flow Control	Create	Detail	Delete
1		Enabled					Disabled	Create	Detail	Delete
2		Enabled					Disabled	Create	Detail	Delete
3		Enabled					Disabled	Create	Detail	Delete
4		Enabled					Disabled	Create	Detail	Delete
5		Enabled					Disabled	Create	Detail	Delete
6		Enabled					Disabled	Create	Detail	Delete
7		Enabled					Disabled	Create	Detail	Delete
8		Enabled					Disabled	Create	Detail	Delete

**Link Aggregation:** You can create multiple links between switches that work as one virtual, aggregate link. An aggregate link offers a dramatic increase in bandwidth for network segments where bottlenecks exist, as well as providing a fault-tolerant link between two switches. You can create up to eight aggregate links on the switch. Each aggregate link can contain up to 8 ports. The switch's two Gigabit ports can also be configured as an aggregate link. The ports at both ends of an aggregate link must be configured in an identical manner, including speed, full-duplex mode, flow control, VLAN assignments, and CoS settings.

Save Settings Cancel Changes

**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.

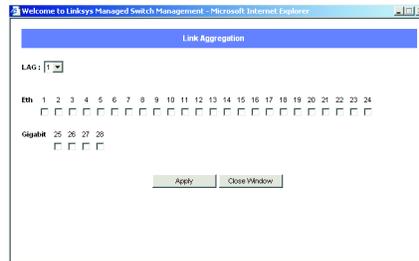
**Link Status**—The link status is displayed here.

**Speed**—The connection speed is displayed here.

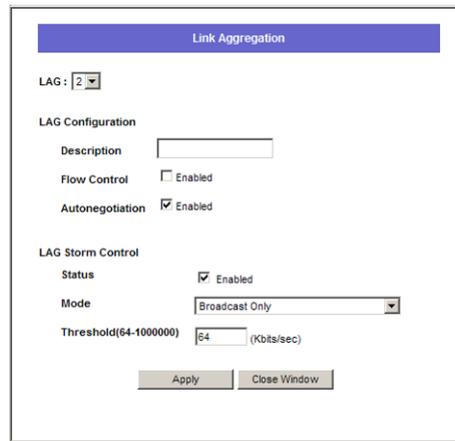
**Duplex**—The connection duplex is displayed here.

**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 button**—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.

The screenshot shows the Linksys web-based utility interface for configuring a 24-port 10/100 PoE Switch. The main navigation bar includes 'Port Management', 'VLAN Management', 'Statistics', 'ACL', 'Security', 'QoS', 'Spanning Tree', 'Multicast', and 'More >>'. The 'Port Management' section is active, with 'Port Settings' selected. The 'LACP' section is expanded, showing 'Global Setting' and 'Port Setting'.

**Global Setting:** System Priority (0-65535) is set to 32768.

**Port Setting:** A table lists 14 ports (e1-e14). Each port is 'Enabled', has 'LACP LAG' set to 1, 'Port Priority' set to 32768, and 'LACP Timeout' set to 'Long'. A 'Set Port Actor' dropdown menu is positioned above the table.

**LACP Note:** The switch supports both static trunking and dynamic Link Aggregation Control Protocol (LACP). Static trunks have to be manually configured at both ends of the link, and the switches must be compatible with the Cisco EtherChannel standard. LACP configured ports can automatically negotiate a trunked link with LACP-configured ports on another device. You can configure any number of ports on the switch as LACP, as long as they are not already configured as part of a static trunk. If ports on another device are also configured as LACP, the switch and the other device will negotiate a trunk link between them. If an LACP trunk consists of more than eight ports, all other ports will be placed in a standby mode. Should one link in the trunk fail, one of the standby ports will automatically be activated to replace it.

Buttons at the bottom: 'Save Settings' and 'Cancel Changes'.

## 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 -PVE Mapping

Use Private VLAN Edge to restrict communications from a downlink port to a single designated uplink port or LAG.

The screenshot shows the Linksys web-based utility interface. The top navigation bar includes 'Port Management' and 'PVE Mapping'. The main content area displays a table for PVE Mapping configuration.

Group ID	Group Members	PVE Uplink
1	e1, e2, e3, e4, e13, e14, e15, e16	None
2	e5, e6, e7, e8, e17, e18, e19, e20	None
3	e9, e10, e11, e12, e21, e22, e23, e24	None
4	g1	None
5	g2	None
6	g3	None
7	g4	None

**PVE Mapping:**  
Use Private VLAN Edge to restrict communication from downlink ports to designated uplink ports or LAG.

**Group ID**—This displays the PVE group number.

**Group Members**—This displays the ports configured in the Group ID. The ports in the group are forwarded as configured in the PVE Uplink field.

**PVE Uplink**—Specifies the port on which the traffic will be forwarded to if PVE is enabled.

## 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.

**LINKSYS**  
A Division of Cisco Systems, Inc.

24-port 10/100 PoE Switch w/4 gigabit ports SRW224G4P

**Port Management**

Setup Port Management VLAN Management Statistics ACL Security QoS Spanning Tree Multicast More >>

Port Settings Link Aggregation LACP PVE Mapping PoE Power Settings

**PoE Power Settings**

Global Setting

Power Allocation (37-180) 180 watts

Port Setting

1 2 Next >>

Port	Admin Status	Priority	Power Allocation (3000-15400 milliwatts)	Mode	Power Consumption (milliwatts)
e1	<input checked="" type="checkbox"/> Enabled	low	15400	off	0
e2	<input checked="" type="checkbox"/> Enabled	low	15400	off	0
e3	<input checked="" type="checkbox"/> Enabled	low	15400	off	0
e4	<input checked="" type="checkbox"/> Enabled	low	15400	off	0
e5	<input checked="" type="checkbox"/> Enabled	low	15400	off	0
e6	<input checked="" type="checkbox"/> Enabled	low	15400	off	0
e7	<input checked="" type="checkbox"/> Enabled	low	15400	off	0
e8	<input checked="" type="checkbox"/> Enabled	low	15400	off	0
e9	<input checked="" type="checkbox"/> Enabled	low	15400	off	0
e10	<input checked="" type="checkbox"/> Enabled	low	15400	off	0
e11	<input checked="" type="checkbox"/> Enabled	low	15400	off	0
e12	<input checked="" type="checkbox"/> Enabled	low	15400	off	0

**PoE Power Settings:**  
The switch can provide DC power to a wide range of connected devices based on the IEEE 802.3af (802.3af) Power-over-Ethernet (PoE) standard. Once configured to supply power, an automatic detection process is initialized by the switch that is authenticated by a PoE signature from the connected device. Detection and authentication prevent damage to non-802.3af compliant devices.

Save Settings Cancel Changes

CISCO SYSTEMS

## Global Setting

**Power Allocation**—Set the appropriate power setting for the switch.

## Port Settings

Select **Enabled** to enable PoE power on selected ports, set the priority using the drop-down menu 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 menu.

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

**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.

The screenshot shows the 'Create VLAN' screen in the Linksys web-based utility. The interface is divided into several sections:

- Navigation:** A top menu bar with 'VLAN Management' selected, and sub-menus for 'Setup', 'Port Management', 'VLAN Management', 'Statistics', 'ACL', 'Security', 'QoS', 'Spanning Tree', and 'Multicast'. Below this, a secondary menu shows 'Create VLAN' as the active option, with other options like 'Port Settings', 'Ports to VLAN', 'VLAN to Ports', and 'GVRP'.
- Left Sidebar:** A 'Create VLAN' section with two options: 'Single Vlan' (selected) and 'VLAN Range'.
- Main Configuration Area:**
  - VLAN ID (1-4094):** A text input field with an 'Add' button next to it.
  - VLAN Name:** A text input field with an 'Add' button next to it.
  - VLAN Range:** Two text input fields separated by a hyphen, with an 'Add Range' button next to them.
  - VLAN Table:** A table with columns 'VLAN ID', 'VLAN Name', and 'Type'. It contains one entry:
 

VLAN ID	VLAN Name	Type
1	DefaultVlan	Static

 Below the table are 'Remove' and 'Cancel' buttons.
- Right Panel:** A 'VLAN Management' section containing explanatory text about VLANs and a 'Create VLAN:' section with instructions on how to use the 'Add' and 'Remove' buttons.

### Single VLAN

**VLAN ID (1-4094)**—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, press 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.

## 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.

The screenshot shows the 'Port Settings' page for a 24-port 10/100 PoE Switch. The table below represents the data shown in the interface:

Port	Mode	Acceptable Frame Type	PVID	Ingress Filtering	LAG
e1	Access	ALL	1	Enabled	
e2	Access	ALL	1	Enabled	
e3	Access	ALL	1	Enabled	
e4	Access	ALL	1	Enabled	
e5	Access	ALL	1	Enabled	
e6	Access	ALL	1	Enabled	
e7	Access	ALL	1	Enabled	
e8	Access	ALL	1	Enabled	
e9	Access	ALL	1	Enabled	
e10	Access	ALL	1	Enabled	
e11	Access	ALL	1	Enabled	
e12	Access	ALL	1	Enabled	
e13	Access	ALL	1	Enabled	
e14	Access	ALL	1	Enabled	

**Port**—The port number included in the VLAN.

**Mode**—Indicates the port mode. Possible values are:

**General**—The port belongs to one or more 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:

**Tagged**—Indicates that only tagged packets are accepted on the port.

**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.

The screenshot shows the 'Ports to VLAN' configuration page for a 24-port 10/100 PoE Switch. The 'Select VLAN' dropdown is set to '1, DefaultVlan,Static'. The 'Eth' section shows 24 ports, with 'Access' mode selected for all. The 'Gigabit' section shows 4 ports, with 'Access' mode selected for all. The 'Membership' section shows 'Untagged' mode selected for all ports. The 'Save Settings' and 'Cancel Changes' buttons are visible at the bottom.

**Select VLAN**—Select the VLAN number. from the drop-down menu.

### Switch Port Mode

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

**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:

**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 assigning VLAN groups to selected interfaces.

The screenshot shows the 'VLAN to Ports' configuration page in the Linksys web-based utility. The page title is '24-port 10/100 PoE Switch w/4 gigabit ports SRW224G4P'. The navigation menu includes 'Setup', 'Port Management', 'VLAN Management', 'Statistics', 'ACL', 'Security', 'QoS', 'Spanning Tree', 'Multicast', and 'More >>'. The 'VLAN Management' sub-menu is active, showing 'Create VLAN', 'Port Settings', 'Ports to VLAN', 'VLAN to Ports', and 'GVRP'. The 'VLAN to Ports' sub-menu is selected, displaying a table for assigning VLAN groups to selected interfaces. The table has columns for 'Port', 'Mode', 'Join VLAN', 'VLANs', and 'LAG'. The 'Join VLAN' column contains 'Join VLAN' buttons, and the 'VLANs' column contains dropdown menus with '1U' selected. The 'Mode' column shows 'Access' for all ports. The 'Port' column lists ports e1 through e14. A sidebar on the right contains the text 'VLAN to Ports: Assigns VLAN groups to selected interfaces.' and the Cisco Systems logo.

Port	Mode	Join VLAN	VLANs	LAG
e1	Access	Join VLAN	1U	
e2	Access	Join VLAN	1U	
e3	Access	Join VLAN	1U	
e4	Access	Join VLAN	1U	
e5	Access	Join VLAN	1U	
e6	Access	Join VLAN	1U	
e7	Access	Join VLAN	1U	
e8	Access	Join VLAN	1U	
e9	Access	Join VLAN	1U	
e10	Access	Join VLAN	1U	
e11	Access	Join VLAN	1U	
e12	Access	Join VLAN	1U	
e13	Access	Join VLAN	1U	
e14	Access	Join VLAN	1U	

**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.

Join VLAN

**Eth 1 : Access Mode (Only join one VLAN with untagged)**

VLAN ID

Apply
Close Window

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.

LINKSYS  
A Division of Cisco Systems, Inc.

24-port 10/100 PoE Switch w/4 gigabit ports SRW224G4P

**VLAN Management**

[Setup](#)
[Port Management](#)
[VLAN Management](#)
[Statistics](#)
[ACL](#)
[Security](#)
[QoS](#)
[Spanning Tree](#)
[Multicast](#)
[More >>](#)

Create VLAN
GVRP

**GVRP**

**GVRP Status**

**GVRP Table**

**GVRP Status**  Enabled

**GVRP Table** 1 2 Next >>

Port	GVRP Status	GARP Join Timer (20-1000 centiseconds)	GARP Leave Timer (60-3000 centiseconds)	GARP LeaveAll Timer (500-16000 centiseconds)	LAG Member
e1	<input type="checkbox"/> Enabled	20	60	0'000	
e2	<input type="checkbox"/> Enabled	20	60	0'000	
e3	<input type="checkbox"/> Enabled	20	60	0'000	
e4	<input type="checkbox"/> Enabled	20	60	0'000	
e5	<input type="checkbox"/> Enabled	20	60	0'000	
e6	<input type="checkbox"/> Enabled	20	60	0'000	
e7	<input type="checkbox"/> Enabled	20	60	0'000	
e8	<input type="checkbox"/> Enabled	20	60	0'000	
e9	<input type="checkbox"/> Enabled	20	60	0'000	
e10	<input type="checkbox"/> Enabled	20	60	0'000	
e11	<input type="checkbox"/> Enabled	20	60	0'000	
e12	<input type="checkbox"/> Enabled	20	60	0'000	
e13	<input type="checkbox"/> Enabled	20	60	0'000	
e14	<input type="checkbox"/> Enabled	20	60	0'000	

**GVRP:**  
 GVRP defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network. VLANs are dynamically configured based on join messages issued by host devices and propagated throughout the network. GVRP must be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.  
**GVRP Status:** Sets GVRP for the interface. When disabled, any GVRP packets received on this port are discarded and no GVRP registrations are propagated from other ports.  
**GVRP Table:** GARP is used by GVRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GVRP registration/deregistration.

Cisco Systems

Save Settings Cancel Changes

**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.

**Port**—Displays the interface number.

**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.

Interface Statistics	
Drop Events	0
Received Bytes	746269E
Received Packets	2622E
Broadcast Packets Received	1208E
Multicast Packets Received	5777
CRC & Align Errors	C
Undersize Packets	C
Oversize Packets	C
Fragments	C
Jabbers	C
Collisions	C
Frame of 64 Bytes	821C
Frame of 65 to 127 Bytes	12371
Frame of 128 to 255 Bytes	313
Frame of 256 to 511 Bytes	152E
Frame of 512 to 1023 Bytes	2E
Frame of 1024 to 1518 Bytes	3782

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

**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**—Defines the specific port 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 button**—This option will reset all of the statistic counts.

**Query button**—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.

The screenshot shows the Linksys web-based utility interface for a 24-port 10/100 PoE Switch. The 'Statistics' tab is active, and the 'RMON History' sub-tab is selected. The 'History Control Table' section includes the following fields and values:

- Source Interface:
- Port:
- Sampling Interval (1-3600 sec):
- Sampling Requested (1-65535):
- Owner (0-127):

The 'Add' button is located below these fields. The table below shows the current entries in the History Control Table:

Index	Source Interface	Sampling Request	Sampling Interval	Owner
1	Eth1	8	1800	
2	Eth1	8	30	
3	Eth2	8	1800	
4	Eth2	8	30	
5	Eth3	8	1800	
6	Eth3	8	30	
7	Eth4	8	1800	
8	Eth4	8	30	
9	Eth5	8	1800	
10	Eth5	8	30	
11	Eth6	8	1800	
12	Eth6	8	30	
13	Eth7	8	1800	
14	Eth7	8	30	
15	Eth8	8	1800	

Below the table are 'Remove' and 'Cancel' buttons. At the bottom of the screen is a 'View History Table' button.

### History Control Table

**Source Interface**—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)

The **Add** button adds the configured RMON sampling to the Log Table at the bottom of the screen.

## History Table

**View History Table button**—This button opens the *History Table* screen.

Index	Sample Index	Interval Start	Description	Octets	Packets	Broadcast Packets	Multicast Packets	CRCA Align Errors	Undersize Packets	Oversize Packets	Fragments	Jabbers	Collisions	Utilization
2	34	104200	0	10002	247	0	0	0	0	0	0	0	0	
2	37	109200	0	11600	151	1	0	0	0	0	0	0	0	
2	38	112200	0	6002	97	0	0	0	0	0	0	0	0	
2	39	115200	0	64	1	1	0	0	0	0	0	0	0	
2	40	118200	0	16639	218	0	0	0	0	0	0	0	0	
2	41	121200	0	14294	187	1	0	0	0	0	0	0	0	
2	42	124200	0	0	0	0	0	0	0	0	0	0	0	
2	43	127200	0	7159	92	15	0	0	0	0	0	0	0	
4	26	104200	0	0	0	0	0	0	0	0	0	0	0	
4	37	109200	0	0	0	0	0	0	0	0	0	0	0	
4	38	112200	0	0	0	0	0	0	0	0	0	0	0	
4	39	115200	0	0	0	0	0	0	0	0	0	0	0	
4	40	118200	0	0	0	0	0	0	0	0	0	0	0	
4	41	121200	0	0	0	0	0	0	0	0	0	0	0	
4	42	124200	0	0	0	0	0	0	0	0	0	0	0	

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 Alarms

The *RMON Alarms* 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 RMON 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 screenshot shows the Linksys web-based utility interface for configuring RMON Alarms. The main configuration area includes the following fields:

- Interface:** Port e1
- Statistics:** Drop Events
- Interval (secs):** 0
- Sample Type:** Absolute
- Startup Alarm:** Rising
- Rising Threshold:** (empty field)
- Falling Threshold:** (empty field)
- Rising Event Index (0-65535):** (empty field)
- Falling Event Index (0-65535):** (empty field)
- Owner (0-127):** (empty field)

Below the configuration fields is a table of RMON Alarms:

Interface	Statistics	Interval	Sample Type	Value	Startup Alarm
Eth1	Broadcast Packets Received	30	Delta	40	R or F
Eth2	Broadcast Packets Received	30	Delta	0	R or F
Eth3	Broadcast Packets Received	30	Delta	0	R or F
Eth4	Broadcast Packets Received	30	Delta	0	R or F
Eth5	Broadcast Packets Received	30	Delta	0	R or F
Eth6	Broadcast Packets Received	30	Delta	0	R or F
Eth7	Broadcast Packets Received	30	Delta	0	R or F
Eth8	Broadcast Packets Received	30	Delta	0	R or F
Eth9	Broadcast Packets Received	30	Delta	0	R or F
Eth10	Broadcast Packets Received	30	Delta	0	R or F
Eth11	Broadcast Packets Received	30	Delta	0	R or F
Eth12	Broadcast Packets Received	30	Delta	0	R or F

Buttons for 'Remove' and 'Cancel' are located at the bottom of the table.

The Alarm Control Table allows you to add, update and delete specific index entries.

**Interface**— The selected interface on the Switch.

**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**—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**—The index of the Event that will be used if a rising 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.

**Falling Event Index**—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**—Displays an index for the 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.

The screenshot shows the Linksys web-based utility interface for configuring RMON Events. The top navigation bar includes 'Statistics' and various configuration tabs like 'Setup', 'Port Management', 'VLAN Management', 'ACL', 'Security', 'QoS', 'Spanning Tree', 'Multicast', and 'More >>'. The 'RMON Events' tab is selected, and the 'Event Setting' section is active. The form contains the following fields:

- Event Description (0-127)**: A text input field.
- Type**: A dropdown menu currently set to 'none'.
- Community (0-127)**: A text input field.
- Owner (0-127)**: A text input field.

Below the form is an **Add** button. Underneath is a table with the following columns: Index, Description, Type, Community, Last Time Sent, and Owner. The table is currently empty. Below the table are **Remove** and **Cancel** buttons. At the bottom of the main content area is a **View Log Table** button. On the right side, there is a sidebar with the following text:

**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. If the response corresponding to an alarm has not yet been defined, use the RMON Event screen to configure the Event Setting table. The Log Table shows the log index number, the time of an event, and the description of the event that activated the entry.

At the bottom of the page, there are **Save Settings** and **Cancel Changes** buttons.

### 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.

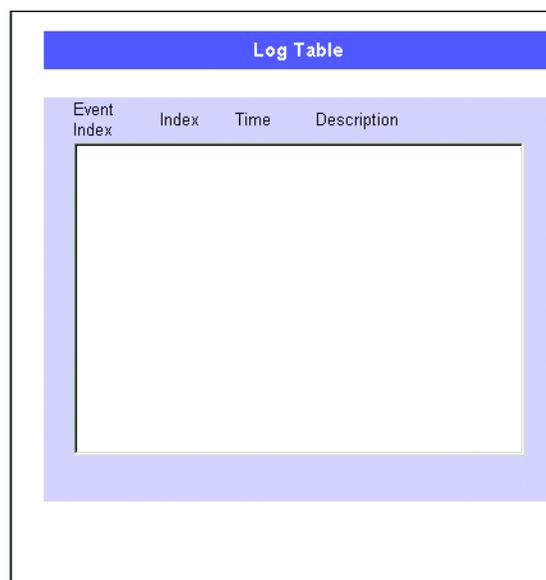
**Owner**—Displays the device or user that defined the event. (Maximum 127 characters).

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.

### Log Table

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.

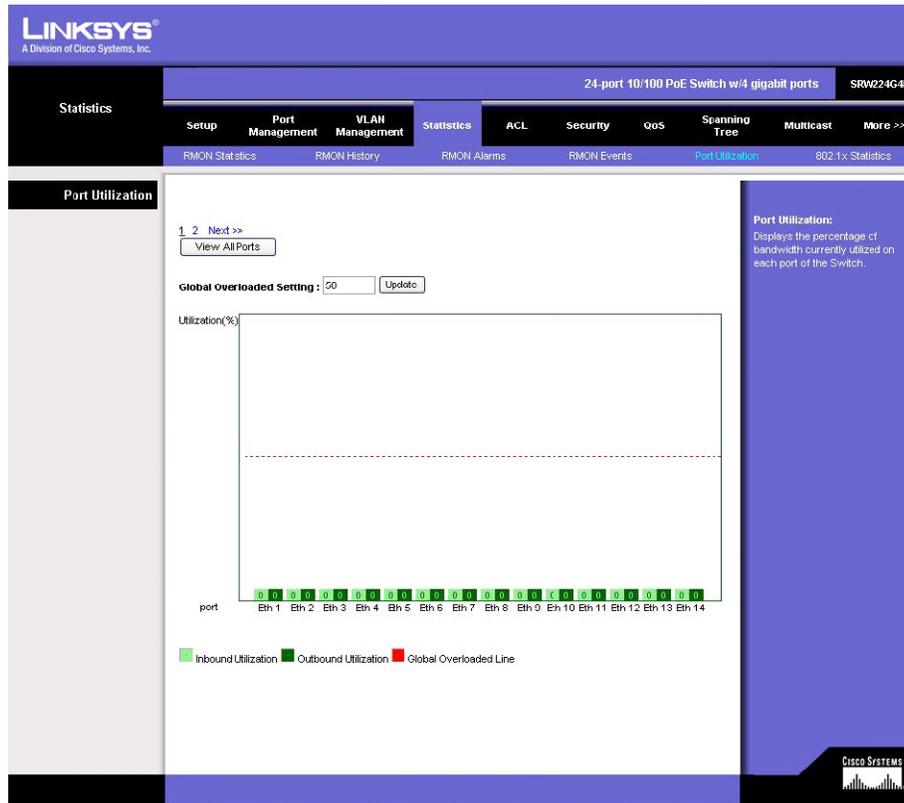


Log Table			
Event Index	Index	Time	Description

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**—Indicates the overload boundary marked in the utilization graphs, above which ports are consuming an excessive amount of resources.

## Statistics Tab—802.1x Statistics

The *802.1X Statistics* screen contains information about EAP packets received on a specific port.

The screenshot shows the Linksys web-based utility interface for a 24-port 10/100 PoE Switch. The 'Statistics' tab is active, and the '802.1x Statistics' sub-tab is selected. The interface includes a 'Refresh Rate' dropdown menu set to 'No Refresh' and an 'Interface' dropdown menu set to 'e1'. A 'Query' button is present below the interface selection. The main content area displays a table of 802.1x statistics for interface e1, with columns for Name, Description, and Packet count. The table lists various statistics such as Received EAPOL Start, Received EAPOL Logoff, Received EAPOL Invalid, Received EAPOL Total, Received EAP Resp/Id, Received EAP Resp/oth, Received EAP LenError, Received Last EAPOL Ver, Received Last EAPOL Src, Transmit EAPOL Total, Transmit EAPOL/Id, and Transmit EAPOL/oth. The Packet column shows values of 0 for most statistics, except for 'Received Last EAPOL Src' which shows '00-00-00-00-00-00' and 'Transmit EAPOL Total' which shows '1'. A 'Cisco Systems' logo is visible in the bottom right corner of the interface.

Name	Description	Packet
Received EAPOL Start	The number of EAPOL Start frames that have been received by this Authenticator	0
Received EAPOL Logoff	The number of EAPOL Logoff frames that have been received by this Authenticator	0
Received EAPOL Invalid	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized	0
Received EAPOL Total	The number of valid EAPOL frames of any type that have been received by this Authenticator	0
Received EAP Resp/Id	The number of EAP Resp/Id frames that have been received by this Authenticator	0
Received EAP Resp/oth	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator	0
Received EAP LenError	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid	0
Received Last EAPOL Ver	The protocol version number carried in the most recently received EAPOL frame	0
Received Last EAPOL Src	The source MAC address carried in the most recently received EAPOL frame	00-00-00-00-00-00
Transmit EAPOL Total	The number of EAPOL frames of any type that have been transmitted by this Authenticator	1
Transmit EAPOL/Id	The number of EAP Req/Id frames that have been transmitted by this Authenticator	0
Transmit EAPOL/oth	The number of EAP Request frames (other than Req/Id frames) that have been transmitted by this Authenticator	0

**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.
- **3 Sec**—Indicates that the EAP statistics are refreshed every 3 seconds.
- **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.

To view the statistics for a port, select the required interface from the drop-down menu and click **Query**.

**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), IPv6 frames, 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.

**LINKSYS**  
A Division of Cisco Systems, Inc.

24-port 10/100 PoE Switch w/4 gigabit ports SRW24G4P

ACL

Setup Port Management VLAN Management Statistics ACL Security QoS Spanning Tree Multicast More >>

IP based ACL IPv6 based ACL MAC based ACL TCAM Utilization

**IP based ACL**  
Add ACL/ACE

**Target**

ACL Name ===  New ACL Name

**Action**

Permit  Deny

**Protocol**

Select from list ANY  Protocol ID to Match

**TCP Flags**

Urg  Ack  Psh  Rst  Syn  Fin

**Source Port**

**Destination Port**

**Source IP Address**  Wildcard Mask   Any

**Dest. IP Address**  Wildcard Mask   Any

**Match CoS**

DSCP(0-63)  IP Precedence (0-7)

Action	Source	Destination	CoS	Pro- to- col	Src Port	Dst Port	TCP Flags
(none)	IP Address/Wildcard Mask	IP Address/Wildcard Mask	Prece- dence/DSCP				

**ACL**

An ACL is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. The switch tests ingress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match for a list of all permit rules, the packet is dropped, and if no rules match for a list of all deny rules, the packet is accepted. Each ACL can have up to 32 rules and the maximum number of ACLs is 32. To filter incoming packets, first create an ACL, add the required rules and then bind the ACL to specific ports.

CISCO SYSTEMS

**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 dropdown menu.

- **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.

**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.
- **IPv6**—Indicates that IP Version 6 (IPv6) packet types is used to classify network flows.
- **OSPF**—Matches the packet to the Open Shortest Path First (OSPF) protocol.
- **RIP**—Matches the packet to the Routing Information Protocol (RIP).
- **RTP**—Indicates that Real-time Transport Protocol (RTP) is used to classify network flows.
- **TCP**—Indicates that the Transmission Control Protocol is used to classify network flows.
- **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.
- 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**—Port number for the specified protocol type. The possible field range is 0—65535.

**Destination Port**—Port number for the specified protocol type. 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.

**Dest. 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 CoS**—Either the DSCP value or the IP Precedence value is used to match packets to ACLs.

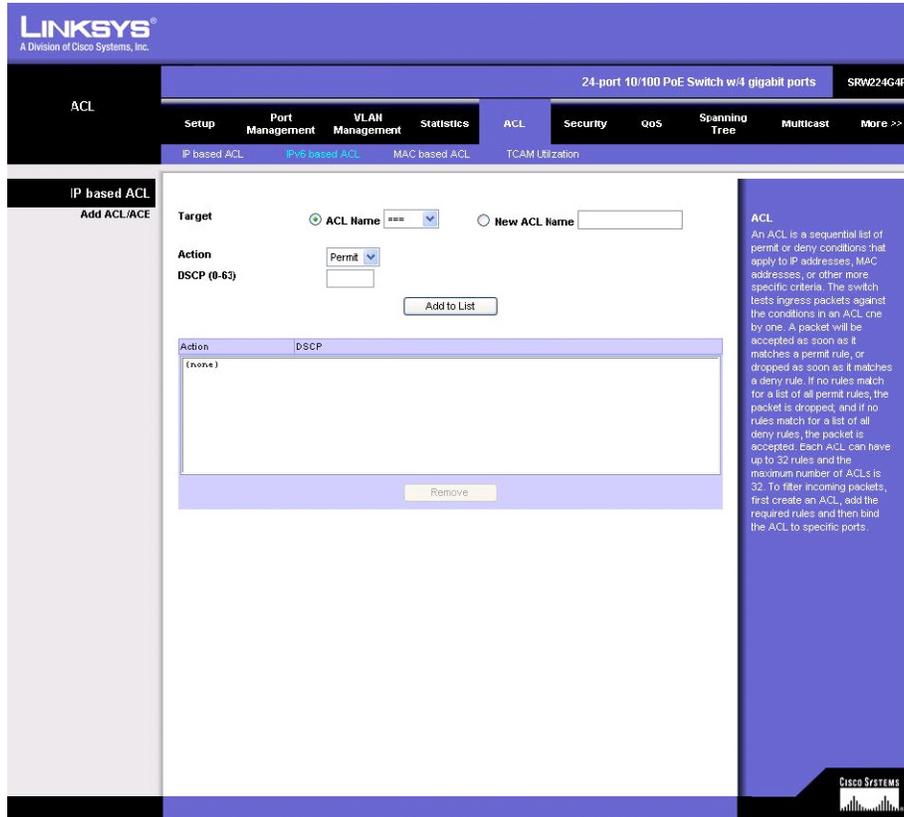
**DSCP**—Matches the packet DSCP value to the ACE. The possible field range is 0-63.

**IP Precedence**—Matches the packet IP Precedence value to the ACE. 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 dropdown menu.

- **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 which meet the ACL criteria.
- **Deny**—Drops packets which meet the ACL criteria.

**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.

**Dest. 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.

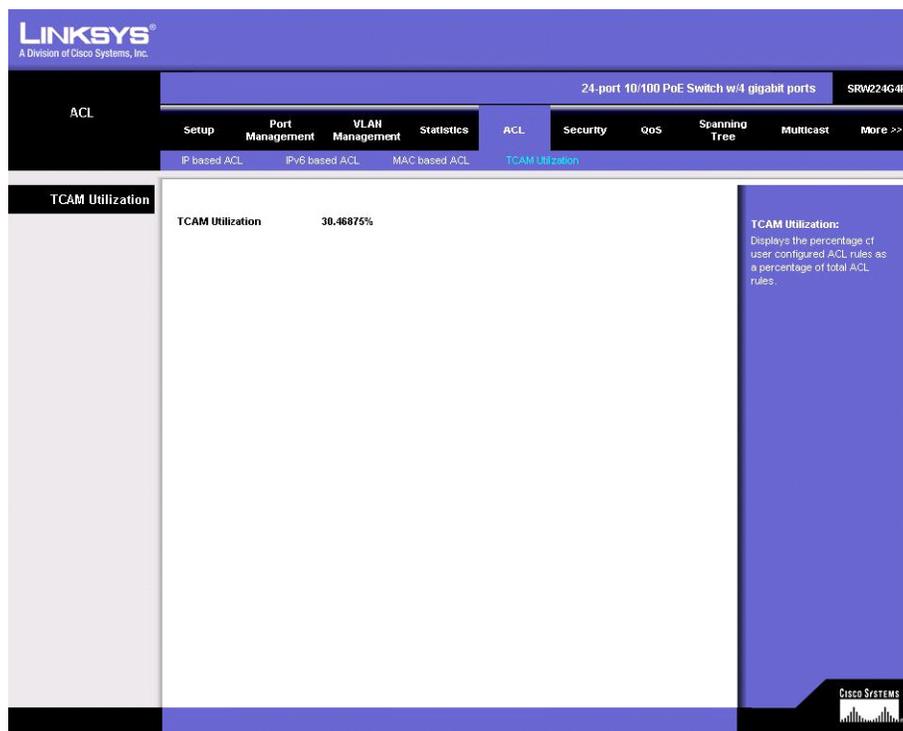
**Ethernet Type**—Specifies the packet's Ethernet type. This option can only be used to filter Ethernet II formatted packets. (Range: 0-65535) A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), 8137 (IPX)

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

Mark the Enable checkbox for the port you want to bind to an ACL. Select the required ACL from the drop-down menu.

The screenshot shows the Linksys web-based utility interface for configuring ACL Binding. The main content area is titled "ACL Binding" and contains a table with the following structure:

Port	IP (Input)	MAC (Input)
e1	<input checked="" type="checkbox"/> Enabled (none)	<input checked="" type="checkbox"/> Enabled (none)
e2	<input checked="" type="checkbox"/> Enabled (none)	<input checked="" type="checkbox"/> Enabled (none)
e3	<input checked="" type="checkbox"/> Enabled (none)	<input checked="" type="checkbox"/> Enabled (none)
e4	<input checked="" type="checkbox"/> Enabled (none)	<input checked="" type="checkbox"/> Enabled (none)
e5	<input checked="" type="checkbox"/> Enabled (none)	<input checked="" type="checkbox"/> Enabled (none)
e6	<input checked="" type="checkbox"/> Enabled (none)	<input checked="" type="checkbox"/> Enabled (none)
e7	<input checked="" type="checkbox"/> Enabled (none)	<input checked="" type="checkbox"/> Enabled (none)
e8	<input checked="" type="checkbox"/> Enabled (none)	<input checked="" type="checkbox"/> Enabled (none)
e9	<input checked="" type="checkbox"/> Enabled (none)	<input checked="" type="checkbox"/> Enabled (none)
e10	<input checked="" type="checkbox"/> Enabled (none)	<input checked="" type="checkbox"/> Enabled (none)
e11	<input checked="" type="checkbox"/> Enabled (none)	<input checked="" type="checkbox"/> Enabled (none)
e12	<input checked="" type="checkbox"/> Enabled (none)	<input checked="" type="checkbox"/> Enabled (none)
e13	<input checked="" type="checkbox"/> Enabled (none)	<input checked="" type="checkbox"/> Enabled (none)
e14	<input checked="" type="checkbox"/> Enabled (none)	<input checked="" type="checkbox"/> Enabled (none)

The interface also includes a "Security" sidebar on the right with the following text:

**Security**  
The Security tab provides configuration for ACL port binding, authentication servers, IEEE 802.1X, port security, HTTPS management, IP filtering, dynamic VLAN configuration, network access based on host MAC address, and SSH.

**ACL Binding:**  
After configuring ACLs, you can bind them to the ports that need to filter traffic. The switch only supports ACLs for ingress filtering. You can only bind one IP ACL and one MAC ACL to any port for ingress filtering.

At the bottom of the page, there are "Save Settings" and "Cancel Changes" buttons.

**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 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.

**Authentication Servers**

**RADIUS Server Settings**

Index	Server IP Address	Server Port Number (1-65535)	Secret Key String	Number of Retries (1-30)	Timeout for Reply (1-65535 sec)
Global		1812		2	5
1					
2					
3					
4					
5					

**TACACS Server Settings**

Index	Server IP Address	Server Port Number (1-65535)	Secret Key String
1		49	

**Authentication Servers:** Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) are login authentication protocols that use software running on a central server to control access to RADIUS-aware or TACACS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user that requires management access to the switch. By default, management access is always checked against the authentication database stored on the local switch. If a remote authentication server is used, you must specify the authentication sequence and the corresponding parameters for the remote authentication protocol. Local and remote login authentication control management access via the console port, web browser, or Telnet.

More ...

Save Settings Cancel Changes

## RADIUS Server Setting

**Index**—Indicates the server number or global setting.

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

**Server Port Number (1-65535)**—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 (1-65535 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.)

LINKSYS®  
A Division of Cisco Systems, Inc.

24-port 10/100 PoE Switch w/4 gigabit ports SRW224G4P

Security

Setup Port Management VLAN Management Statistics ACL Security QoS Spanning Tree Multicast More >>

ACL Binding Authentication Servers 802.1x Settings Port Security HTTPS Settings More >>

802.1x Settings

Authentication Type  Disabled  RADIUS

802.1x System Authentication: Disabled

1 2 Next >>

Port	Operation Mode	Maximum Count (1-1024)	Mode	Authorized	Supplicant	LAG	Detail
e1	Single-Host	5	Force-Authorized	No	00-00-00-00-00-00	00-00-00-00-00-00	Detail
e2	Single-Host	5	Force-Authorized		00-00-00-00-00-00	00-00-00-00-00-00	Detail
e3	Single-Host	5	Force-Authorized		00-00-00-00-00-00	00-00-00-00-00-00	Detail
e4	Single-Host	5	Force-Authorized		00-00-00-00-00-00	00-00-00-00-00-00	Detail
e5	Single-Host	5	Force-Authorized		00-00-00-00-00-00	00-00-00-00-00-00	Detail
e6	Single-Host	5	Force-Authorized		00-00-00-00-00-00	00-00-00-00-00-00	Detail
e7	Single-Host	5	Force-Authorized		00-00-00-00-00-00	00-00-00-00-00-00	Detail
e8	Single-Host	5	Force-Authorized		00-00-00-00-00-00	00-00-00-00-00-00	Detail
e9	Single-Host	5	Force-Authorized		00-00-00-00-00-00	00-00-00-00-00-00	Detail
e10	Single-Host	5	Force-Authorized		00-00-00-00-00-00	00-00-00-00-00-00	Detail
e11	Single-Host	5	Force-Authorized		00-00-00-00-00-00	00-00-00-00-00-00	Detail
e12	Single-Host	5	Force-Authorized		00-00-00-00-00-00	00-00-00-00-00-00	Detail
e13	Single-Host	5	Force-Authorized		00-00-00-00-00-00	00-00-00-00-00-00	Detail
e14	Single-Host	5	Force-Authorized		00-00-00-00-00-00	00-00-00-00-00-00	Detail

802.1x Settings:  
The IEEE 802.1X (802.1X) 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 RADIUS server, which means that authorized users can use the same credentials for authentication from any point within the network. Each client that needs to be authenticated must have 802.1x client software installed and properly configured. The RADIUS server and 802.1x client also have to support the same Extensible Authentication Protocol (EAP) authentication type - MD5. Note that the 802.1X protocol must first be enabled globally for the switch system before port settings are active.

More...

Save Settings Cancel Changes

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.

**LAG**—Indicates if the port is a member of a LAG. If it is a member of a LAG, it cannot be configured to use 802.1X port authentication.

Modify the parameters required using the drop-down menus 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 **Apply** to apply the changes.

## 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.

The screenshot shows the Linksys web-based utility interface for a 24-port 10/100 PoE Switch. The main navigation menu includes Setup, Port Management, VLAN Management, Statistics, ACL, Security, QoS, Spanning Tree, Multicast, and More. The Security tab is active, and the Port Security configuration page is displayed. The page shows a table of port configurations with columns for Port, Name, Action, Security Status, Maximum MAC Count (0-1024), and LAG. The table lists ports e1 through e14, all with Action set to None, Security Status set to Enabled, and Maximum MAC Count set to 0. A detailed explanation of Port Security is provided on the right side of the page.

Port	Name	Action	Security Status	Maximum MAC Count (0-1024)	LAG
e1		None	<input type="checkbox"/> Enabled	0	
e2		None	<input type="checkbox"/> Enabled	0	
e3		None	<input type="checkbox"/> Enabled	0	
e4		None	<input type="checkbox"/> Enabled	0	
e5		None	<input type="checkbox"/> Enabled	0	
e6		None	<input type="checkbox"/> Enabled	0	
e7		None	<input type="checkbox"/> Enabled	0	
e8		None	<input type="checkbox"/> Enabled	0	
e9		None	<input type="checkbox"/> Enabled	0	
e10		None	<input type="checkbox"/> Enabled	0	
e11		None	<input type="checkbox"/> Enabled	0	
e12		None	<input type="checkbox"/> Enabled	0	
e13		None	<input type="checkbox"/> Enabled	0	
e14		None	<input type="checkbox"/> Enabled	0	

**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. Note that when a port is disabled (shut down) due to a security violation, it must be manually re-enabled from the Port Configuration screen.

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 age out. 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, and set the maximum number of MAC addresses allowed on a port.

Disabled ports are activated from the Port Security page.

**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. When the mode is changed, the Lock Interface can be reinstated.

Click **Save Settings** 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.

The screenshot shows the Linksys web interface for a 24-port 10/100 PoE Switch. The 'Security' tab is selected, and the 'HTTPS Settings' sub-tab is active. The 'HTTPS Status' is set to 'Enabled' with a checked checkbox. The 'Change HTTPS Port Number (1-65535)' is set to '443'. A 'Save Settings' button and a 'Cancel Changes' button are at the bottom. A help text box on the right explains the HTTPS settings.

**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. Both the HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure both services to use the same UDP port. If you change the default HTTPS port number, clients attempting to connect to the HTTPS server must specify the port number in the URL in this format: https://device.port\_number

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

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

## Security Tab—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 screenshot shows the Linksys web interface for configuring the Management ACL. The top navigation bar includes 'Security' and various management options. The main content area is titled 'Management ACL' and is divided into three sections: Web IP Filtering, SNMP IP Filtering, and Telnet IP Filtering. Each section has input fields for 'Start IP Address' and 'End IP Address', an 'Add' button, and a list of entries with 'Remove' buttons. A right-hand sidebar contains a 'Management ACL' help text explaining the configuration process.

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

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 screenshot shows the Linksys web-based utility interface. At the top, it identifies the device as a "24-port 10/100 PoE Switch w/4 gigabit ports" (SRW224G4P). The navigation menu includes "Security", "QoS", "Spanning Tree", and "Multicast". The "Security" tab is active, and the "Dynamic VLAN" sub-tab is selected. The main content area displays a table for configuring Dynamic VLAN settings for ports e1 through e14. Each port has a checkbox for "Dynamic VLAN" (all are checked) and a "LAG Member" column. A "Configuration" sidebar on the left shows "1 2 Next >>". A "Dynamic VLAN" help text box on the right explains the feature. At the bottom, there are "Save Settings" and "Cancel Changes" buttons.

Port	Dynamic VLAN	LAG Member
e1	<input checked="" type="checkbox"/> Enabled	
e2	<input checked="" type="checkbox"/> Enabled	
e3	<input checked="" type="checkbox"/> Enabled	
e4	<input checked="" type="checkbox"/> Enabled	
e5	<input checked="" type="checkbox"/> Enabled	
e6	<input checked="" type="checkbox"/> Enabled	
e7	<input checked="" type="checkbox"/> Enabled	
e8	<input checked="" type="checkbox"/> Enabled	
e9	<input checked="" type="checkbox"/> Enabled	
e10	<input checked="" type="checkbox"/> Enabled	
e11	<input checked="" type="checkbox"/> Enabled	
e12	<input checked="" type="checkbox"/> Enabled	
e13	<input checked="" type="checkbox"/> Enabled	
e14	<input checked="" type="checkbox"/> Enabled	

**Dynamic VLAN:**  
Enables 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.

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.

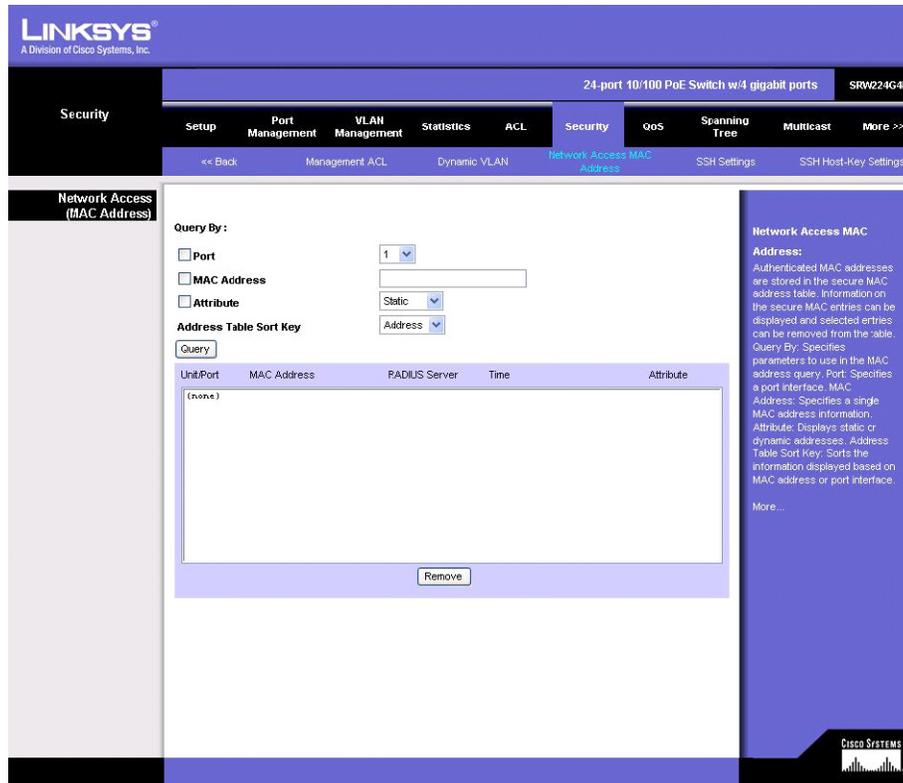
If dynamic VLAN assignment is enabled on a port and the RADIUS server returns no VLAN configuration, the authentication is still treated as a success, and the host assigned to the default untagged VLAN.

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

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

## 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.

The screenshot shows the Linksys web-based utility interface for configuring SSH settings on a 24-port 10/100 PoE Switch w/4 gigabit ports (SRW224G4P). The navigation menu includes Setup, Port Management, VLAN Management, Statistics, ACL, Security, QoS, Spanning Tree, and Multicast. The breadcrumb trail is: << Back >> Management ACL > Dynamic VLAN > Network Access MAC Address > SSH Settings. The main content area is titled 'SSH Settings' and contains the following configuration options:

SSH Server Status	<input type="checkbox"/> Enabled
Version	2.0
SSH Authentication Timeout (1-120)	120 seconds
SSH Authentication Retries (1-5)	3
SSH Server-Key Size (512-896)	768

At the bottom of the page, there are 'Save Settings' and 'Cancel Changes' buttons. A help sidebar on the right provides information about SSH settings, including a note that an SSH client must be installed on the management station to access the switch via SSH.

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)

## Security Tab—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.

The screenshot shows the Linksys web-based utility interface for configuring a 24-port 10/100 PoE Switch. The 'Security' tab is active, and the 'SSH Host-Key Settings' page is displayed. The 'Public-Key of Host-Key' section contains two key pairs: RSA and DSA. The RSA key pair is selected, showing a size of 1024 bits and a public exponent of 65537. The DSA key pair is also visible, showing a size of 1024 bits and a public exponent of 65537. The 'Host-Key Type' is set to 'Both'. There are buttons for 'Generate' and 'Clear'.

**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. 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.

**LINKSYS**  
A Division of Cisco Systems, Inc.

24-port 10/100 PoE Switch w/4 gigabit ports SRW224G4P

QoS

Setup Port Management VLAN Management Statistics ACL Security QoS Spanning Tree Multicast More >>

CoS Settings Queue Settings DSCP Settings DiffServ Settings DiffServ Port Binding Bandwidth

**CoS Settings**  
CoS to Queue

Class of Service	Queue (1-4)
0	2 (1-4)
1	1 (1-4)
2	1 (1-4)
3	2 (1-4)
4	3 (1-4)
5	3 (1-4)
6	4 (1-4)
7	4 (1-4)

Restore Default

1 2 Next >>

Port	Default CoS (0-7)	LAG
e1	0	
e2	0	
e3	0	
e4	0	
e5	0	
e6	0	
e7	0	
e8	0	
e9	0	
e10	0	

**QoS**  
Quality of Service (QoS) allows you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. The switch supports Class of Service (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.

**CoS Settings:**  
The switch processes CoS priority tagged traffic by using the four priority queues for each port, with service schedules based on strict or Weighted Round Robin (WRR).

More ...

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 value)

**Queue (1-4)**—The output priority queue. (Range: 1-4, where 4 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	Strict Priority	WRR	Scheduling	
			WRR Weight	% of WRR Bandwidth
1	<input type="radio"/>	<input checked="" type="radio"/>	1	7%
2	<input type="radio"/>	<input checked="" type="radio"/>	2	13%
3	<input type="radio"/>	<input checked="" type="radio"/>	4	27%
4	<input type="radio"/>	<input checked="" type="radio"/>	8	53%

Note: The WRR weight value is just an information and can not be changed.

**Queue Settings:**  
You can set the switch to service the queues based on a strict rule that requires all traffic in a higher priority queue to be transmitted before lower priority queues are serviced, or use Weighted Round-Robin (WRR) queuing that specifies a relative weight of each queue. WRR uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. Note that the queue weighting is fixed for the Switch and cannot be configured.

**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 Class of Service value by the Switch and the traffic 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.

The screenshot shows the Linksys web-based utility interface for a 24-port 10/100 PoE Switch. The 'QoS' tab is selected, and the 'DSCP Settings' sub-tab is active. The 'DSCP Priority Status' checkbox is checked (Enabled). Below it is a 'Restore Default' button. A table maps DSCP values (0-15) to CoS values (0-7). The table has columns for DSCP and CoS, with each cell containing a dropdown menu.

DSCP	CoS	DSCP	CoS	DSCP	CoS	DSCP	CoS
0	0	16	2	32	4	48	6
1	0	17	0	33	0	49	0
2	0	18	3	34	4	50	0
3	0	19	0	35	0	51	0
4	0	20	3	36	4	52	0
5	0	21	0	37	0	53	0
6	0	22	3	38	5	54	0
7	0	23	0	39	0	55	0
8	1	24	3	40	5	56	7
9	0	25	0	41	0	57	0
10	2	26	4	42	5	58	0
11	0	27	0	43	0	59	0
12	2	28	4	44	0	60	0
13	0	29	0	45	0	61	0
14	2	30	4	46	7	62	0
15	0	31	0	47	0	63	0

Buttons at the bottom: Save Settings, Cancel Changes.

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.

The screenshot shows the Linksys web-based utility interface for configuring DiffServ settings on a 24-port 10/100 PoE Switch. The navigation menu includes Setup, Port Management, VLAN Management, Statistics, ACL, Security, QoS, Spanning Tree, Multicast, and More. The QoS tab is selected, and the DiffServ Settings sub-tab is active. The interface is split into two main areas: Class Map and Policy Map. The Class Map section has input fields for Class Name, Type (set to 'match-any'), and Description, followed by an 'Add' button. Below this is a table with columns for Class Name, Type, and Description, showing a single entry '(none)'. The Policy Map section has input fields for Policy Name and Description, followed by an 'Add' button. Below this is a table with columns for Policy Name and Description, showing a single entry '(none)'. A sidebar on the right provides a 'DiffServ Settings' overview and a 'More...' link.

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)

**Type**—Only one match command is permitted per class map, so the match-any field refers to the criteria specified by the lone match command.

**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.

**Remove**—Removes the selected class from the list.

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

The screenshot shows a web utility window titled "Edit Class Element". At the top, there is a blue header bar with the title. Below the header, the "Class Name" field contains the text "a". The "Class Rule" field contains a dropdown menu with "ACL" selected and another dropdown menu with "a" selected. Below these fields is an "Add" button. A large light blue rectangular area is highlighted, containing a "Class Rule" section with a text area that has "ACL a" entered. Below this text area is a "Remove" button. At the bottom of the highlighted area is a "Close Window" button.

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 menu, then click **Add**.

**Class Rule**—Edits the rules for the class by specifying the type of traffic based on an access list.

**ACL**—Name of an access control list. Any type of ACL can be specified, including IP ACLs, IPv6 ACLs, and MAC ACLs. (Range: 1-16 characters)

**Add**—Adds the specified criteria to the class. One or more ACLs may be specified 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)

**Add**—Creates a new policy using the entered policy name and description.

**Remove**—Removes the selected policy from the list.

**Edit Policy Element**—Configures a policy for traffic that matches criteria defined in this class by setting the quality of service that an IP packet will receive (in the Action field), defining the maximum throughput and burst rate (in the Meter field), and the action that results from a policy violation (in the Exceed Action field).

Class Name	Action	Meter Rate (kbit)	Burst (byte)	Exceed Action
(none)				

**Class Name**—Name of class map. Use the drop-down menu 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 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 (bytes)**—Burst in bytes. (Range: 64-1522)

**Exceed Action**—Specifies whether the traffic that exceeds the specified rate or burst will be dropped or the DSCP service level will be reduced.

**Set**—Decreases DSCP priority for out of conformance 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 menus 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, set an ACL mask to match the criteria defined in the class map, then define a policy map, and finally bind the service policy to the required interface. You can only bind one policy map to an interface. The current firmware does not allow you to bind a policy map to an egress queue.

The screenshot shows the Linksys web-based utility interface for configuring DiffServ Port Binding. The page title is "DiffServ Port Binding" and it is part of the "QoS" tab. The interface includes a navigation menu with options like "Setup", "Port Management", "VLAN Management", "Statistics", "ACL", "Security", "QoS", "Spanning Tree", "Multicast", and "More >>". The "QoS" tab is selected, and the "DiffServ Port Binding" sub-tab is active. The main content area shows a table with columns "Port" and "Ingress". The "Port" column lists ports e1 through e14. The "Ingress" column contains a checkbox and a dropdown menu for each port, all currently set to "(none)". To the left of the table is a "Service Policy" section, and to the right is a "DiffServ Port Binding" description: "Binds a policy map to the ingress queue of a particular interface. You can only bind one policy map to an interface. The switch only allows you to bind a policy map to an ingress queue." At the bottom of the page, there are "Save Settings" and "Cancel Changes" buttons.

Port	Ingress
e1	<input type="checkbox"/> (none)
e2	<input type="checkbox"/> (none)
e3	<input type="checkbox"/> (none)
e4	<input type="checkbox"/> (none)
e5	<input type="checkbox"/> (none)
e6	<input type="checkbox"/> (none)
e7	<input type="checkbox"/> (none)
e8	<input type="checkbox"/> (none)
e9	<input type="checkbox"/> (none)
e10	<input type="checkbox"/> (none)
e11	<input type="checkbox"/> (none)
e12	<input type="checkbox"/> (none)
e13	<input type="checkbox"/> (none)
e14	<input type="checkbox"/> (none)

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

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 into the Switch. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

**LINKSYS**  
A Division of Cisco Systems, Inc.

24 port 10/100 PoE Switch w/4 gigabit ports SRW224G4P

QoS

Setup Port Management VLAN Management Statistics ACL Security QoS Spanning Tree Multicast More >>

CoS Settings Queue Settings DSCP Settings DiffServ Settings DiffServ Port Binding **Bandwidth**

**Bandwidth**

1 2 Next >>

Port	Ingress Rate Limit		Egress Shaping			LAG
	Status	Rate Limit (Kbits/sec)	Status	CIR (Kbits/sec)	CBS (KBytes)	
e1	<input type="checkbox"/> Enabled	100000	<input type="checkbox"/> Enabled	100000	--	
e2	<input type="checkbox"/> Enabled	100000	<input type="checkbox"/> Enabled	100000	--	
e3	<input type="checkbox"/> Enabled	100000	<input type="checkbox"/> Enabled	100000	--	
e4	<input type="checkbox"/> Enabled	100000	<input type="checkbox"/> Enabled	100000	--	
e5	<input type="checkbox"/> Enabled	100000	<input type="checkbox"/> Enabled	100000	--	
e6	<input type="checkbox"/> Enabled	100000	<input type="checkbox"/> Enabled	100000	--	
e7	<input type="checkbox"/> Enabled	100000	<input type="checkbox"/> Enabled	100000	--	
e8	<input type="checkbox"/> Enabled	100000	<input type="checkbox"/> Enabled	100000	--	
e9	<input type="checkbox"/> Enabled	100000	<input type="checkbox"/> Enabled	100000	--	
e10	<input type="checkbox"/> Enabled	100000	<input type="checkbox"/> Enabled	100000	--	
e11	<input type="checkbox"/> Enabled	100000	<input type="checkbox"/> Enabled	100000	--	
e12	<input type="checkbox"/> Enabled	100000	<input type="checkbox"/> Enabled	100000	--	
e13	<input type="checkbox"/> Enabled	100000	<input type="checkbox"/> Enabled	100000	--	
e14	<input type="checkbox"/> Enabled	100000	<input type="checkbox"/> Enabled	100000	--	

**Bandwidth:**  
This function allows the network manager to control the maximum rate for traffic transmitted or received on a port. Rate limiting is configured on ports at the edge of a network to limit traffic coming into the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped. Egress shaping controls the level of traffic leaving an interface by using a policy based on a token bucket, where bucket depth (that is, the maximum burst before the bucket overflows) is specified by the committed burst size (CBS), and the average rate tokens are removed from the bucket is specified by the committed information rate (CIR). Traffic exceeding the specified policy will be dropped. Rate limiting and shaping can be applied to individual ports or LAGs.

Save Settings Cancel Changes

CISCO SYSTEMS

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

**Port**—Displays the port or LAG number.

### Ingress Rate Limit

**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).

### Egress Shaping

Shapes egress traffic by using a policy based on a token bucket, where bucket depth (that is, the maximum burst before the bucket overflows) is specified by the committed burst size (CBS), and the average rate tokens are removed from the bucket is specified by the committed information rate (CIR). Traffic exceeding the specified policy will be dropped.

**Status** – Enables or disable egress shaping.

**CIR (Kbits/sec)**—The committed information rate. (Range: 64-10000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower).

**CBS (KBytes)**—The committed burst size. (Range: 4-16380 at a granularity of 4k bytes)

**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, 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 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.

**LINKSYS**  
A Division of Cisco Systems, Inc.

24-port 10/100 PoE Switch w/4 gigabit ports SRW224G4P

Spanning Tree

Setup Port Management VLAN Management Statistics ACL Security QoS Spanning Tree Multicast More >>

STP Status Global STP STP Port Settings RSTP Port Settings MSTP Properties More >>

**STP Status**

Spanning Tree State	Enabled
Spanning Tree Mode	RSTP
Bridge ID	32768.001C10ECD56D
Designated Root	32768.001C10ECD56D
Root Port	0
Root Path Cost	0
Root Maximum Age (sec)	20
Root Hello Time (sec)	2
Root Forward Delay (sec)	15
Topology Changes Counts	0
Last Topology Change	0 d 3 h 58 min 46 s

**Spanning Tree**  
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 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. The spanning tree algorithms supported by the switch include: IEEE 802.1D Spanning Tree Protocol (STP), IEEE 802.1w Rapid Spanning Tree Protocol (RSTP), and IEEE 802.1s Multiple Spanning Tree (MSTP).

**STP Status:**  
Displays a summary of the current bridge STA information that applies to the entire switch.

CISCO SYSTEMS

**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 cost path 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 device Maximum Age Time. The Maximum Age Time 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 device Hello Time. The Hello Time indicates the amount of time in 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 device forward delay time. The Forward Delay Time indicates the amount of time in 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 a day hour minute second format, 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.

The screenshot displays the Linksys web-based utility interface for configuring Spanning Tree (STP) settings. The page title is "Spanning Tree Tab—Global STP". The navigation menu includes "Setup", "Port Management", "VLAN Management", "Statistics", "ACL", "Security", "QoS", "Spanning Tree", and "Multicast". The "Spanning Tree" sub-tab is active, showing "Global STP" settings. The "Spanning Tree State" is checked (Enabled). The "Spanning Tree Type" is set to "RSTP". The "Path Cost Method" is set to "Long". The "Priority (0-61440), in steps of 4096" is set to 32768. The "Hello Time (1-10)" is set to 2, "Maximum Age (6-40)" is set to 20, and "Forward Delay (4-30)" is set to 15. A "Global STP" help box on the right explains that it configures STA settings that apply to the entire switch, noting that RSTP/MSTP support connections to other STP or RSTP nodes by monitoring incoming protocol messages and dynamically adjusting the type of protocol messages the switch transmits. At the bottom, there are "Save Settings" and "Cancel Changes" buttons.

**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.
- **MSTP:** Multiple Spanning Tree (IEEE 802.1s)

**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.

**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 device Hello Time. The Hello Time indicates the amount of time in 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.

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

## Spanning Tree Tab—STP Port Settings

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

The screenshot shows the Linksys web-based utility interface for configuring STP Port Settings. The page title is "24-port 10/100 PoE Switch w/4 gigabit ports" and the device model is "SRW24G4P". The navigation menu includes Setup, Port Management, VLAN Management, Statistics, ACL, Security, QoS, Spanning Tree, Multicast, and More >>. The Spanning Tree section is active, showing STP Status, Global STP, STP Port Settings, RSTP Port Settings, MSTP Properties, and More >>. The STP Port Settings page displays a table of port configurations and a "Save Settings" button.

Port	State	Status	Role	Forward Transitions	Operational Edge Port	Detail
e1	<input checked="" type="checkbox"/> Enabled	Forwarding	Designated	2	Enabled	<a href="#">Detail</a>
e2	<input checked="" type="checkbox"/> Enabled	Discarding	Disabled	0	Enabled	<a href="#">Detail</a>
e3	<input checked="" type="checkbox"/> Enabled	Discarding	Disabled	0	Enabled	<a href="#">Detail</a>
e4	<input checked="" type="checkbox"/> Enabled	Discarding	Disabled	0	Enabled	<a href="#">Detail</a>
e5	<input checked="" type="checkbox"/> Enabled	Discarding	Disabled	0	Enabled	<a href="#">Detail</a>
e6	<input checked="" type="checkbox"/> Enabled	Discarding	Disabled	0	Enabled	<a href="#">Detail</a>
e7	<input checked="" type="checkbox"/> Enabled	Discarding	Disabled	0	Enabled	<a href="#">Detail</a>
e8	<input checked="" type="checkbox"/> Enabled	Discarding	Disabled	0	Enabled	<a href="#">Detail</a>
e9	<input checked="" type="checkbox"/> Enabled	Discarding	Disabled	0	Enabled	<a href="#">Detail</a>
e10	<input checked="" type="checkbox"/> Enabled	Discarding	Disabled	0	Enabled	<a href="#">Detail</a>
e11	<input checked="" type="checkbox"/> Enabled	Discarding	Disabled	0	Enabled	<a href="#">Detail</a>
e12	<input checked="" type="checkbox"/> Enabled	Discarding	Disabled	0	Enabled	<a href="#">Detail</a>
e13	<input checked="" type="checkbox"/> Enabled	Discarding	Disabled	0	Enabled	<a href="#">Detail</a>
e14	<input checked="" type="checkbox"/> Enabled	Discarding	Disabled	0	Enabled	<a href="#">Detail</a>

**STP Port Settings:**  
STP uses a distributed algorithm to select a bridging device (STP-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.

More ...

[Save Settings](#) [Cancel Changes](#)

**State**—Enables or disables Spanning Tree on an 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 STP Port Settings for an interface, including Path Cost, Priority, and Port Fast forwarding.

STP Port Setting	
Interface	g1
Designated Cost	100000
Designated Port	128.1
Designated Bridge	32768.0.0016B6F03BEC
Path Cost (1-200000000, 0: Auto)	0
Priority (0-240, in steps of 16)	128
Port Fast	<input checked="" type="checkbox"/> Enabled

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 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

**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.

- Default: 128
- Range: 0-240, in steps of 16

**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, 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, and also 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)

## Spanning Tree Tab—RSTP Port Settings

Displays the current status of ports and LAGs for the Rapid Spanning Tree Protocol.

**LINKSYS**  
A Division of Cisco Systems, Inc.

24-port 10/100 PoE Switch w/4 gigabit ports SRW224G-4P

Spanning Tree

Setup Port Management VLAN Management Statistics ACL Security QoS Spanning Tree Multicast More >>

STP Status Global STP STP Port Settings **RSTP Port Settings** MSTP Properties More >>

**RSTP Port Settings**

1 2 Next >>

Port	State	Status	Role	Forward Transitions	Operational Edge Port	Operational Link Type	Detail
e1	Enabled	Forwarding	Designated	2	Enabled	Point-to-Point	<a href="#">Detail</a>
e2	Enabled	Discarding	Disabled	0	Enabled	Shared	<a href="#">Detail</a>
e3	Enabled	Discarding	Disabled	0	Enabled	Shared	<a href="#">Detail</a>
e4	Enabled	Discarding	Disabled	0	Enabled	Shared	<a href="#">Detail</a>
e5	Enabled	Discarding	Disabled	0	Enabled	Shared	<a href="#">Detail</a>
e6	Enabled	Discarding	Disabled	0	Enabled	Shared	<a href="#">Detail</a>
e7	Enabled	Discarding	Disabled	0	Enabled	Shared	<a href="#">Detail</a>
e8	Enabled	Discarding	Disabled	0	Enabled	Shared	<a href="#">Detail</a>
e9	Enabled	Discarding	Disabled	0	Enabled	Shared	<a href="#">Detail</a>
e10	Enabled	Discarding	Disabled	0	Enabled	Shared	<a href="#">Detail</a>
e11	Enabled	Discarding	Disabled	0	Enabled	Shared	<a href="#">Detail</a>
e12	Enabled	Discarding	Disabled	0	Enabled	Shared	<a href="#">Detail</a>
e13	Enabled	Discarding	Disabled	0	Enabled	Shared	<a href="#">Detail</a>
e14	Enabled	Discarding	Disabled	0	Enabled	Shared	<a href="#">Detail</a>

**RSTP Port Settings:**  
RSTP is designed as a general replacement for the slower, legacy STP. RSTP is also incorporated into MSTP. RSTP achieves much faster reconfiguration (i.e., around 1 to 3 seconds, compared to 30 seconds or more for STP) by reducing the number of state changes before active ports start learning, presiding an alternate mode that can be used when a node or port fails, and retaining the forwarding database for ports insensitive to changes in the tree structure when reconfiguration occurs.

More...

CISCO SYSTEMS

**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.

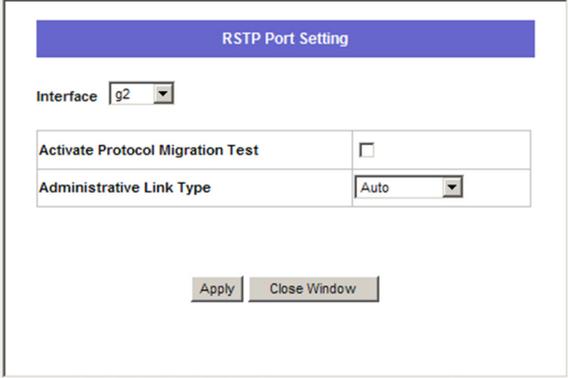
**Forward Transitions**—The number of times this port has transitioned from the Learning state to the Forwarding state.

**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.



The screenshot shows a web-based configuration window titled "RSTP Port Setting". It contains the following elements:

- A header bar with the text "RSTP Port Setting".
- An "Interface" dropdown menu with "g2" selected.
- A table with two rows:
  - Row 1: "Activate Protocol Migration Test" with an unchecked checkbox.
  - Row 2: "Administrative Link Type" with a dropdown menu showing "Auto".
- At the bottom, two buttons: "Apply" and "Close Window".

Click **Detail** to activate the protocol migration test, or to configure the Administrative Link Type.

**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.)

After completing any configuration changes, click **Apply**.

## Spanning Tree Tab—MSTP Properties

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

The screenshot shows the Linksys web-based utility interface for configuring MSTP properties. The top navigation bar includes 'Spanning Tree' and 'Multicast'. The 'Spanning Tree' sub-menu is active, showing 'MSTP Properties' as the selected option. The main content area displays the following configuration fields:

Region Name	<input type="text" value="00 1c 10 ec d5 6d"/>
Revision (#-65535)	<input type="text" value="0"/>
Max Hops (1-40)	<input type="text" value="20"/>
IST Master	32768.001C10ECD56D

The right sidebar provides a detailed explanation of these settings:

**MSTP Properties:**  
Configures MSTP settings that apply to the entire switch, including region name, revision and max hops.  
Region Name: The name for this MSTI.  
Revision: The revision for this MSTI.  
Max Hops: The maximum number of hops allowed in the MST region before a BPDU is discarded.  
IST Master: The root device of the Internal Spanning Tree to which this switch belongs. The IST identifier consists of port priority, MST ID, and bridge MAC address.  
Note that the MST name and revision number are both required to uniquely identify an MST region.

At the bottom of the page, there are 'Save Settings' and 'Cancel Changes' buttons.

**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.

**LINKSYS**  
A Division of Cisco Systems, Inc.

24-port 10/100 PoE Switch w/4 gigabit ports SRW224G4P

Spanning Tree

Setup Port Management VLAN Management Statistics ACL Security QoS Spanning Tree Multicast More >>

<< Back MSTP Instance Settings MSTP Interface Settings

**MSTP Instance Settings**

Instance Configuration

MST ID (0-4094):  VLAN ID:

Instance ID

Included VLANs

Included VLAN

Instance Settings

Bridge Priority (0-61440, in steps of 4096)

Designated Root Bridge ID 32768.001C10ECD56D

Root Port

Root Path Cost

Bridge ID 32768.001C10ECD56D

Remaining Hops

**MSTP Instance Settings:**  
MST ID: Instance identifier to configure. VLAN ID: VLAN to assign to this selected MST instance. MST Instance ID: Instance identifier of this spanning tree. Included VLANs: VLANs assigned 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.) Default: 32768. Range: 0-61440, in steps of 4096. Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440. More ...

CISCO SYSTEMS

**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

Displays the current status of ports and LAGs for the Multiple Spanning Tree Protocol.

**MSTP Interface Settings:**  
 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 bridging device through which this switch must communicate with the root of the Spanning Tree. Designated Bridge: The priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree. Path Cost: The path cost from the root port on this switch to the root device.

Port	State	Status	Role	Forward Transitions	Operational Edge Port	Detail
e1	Enabled	Forwarding	Designated	2	Enabled	<a href="#">Detail</a>
e2	Enabled	Discarding	Disabled	0	Enabled	<a href="#">Detail</a>
e3	Enabled	Discarding	Disabled	0	Enabled	<a href="#">Detail</a>
e4	Enabled	Discarding	Disabled	0	Enabled	<a href="#">Detail</a>
e5	Enabled	Discarding	Disabled	0	Enabled	<a href="#">Detail</a>
e6	Enabled	Discarding	Disabled	0	Enabled	<a href="#">Detail</a>
e7	Enabled	Discarding	Disabled	0	Enabled	<a href="#">Detail</a>
e8	Enabled	Discarding	Disabled	0	Enabled	<a href="#">Detail</a>
e9	Enabled	Discarding	Disabled	0	Enabled	<a href="#">Detail</a>
e10	Enabled	Discarding	Disabled	0	Enabled	<a href="#">Detail</a>
e11	Enabled	Discarding	Disabled	0	Enabled	<a href="#">Detail</a>
e12	Enabled	Discarding	Disabled	0	Enabled	<a href="#">Detail</a>
e13	Enabled	Discarding	Disabled	0	Enabled	<a href="#">Detail</a>
e14	Enabled	Discarding	Disabled	0	Enabled	<a href="#">Detail</a>

**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 prevents the Switch from broadcasting the traffic to all ports and possibly disrupting network performance.

The screenshot displays the Linksys web-based utility interface for a 24-port 10/100 PoE Switch w/4 gigabit ports (SRW224G4P). The Multicast tab is selected, and the Global Settings section is active. The interface includes a navigation menu with options like Setup, Port Management, VLAN Management, Statistics, ACL, Security, QoS, Spanning Tree, and Multicast. The Global Settings section contains the following configuration options:

- IGMP Version (1, 2, 3):** A dropdown menu set to 2.
- IGMP Snooping Status:** A checkbox labeled "Enabled" which is checked.
- MRouter Timeout (300-500):** A text input field set to 300 seconds.
- IGMP Querier Status:** A checkbox labeled "Enabled" which is unchecked.
- Query Count (2-10):** A text input field set to 2.
- Query Interval (60-125):** A text input field set to 125 seconds.
- Maximum Response Time (5-25):** A text input field set to 10 seconds.

At the bottom of the page, there are "Save Settings" and "Cancel Changes" buttons. A sidebar on the right provides a brief explanation of Multicast and Global Settings.

**IGMP Version**—Sets the protocol version for compatibility with other devices on the network. All systems on the subnet must support the same version. Also note that some attributes are only enabled for IGMPv2 and/or v3, including Act as IGMP Querier, IGMP Report Delay and IGMP Query Timeout. (Range: 1-3; Default: 2)

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

**MRouter Timeout**—The time 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 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).

**Query Count**—Sets the maximum number of queries issued for which there has been no response before the Switch takes action to drop a client from the multicast group. (Range: 2-10; Default: 2)

**Query Interval**—Sets the frequency at which the Switch sends IGMP host-query messages. (Range: 60-125 seconds; Default: 125)

**Maximum Response Time**—Sets the time 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)

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

## Multicast Tab—Static Member Ports

Multicast filtering can be dynamically configured using IGMP, but for certain applications that require tighter control, you can statically configure a multicast service on the switch. First add all the ports attached to participating hosts to a common VLAN, then assign the multicast service to that VLAN group. Note that static multicast addresses are never aged out from the switch.

The screenshot shows the Linksys web-based utility interface. At the top, it displays the Linksys logo and the device model: "24-port 10/100 PoE Switch w/4 gigabit ports SRW24G4P". The navigation menu includes Setup, Port Management, VLAN Management, Statistics, ACL, Security, QoS, Spanning Tree, Multicast, and More >>. The Multicast tab is selected, and the "Static Member Ports" sub-tab is active. The configuration page includes a "VLAN ID" dropdown menu set to "1", a "Multicast IP Address" input field, and a "Select Multicast Group Member" section with checkboxes for Ethernet (Eth) ports 1-24, Gigabit ports 1-4, and LAG ports 1-8. An "Add" button is located below the member selection. At the bottom, there is a table with columns for "Multicast IP Address" and "Members", and "Remove" and "Cancel" buttons.

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, the switch 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 trunk) 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.

**LINKSYS**  
A Division of Cisco Systems, Inc.

24 port 10/100 PoE Switch w/4 gigabit ports SRW224G4P

**Multicast**

Setup Port Management VLAN Management Statistics ACL Security QoS Spanning Tree Multicast More >>

Global Settings Static Member Ports **Static Router Ports** Member Ports Query Router Ports Query

**Static Router Ports**

VLAN ID: 1

**Select Multicast Router Port**

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

Gigabit 1 2 3 4

LAG 1 2 3 4 5 6 7 8

**Static Router Ports:**  
Depending on your network connections, the switch 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 trunk) 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.

Save Settings Cancel Changes

CISCO SYSTEMS

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.

The screenshot shows the Linksys web-based utility interface. At the top, the Linksys logo is displayed as "LINKSYS A Division of Cisco Systems, Inc.". Below the logo, the device information is shown: "24-port 10/100 PoE Switch w/4 gigabit ports" and "SRV224G4P". The navigation menu includes "Multicast" and "More >>". Under "Multicast", there are sub-menus: "Setup", "Port Management", "VLAN Management", "Statistics", "ACL", "Security", "QoS", "Spanning Tree", and "Multicast". The "Multicast" sub-menu is expanded, showing "Global Settings", "Static Member Ports", "Static Router Ports", "Member Ports Query" (highlighted), and "Router Ports Query".

The "Member Ports Query" screen has a title bar "Member Ports Query". It features two drop-down menus: "VLAN ID:" with the value "1" and "Multicast IP Address" with the value "(none)". Below these is a table with the following structure:

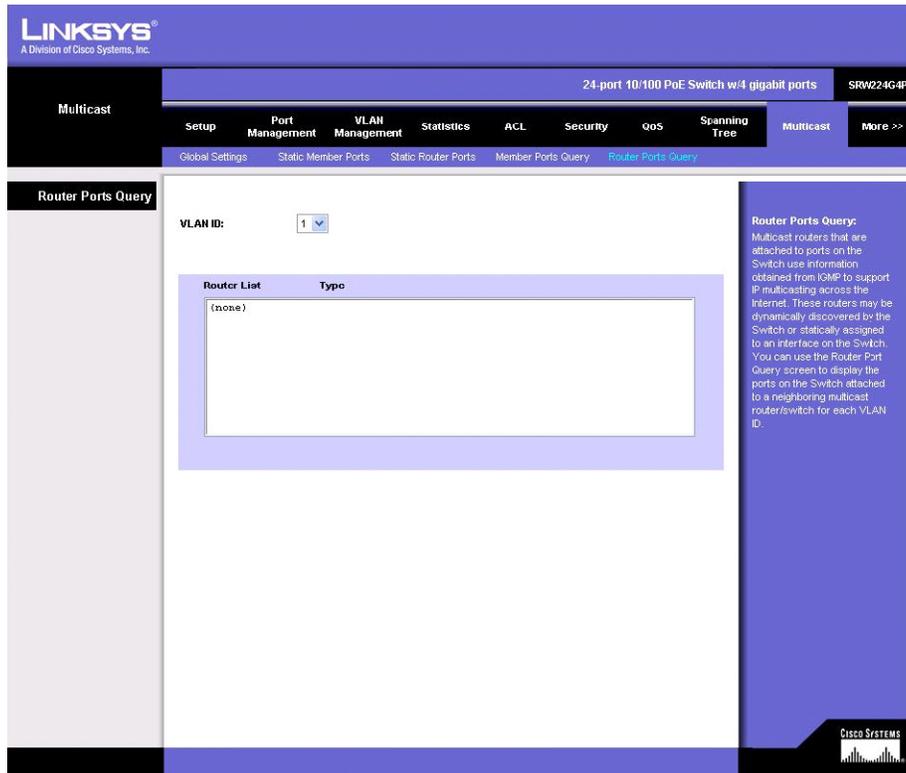
Member Port	Type
(none)	

On the right side of the screen, there is a help text box titled "Member Ports Query:" with the following content: "Displays 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 menus. The Switch will display all the interfaces that are propagating this multicast service." The Cisco Systems logo is visible in the bottom right corner of the interface.

Select a VLAN ID and the IP address for a multicast service from the drop-down menus. The Switch will display all the interfaces that are propagating this multicast service.

## Multicast Tab—Router Ports Query

Multicast routers that are attached to ports on 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 menus. 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.

The screenshot shows the Linksys web-based utility interface for configuring SNMP. The main content area is titled "Global Parameters" and is divided into several sections:

- SNMPv3:**
  - Local Engine ID:** A text input field containing the hexadecimal value "80000f7303001c10ecd5690000".
  - User Default:** A checkbox that is currently unchecked.
- Notifications:**
  - Enable Authentication Traps:** A checked checkbox.
  - Enable Link-up and Link-down Traps:** A checked checkbox.
- SNMPv3 Remote Engine ID:** A table with three columns: "Remote Engine ID", "Remote IP Host", and "Action". The table is currently empty, and there is an "Add" button in the "Action" column.

At the bottom of the page, there are "Save Settings" and "Cancel Changes" buttons. A sidebar on the right contains a description of the SNMP tab and the Global Parameters section.

### 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.

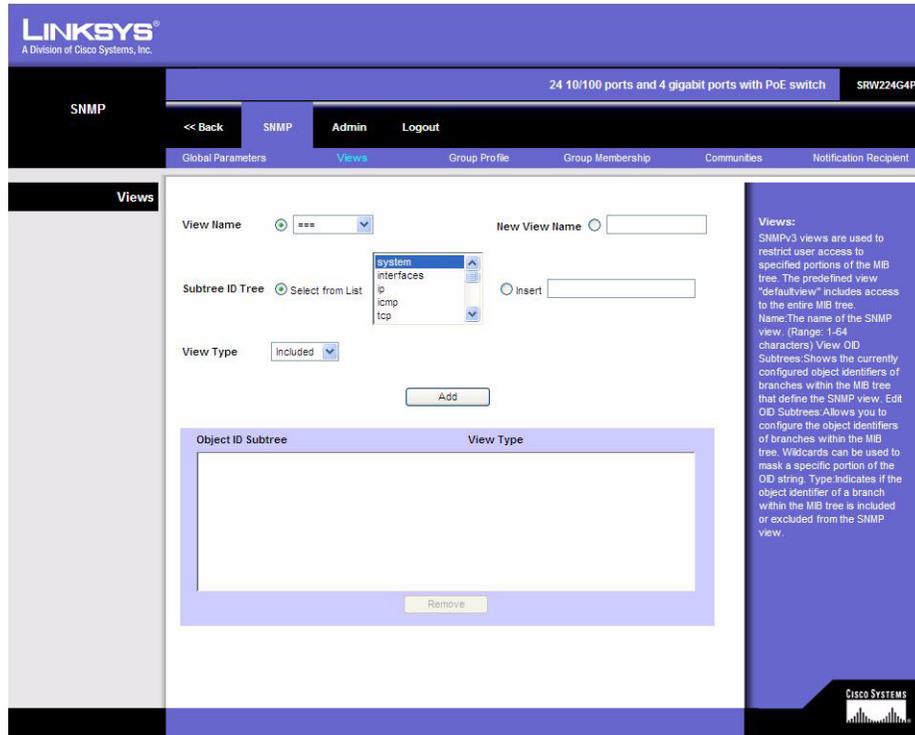
**Remote IP Host**—This is the address of a new management station to receive trap messages.

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 an 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.

**LINKSYS**  
A Division of Cisco Systems, Inc.

24 10/100 ports and 4 gigabit ports with PoE switch SRW224G4P

SNMP << Back SNMP Admin Logout

Global Parameters Views **Group Profile** Group Membership Communities Notification Recipient

**Group Profile**

Group Name:

Security Model: v1

Security Level: noAuthNoPriv

Operation:  Read defaultview  Write defaultview  Notify defaultview

Add

Group Name	Security Model	Security Level	Read	Operation Write	Notify
public	v1	noAuthNoPriv	defaultview	none	none
public	v2c	noAuthNoPriv	defaultview	none	none
private	v1	noAuthNoPriv	defaultview	defaultview	none
private	v2c	noAuthNoPriv	defaultview	defaultview	none

Remove

**Group Profile:**  
An SNMPv3 group sets the access policy for its assigned users, restricting them to specific read and write views. You can use the pre-defined default groups or create new groups to map a set of SNMP users to SNMP views. Group Name: The name of the SNMP group. (Range: 1-32 characters) Model: The group security model; SNMP v1, v2c or v3. Level: The security level used for the group—noAuthNoPriv: There is no authentication or encryption used in SNMP communications.—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).  
More...

CISCO SYSTEMS

**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.

**LINKSYS**  
A Division of Cisco Systems, Inc.

24 10/100 ports and 4 gigabit ports with PoE switch SRW224G4P

SNMP

<< Back SNMP Admin Logout

Global Parameters Views Group Profile Group Membership Communities Notification Recipient

**Group Membership**

User Name:

Local  Remote (none)

Group Name: public

Security Model: v1

Security Level: noAuthNoPriv

User Authentication:

Authentication Protocol: MD5

Authentication Password:

Data Privacy:

Privacy Protocol: DES56

Privacy Password:

Add

User Name	Engine ID	Group Name	Model	Level	Auth	Privacy
(none)						

Remove

**Group Membership:**  
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) 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 user. -noAuthNoPriv: There is no authentication or encryption used in SNMP communications. -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).  
More...

### 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).

LINKSYS  
A Division of Cisco Systems, Inc.

24 10/100 ports and 4 gigabit ports with PoE switch SRW224G4P

SNMP << Back SNMP Admin Logout

Global Parameters Views Group Profile Group Membership Communities Notification Recipient

SNMP Communities

Community String

Basic Access Mode

Add

Community String	Access Mode
public	ReadOnly
private	ReadWrite

Remove Cancel

Communities:  
Displays a list of the community strings currently configured. Default strings are public (read-only access) and private (read/write access).  
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).  
Access Mode Sets the access rights for the new community that you are creating. Read-Only - Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.  
Read/Write - Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects.

CISCO SYSTEMS

**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.

**Notification Recipient:**  
Use this page to configure the community strings authorized for management access, and to specify the trap managers that will receive SNMP notifications or trap messages. Recipient IP: address of a new management station to receive trap messages. Notification Type: Specifies whether to send notifications as SNMP v1, v2c, or v3 traps. (Default: Version 1) 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 as SNMP v1 or SNMP v2c. (Default: Version 1)

Recipient IP	Notification Type	Community String	Notification Version	UDP Port	Timeout	Retries
(none)						

**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).

**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 5 user names and passwords for management access (console, Telnet, 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.

The screenshot shows the Linksys web-based utility interface for user authentication. The top navigation bar includes 'Admin', '<< Back', 'SNMP', 'Admin', and 'Logout'. The main content area is titled 'User Authentication' and contains a form for adding a new user account. The form has fields for 'User Name', 'Password', and 'Confirm Password', and an 'Add' button. Below the form is a table with one entry: 'admin'. The table has 'Remove' and 'Cancel' buttons. The 'Authentication Setting' section shows 'Authentication Type' set to 'Local'. The right sidebar contains an 'Admin' section with a warning about the default 'admin' account and a 'User Authentication' section with a warning about the switch's user limits. The bottom of the page has 'Save Settings' and 'Cancel Changes' buttons.

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 it is entered an “\*” corresponding to each character is displayed in the field. (Range: 1-159 characters)

**Confirm Password**—Confirms the new password. The password entered into this field must be exactly the same as 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.

**LINKSYS**  
A Division of Cisco Systems, Inc.

Admin 24 10/100 ports and 4 gigabit ports with PoE switch SRW224G4P

<< Back SNMP Admin Logout

User Authentication **Forwarding Database** Log Port Mirroring Cable Test More >>

**Forwarding Database**

Address Aging

Aging Status  Enabled

Aging Interval(secs) (10-630):  seconds

Static Address Setting

Static Address Counts

Interface  Port   LAG

MAC Address (XX-XX-XX-XX-XX-XX)

VLAN

Interface	MAC Address	VLAN
(none)		

Dynamic Address Query

Dynamic Address Counts

Query by:

Interface  Port   LAG

MAC Address

VLAN

Address Table Sort Key

Interface	MAC Address	VLAN
Eth 13	00-0D-60-AD-41-63	1

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 age out dynamically learned forwarding information.

Dynamic Addresses: Dynamic addresses in the MAC addresses table are learned by monitoring the source address for traffic entering the switch.

More...

Cisco Systems

### Address Aging

Sets the aging time for entries in the forwarding database. The aging time is used to age out dynamically learned forwarding information.

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

**Aging Interval (secs) (10-1000000)**—This is the amount of time after which dynamic address table entries are discarded.

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

### 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 moved. When a static address is seen 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 (XX-XX-XX-XX-XX-XX)**—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).

Specify the search type (that is, check the Interface, MAC Address, or VLAN checkbox), select the method of sorting the displayed addresses, and then 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**.

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

## 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.

**LINKSYS**  
A Division of Cisco Systems, Inc.

24 10/100 ports and 4 gigabit ports with PoE switch SRW224G4P

Admin << Back SNMP Admin Logout

User Authentication Forwarding Database Log Port Mirroring Cable Test More >>

**Log**

System Logging

System Log Status  Enabled

Flash Logging (0-7) 3 - Error

Memory Logging (0-7) 7 - Debugging

Syslog

Remote Log Status  Enabled

Logging Facility (16-23) 23

Logging Trap (0-7) 7 - Debugging

Syslog Server	IP Address
1	<input type="text"/>
2	<input type="text"/>
3	<input type="text"/>
4	<input type="text"/>
5	<input type="text"/>

Log:

The switch allows you to control the logging of error messages, including the type of events that are recorded in switch memory, logging to a remote System Log (syslog) server, and displays a list of recent event messages.

System Logging: The system allows you to enable or disable event logging, and specify which 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. Up to 4096 log entries can be stored in the flash memory, with the oldest entries being overwritten first when the available log memory (256 kilobytes) has been exceeded. The System Logs page allows you to configure and limit system messages that

are logged to flash or RAM memory. The default is for event levels 0 to 3 to be logged to flash and levels 0 to 7 to be logged to RAM.

SMTP Setting

Admin Status  Enabled

Severity 7 - Debugging

SMTP	IP Address
1	<input type="text"/>
2	<input type="text"/>
3	<input type="text"/>

Source Email Address

Destination Email Address 1

Destination Email Address 2

Destination Email Address 3

Destination Email Address 4

Destination Email Address 5

CISCO SYSTEMS

The following table describes the system event levels.

Level*	Severity Name	Description
7	Debug	Debugging messages
6	Informational	Informational messages only
5	Notice	Normal but significant condition, such as a cold start
4	Warning	Warning conditions, such as return false or unexpected return

Level*	Severity Name	Description
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

\* There are only Level 2, 5 and 6 event messages for the current firmware release

### System Logging

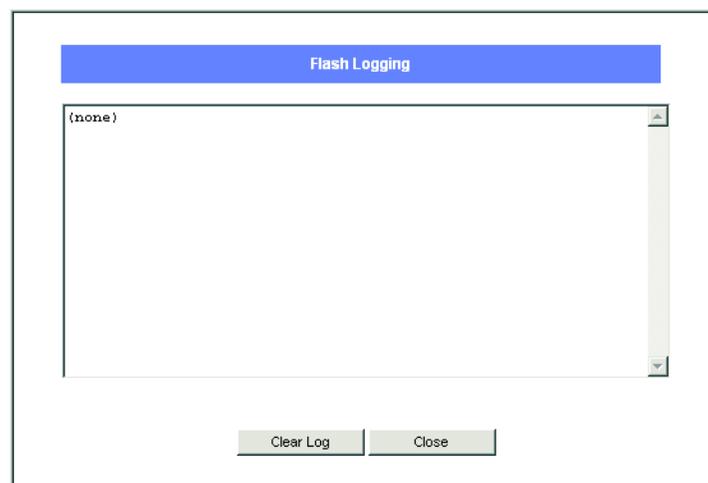
The system allows you to enable or disable event logging, and specify which event levels are logged to RAM or flash memory. Severe error messages that are logged to flash memory are permanently stored in the Switch to assist in troubleshooting network problems.

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

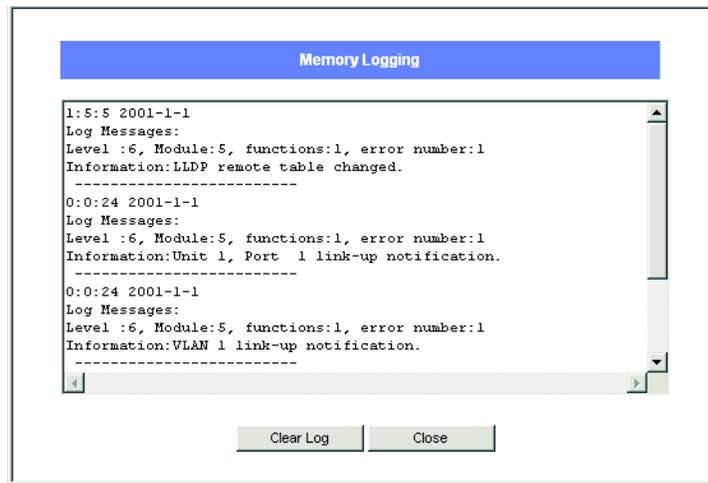
**Flash Logging (0-7)**—Limits log messages saved to the Switch's permanent flash memory for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be logged to flash. Note that the Flash Level must be equal to or less than the Ram Level.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

**Memory Logging (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 3 is specified, all messages from level 0 to level 3 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 7 will report all events from level 7 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 screenshot shows the Linksys web-based utility interface for configuring port mirroring. The top navigation bar includes 'Admin', 'SNMP', 'Admin', and 'Logout'. The main menu has 'User Authentication', 'Forwarding Database', 'Log', 'Port Mirroring', 'Cable Test', and 'More >>'. The 'Port Mirroring' section is active, showing a form with the following fields:

- Source Port: e1
- Type: Receive
- Target Port: e1

Below these fields is an 'Add' button. A table below the 'Add' button has the following structure:

Source Port	Type	Target Port
(none)		

At the bottom of the table are 'Remove' and 'Cancel' buttons. A help text box on the right side of the screen reads:

**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 switch supports only a single mirror session from the source port to target port. Note that the target port speed should match or exceed source port speed, otherwise traffic may be dropped.

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.

**LINKSYS**  
A Division of Cisco Systems, Inc.

24 10/100 ports and 4 gigabit ports with PoE switch SRW224G4P

Admin << Back SNMP Admin Logout

User Authentication Forwarding Database Log Port Mirroring **Cable Test** More >>

**Cable Test** ATTENTION: The cable should be connected at both ends. If the cable is not connected, the test result will always fail

1 2 Next >>

Port	Test Result	Cable Fault Distance	Last Update	
e1	Not test yet	0.0		Test
e2	Not test yet	0.0		Test
e3	Not test yet	0.0		Test
e4	Not test yet	0.0		Test
e5	Not test yet	0.0		Test
e6	Not test yet	0.0		Test
e7	Not test yet	0.0		Test
e8	Not test yet	0.0		Test
e9	Not test yet	0.0		Test
e10	Not test yet	0.0		Test
e11	Not test yet	0.0		Test
e12	Not test yet	0.0		Test
e13	Not test yet	0.0		Test
e14	Not test yet	0.0		Test

**Cable Test:**  
To test the connection quality of an attached cable, click on the test button for the port (ports 1-48 only). Note that the cable needs to be connected at both ends, otherwise the test will fail. The cable test results for each port are displayed in the table.

CISCO SYSTEMS

**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.

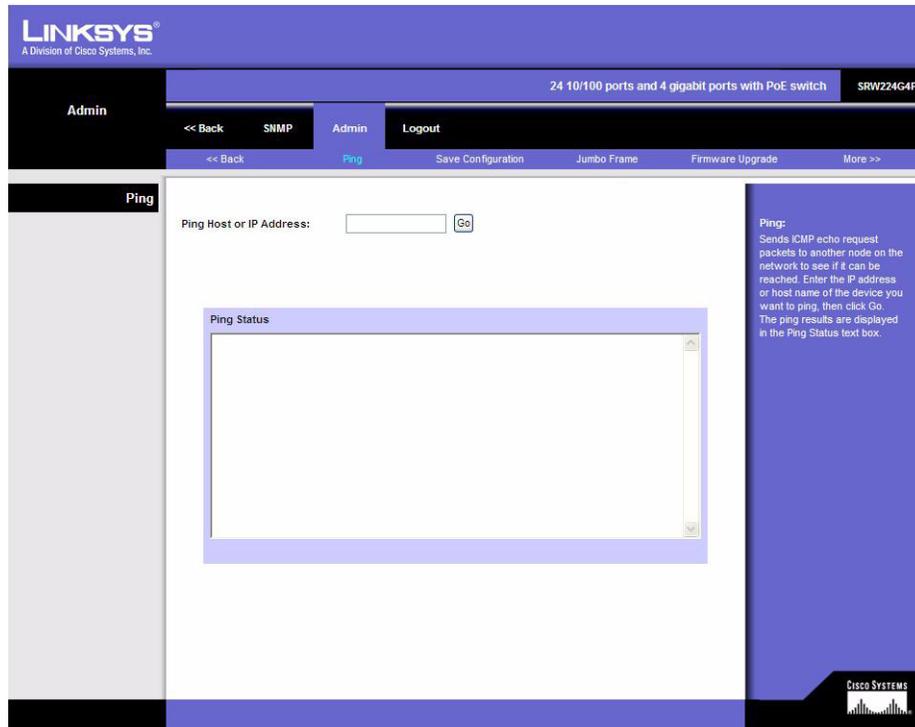
**Cable Fault Distance**—This is the distance from the port at which the cable error occurred.

**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 ten 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.

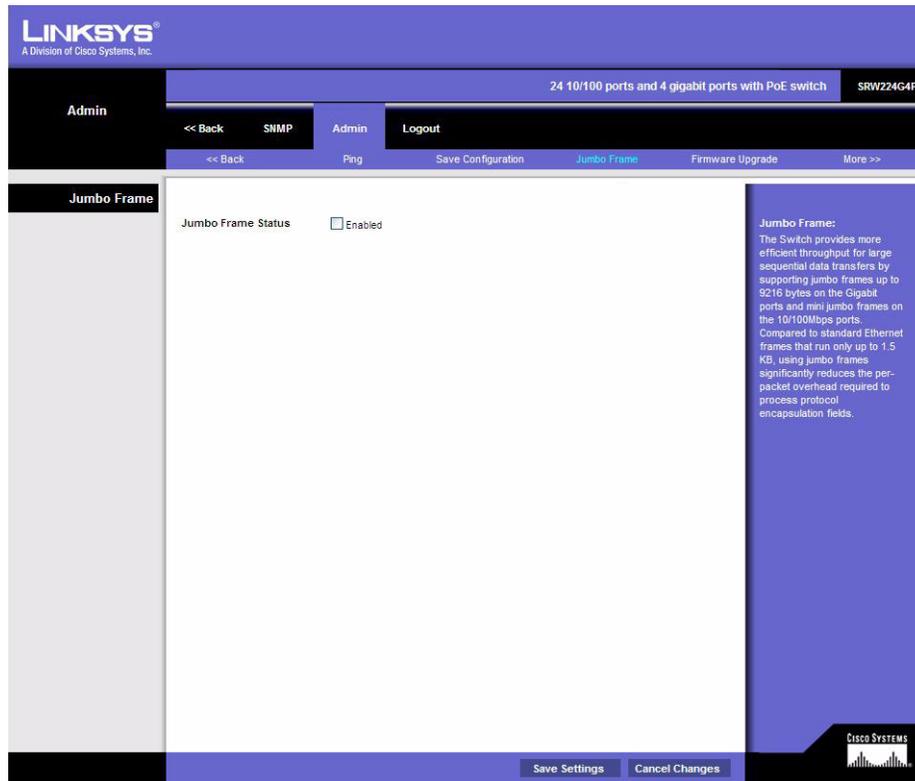
The screenshot shows the 'Save Configuration' page in the Linksys web-based utility. The page has a blue header with the Linksys logo and 'A Division of Cisco Systems, Inc.'. Below the header, there is a navigation bar with 'Admin' selected and 'Logout' visible. The main content area has a left sidebar with 'Save Configuration' selected. The main content area contains two radio buttons: 'Upgrade' (selected) and 'Backup'. Below the radio buttons, there are three input fields: 'TFTP Server', 'Source File', and 'Destination File' (containing 'startup1.cfg'). A 'Proceed' button is located below the 'Destination File' field. On the right side, there is a help sidebar with the following text: '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 the Upgrade or Backup radio button. Enter the IP address of the TFTP server, specify the name of the configuration file on the server, and then click Save Settings.'

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 **Proceed**.

## Admin Tab—Jumbo Frame

The Switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames up to 10240 bytes. 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

Downloads or uploads Switch firmware files from a TFTP server. The Switch allows the runtime software and diagnostic boot files to be upgraded.

The screenshot shows the Linksys web-based utility interface for the Firmware Upgrade page. The page title is "Firmware Upgrade" and the device model is "SRW224G4P". The interface includes a navigation bar with "Admin" and "Logout" buttons, and a breadcrumb trail: "<< Back", "SNMP", "Admin", "Ping", "Save Configuration", "Jumbo Frame", "Firmware Upgrade", and "More >>". The main content area has a "Firmware Upgrade" header and two radio buttons: "Upgrade" (selected) and "Backup". Below these are three input fields: "File Type" (a dropdown menu set to "Software Image"), "TFTP Server" (empty), and "Destination File" (containing "SRW224G4P\_SRW248G4P\_image.bbx"). A "Proceed" button is located below the input fields. On the right side, there is a help text box titled "Firmware Upgrade:" which explains the process of downloading or uploading firmware files from a TFTP server, including instructions on selecting the radio button, file type, and entering the TFTP server details.

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 menu, 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 **Proceed**.

## Admin Tab—HTTP Upgrade

Download new Switch runtime software from the local web management PC.

The screenshot displays the Linksys web management interface. At the top, the Linksys logo is visible, along with the text "A Division of Cisco Systems, Inc.". The page title is "24 10/100 ports and 4 gigabit ports with PoE switch" and the model number "SRW224G4P" is shown in the top right. The navigation menu includes "Admin", "SNMP", "Admin", and "Logout". Below the navigation menu, there are links for "<< Back", "HTTP Upgrade", "Reboot", and "Factory Default". The main content area is titled "HTTP Upgrade" and contains a form with the following fields:

File Type	Firmware
Source File	<input type="text"/> <input type="button" value="Browse..."/>
Destination File	SRW224G4P_SRW248G4P_image.bin
<input type="button" value="Proceed"/>	

On the right side of the form, there is a blue sidebar with the following text:

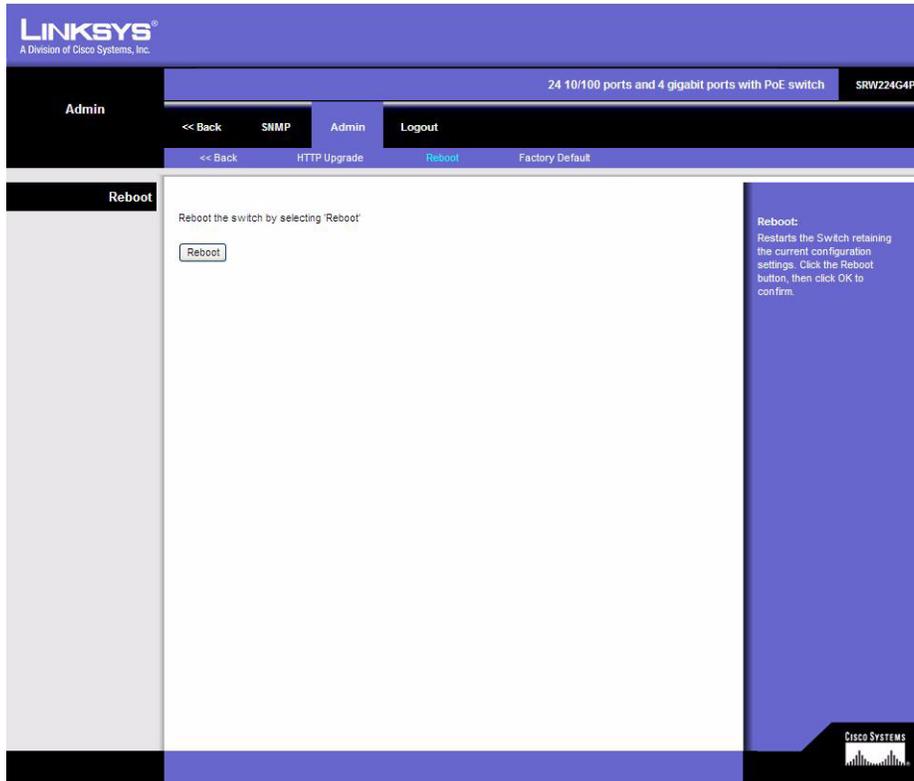
**HTTP Upgrade:**  
Downloads new switch runtime software from the local web management PC. Enter the file name of the software or use the Browse button to locate the file on the PC, then click Save Settings.

The Cisco Systems logo is visible in the bottom right corner of the interface.

Enter the file name of the software or use the Browse button to locate the file on the PC, then click **Proceed**.

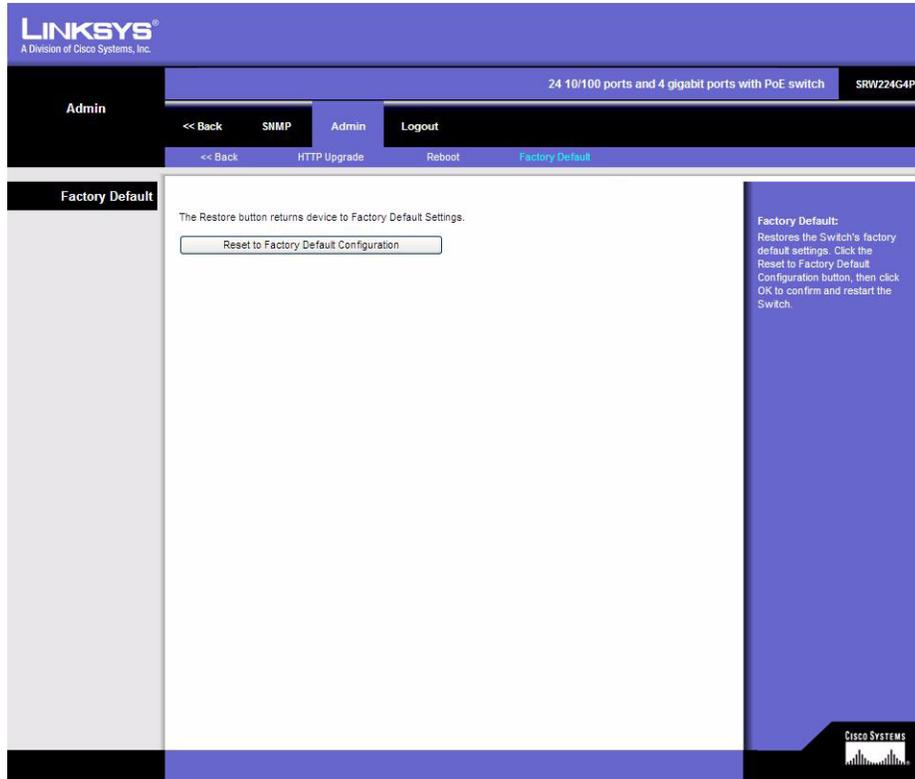
## Admin Tab—Reboot

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.

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

# Specifications

## SRW224G4P Specifications

Model	SRW224G4P
Ports	24 RJ-45 connectors for 10BASE-T, 100BASE-TX and 1000BASE-T with 2 shared SFP slots and 2 gigabit ports
Cabling Type	UTP CAT 5 or better for 10BASE-T/100BASE-TX, UTP CAT 5e or better for 1000BASE-T
LEDs	System, Link/Act, G1-4
Switching Capacity	12.8 Gbps, non-blocking
Web User Interface	Built-in Web UI for easy browser-based configuration (HTTP/HTTPS)
SNMP	Version v1, v2c, v3 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 (SSHv2) 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)—TFTP upgrade
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

### SRW224G4P Specifications

Access Control	ACLs—Drop or rate limit based on: Source and destination MAC address Source and destination IP address Protocol ToS/DSCP Port VLAN Ethertype
Link Aggregation	Link Aggregation using IEEE 802.3ad LACP. Up to 8 ports in up to 8 trunks.
Storm Control	Broadcast, Multicast and Unknown Unicast
Spanning Tree	IEEE 802.1d Spanning Tree, IEEE 802.1w Rapid Spanning Tree, IEEE 802.1s Multiple Spanning Tree, Fast Linkover
IGMP Snooping	IGMP (v1/v2/v3) 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 IPv4 IP precedence/ToS/ DSCP TCP/UDP port
Number of VLANs	256 Active VLANs—4096 range
VLAN	Port-based and 802.1q based VLANs Management VLAN. Automatic configuration of VLANs across multiple switches through GVRP / GARP. Private VLAN edge for simplified network isolation for guest connections or autonomous network. Dynamic VLAN Assignment.
HOL Blocking	Head of line blocking prevention
Jumbo frame	Supports frames up to 10K byte frames
Standards	802.3 10BASE-T Ethernet, 802.3u 100BASE-TX Fast Ethernet, 802.3ab 1000BASE-T Gigabit Ethernet, 802.3z Gigabit Ethernet, 802.3x Flow Control
Power	100-240V 0.5A
Certification	FCC Part15 Class A, CE Class A, UL CSA (CSA22.2), CE mark, CB
Certification	FCC Part15 Class A, CE Class A, UL CSA (CSA22.2), CE mark, CB

**SRW224G4P Specifications**

Dimensions	17.32" x 1.75" x 13.7"
Unit Weight	11.42 lb. (5.18 kg)
Operating Temperature	32 to 122°F (0 to 45°C)
Storage Temperature	-4 to 158°F (-20 to 70°C)
Operating Humidity	20 to 95%
Storage Humidity	5 to 90% noncondensing

### SRW248G4P Specifications

Model	SRW248G4P
Ports	48 RJ-45 connectors for 10BASE-T, 100BASE-TX and 1000BASE-T with 2 shared SFP slots and 2 giga ports
Cabling Type	UTP CAT 5 or better for 10BASE-T/100BASE-TX, UTP CAT 5e or better for 1000BASE-T
LEDs	Power, Link/Act, Speed
Switching Capacity	17.6 Gbps, non-blocking
Web User Interface	Built-in Web UI for easy browser-based configuration (HTTP/HTTPS)
SNMP	Version v1, v2c, v3 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 (SSHv2) 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)—TFTP upgrade
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

Access Control	ACLs—Drop or rate limit based on: Source and destination MAC address Source and destination IP address Protocol ToS/DSCP Port VLAN Ethertype
Link Aggregation	Link Aggregation using IEEE 802.3ad LACP. Up to 8 ports in up to 8 trunks.
Storm Control	Broadcast, Multicast and Unknown Unicast
Spanning Tree	IEEE 802.1d Spanning Tree, IEEE 802.1w Rapid Spanning Tree, IEEE 802.1s Multiple Spanning Tree, Fast Linkover
IGMP Snooping	IGMP (v1/v2/v3) 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 IPv4 IP precedence/ToS/DSCP TCP/UDP port
Number of VLANs	256 Active VLANs—4096 range
VLAN	Port-based and 802.1q based VLANs Management VLAN. Automatic configuration of VLANs across multiple switches through GVRP / GARP. Private VLAN edge for simplified network isolation for guest connections or autonomous network. Dynamic VLAN Assignment.
HOL Blocking	Head of line blocking prevention
Jumbo frame	Supports frames up to 10K byte frames
Standards	802.3 10BASE-T Ethernet, 802.3u 100BASE-TX Fast Ethernet, 802.3ab 1000BASE-T Gigabit Ethernet, 802.3z Gigabit Ethernet, 802.3x Flow Control
Power	100-240V 0.5A
Certification	FCC Part15 Class A, CE Class A, UL CSA (CSA22.2), CE mark, CB
Dimensions	17.32" x 1.75" x 13.7"

Unit Weight	11.42 lb. (5.18 kg)
W x H x D	(440 x 44 x 348 mm)
Operating Temperature	32 to 122°F (0 to 45°C)
Storage Temperature	-4 to 158°F (-20 to 70°C)
Operating Humidity	20 to 95%
Storage Humidity	5 to 90% noncondensing

# 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](http://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](http://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](http://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](http://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

This appendix includes the following regulatory statements:

- ["Federal Communications Commission Interference Statement," on page 135](#)
- ["Industry Canada Statement," on page 135](#)
- ["Règlement d'Industry Canada," on page 135](#)
- ["EC Declaration of Conformity \(Europe\)," on page 136](#)
- ["User Information for Consumer Products Covered by EU Directive 2002/96/EC on Waste Electric and Electronic Equipment \(WEEE\)," on page 136](#)

## Federal Communications Commission Interference Statement

This product has been tested and complies with the specifications 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 according to 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 is found by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment or devices
- Connect the equipment to an outlet other than the receiver's
- Consult a dealer or an experienced radio/TV technician for assistance

## Industry Canada Statement

This device complies with Industry Canada ICES-003 rule.

Operation is subject to the following two conditions:

This device may not cause interference and

This device must accept any interference, including interference that may cause undesired operation of the device.

## Règlement d'Industry Canada

Cet appareil est conforme à la norme NMB003 d'Industrie Canada.

Le fonctionnement est soumis aux conditions suivantes :

- Ce périphérique ne doit pas causer d'interférences;
- Ce périphérique doit accepter toutes les interférences reçues, y compris celles qui risquent d'entraîner un fonctionnement indésirable..

## EC Declaration of Conformity (Europe)

In compliance with the EMC Directive 89/336/EEC, Low Voltage Directive 73/23/EEC, and Amendment Directive 93/68/EEC, this product meets the requirements of the following standards:

- EN55022 Emission
- EN55024 Immunity

The following acknowledgements pertain to this software license.

## User Information for Consumer Products Covered by EU Directive 2002/96/EC on Waste Electric and Electronic Equipment (WEEE)

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.

### **Български (Bulgarian) - Информация относно опазването на околната среда за потребители в Европейския съюз**

Европейска директива 2002/96/ЕС изисква уредите, носещи този символ върху изделието и/или опаковката му, да не се изхвърлят с несортирани битови отпадъци. Символът обозначава, че изделието трябва да се изхвърля отделно от сметосъбирането на обикновените битови отпадъци. Ваша е отговорността този и другите електрически и електронни уреди да се изхвърлят в предварително определени от държавните или общински органи специализирани пунктове за събиране. Правилното изхвърляне и рециклиране ще спомогнат да се предотвратят евентуални вредни за околната среда и здравето на населението последствия. За по-подробна информация относно изхвърлянето на вашите стари уреди се обърнете към местните власти, службите за сметосъбиране или магазина, от който сте закупили уреда.

### **Čeština (Czech)—Informace o ochrání 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 neřádným 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 sbírných 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 získáte 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.

### **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 Haushaltsmüll 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.

**Eesti (Estonian)—Keskonnaalane 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.

**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.

**Ελληνικά (Greek) - Στοιχεία περιβαλλοντικής προστασίας για πελάτες εντός της Ευρωπαϊκής Ένωσης**

Η Κοινοτική Οδηγία 2002/96/ΕΚ 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.

**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.

### **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 nešķīrotā 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 kurios pakuotė yra pažymėta šiuo simboliu (įveskite simboli), 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 perdurbant 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 ghal Kliġenti 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 municipali li ma giex 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 iehor ta' l-elettriku u elettroniku permezz ta' facilitajiet ta' għbir appuntati apposta mill-gvern jew mill-awtoritajiet lokali. Ir-rimi b'mod korrett u r-riciklagg jgħin jipprevjeni konsegwenzi negattivi potenzjali għall-ambjent u għas-saħha tal-bniedem. Għal aktar informazzjoni dettaljata dwar ir-rimi tat-tagħmir antik tiegħek, jekk jogħgbok ikkuntattja lill-awtoritajiet lokali tiegħek, is-servizzi għar-rimi ta' l-iskart, jew il-hanut minn fejn xtrajt il-prodott.

### **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 rendszerektől elkülönített eljárást kell alkalmazni. Az Ön felelőssége, hogy ezt, és más elektromos és elektronikus berendezéseit a kormányzati vagy a helyi hatóságok által kijelölt gyűjtőrendszeren keresztül számolja fel. A megfelelő hulladékfeldolgozás segít a környezetre és az emberi egészségre potenciálisan ártalmas negatív hatások megelőzésében. 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.

#### **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.

#### **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 exhibe 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 das 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.

#### **Română (Romanian) - Informații de mediu pentru clienții din Uniunea Europeană**

Directiva europeană 2002/96/CE impune ca echipamentele care prezintă acest simbol pe produs și/sau pe ambalajul acestuia să nu fie casate împreună cu gunoiul menajer municipal. Simbolul indică faptul că acest produs trebuie să fie casat separat de gunoiul menajer obișnuit. Este responsabilitatea dvs. să cașati acest produs și alte echipamente electrice și electronice prin intermediul unităților de colectare special desemnate de guvern sau de autoritățile locale. Casarea și reciclarea corecte vor ajuta la prevenirea potențialelor consecințe negative asupra sănătății mediului și a oamenilor. Pentru mai multe informații detaliate cu privire la casarea acestui echipament vechi, contactați autoritățile locale, serviciul de salubritate sau magazinul de la care ați achiziționat produsul.

#### **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.

#### **Slovenščina (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 posebno zbirališča, ki jih določijo države 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.

#### **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.

#### **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.

# Safety Information

## Meaning of the Warning Symbol



### **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. This symbol is used to indicate a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.

## General Safety Information



### **WARNING: Work During Lightning Activity**

Do not work on the system or connect or disconnect cables during periods of lightning



### **WARNING: Installation Instructions**

Read the installation instructions before connecting the system to the power source



### **WARNING: SELV Circuit**

To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.



### **WARNING: Equipment Installation**

Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

**WARNING: Local National Electrical Codes**

Installation of the equipment must comply with local and national electrical codes.

**WARNING: Product Disposal**

Ultimate disposal of this product should be handled according to all national laws and regulations.

## Power Safety Information

**WARNING: TN Power**

The device is designed to work with TN power systems.

**WARNING: Warning Ground Conductor Warning**

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

**WARNING: Power Supply Installation Warning**

The power supply must be placed indoors.

**WARNING: Circuit Breaker**

This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 120 VAC, 15A U.S. (240 VAC, 10A international)



**WARNING: Warning Main Disconnecting Device**

The plug-socket combination must be accessible at all times, because it serves as the main disconnecting device.

# Software License Agreement

## Software in Linksys Products:

This product from Cisco-Linksys LLC or from one of its affiliates Cisco Systems-Linksys (Asia) Pte Ltd. or Cisco-Linksys K.K. ("Linksys") contains software (including firmware) originating from Linksys and its suppliers and may also contain software from the open source community. Any software originating from Linksys and its suppliers is licensed under the Linksys Software License Agreement contained at Schedule 1 below. You may also be prompted to review and accept that Linksys Software License Agreement upon installation of the software.

Any software from the open source community is licensed under the specific license terms applicable to that software made available by Linksys at [www.linksys.com/gpl](http://www.linksys.com/gpl) or as provided for in Schedules 2 and 3 below.

Where such specific license terms entitle you to the source code of such software, that source code is upon request available at cost from Linksys for at least three years from the purchase date of this product and may also be available for download from [www.linksys.com/gpl](http://www.linksys.com/gpl). For detailed license terms and additional information on open source software in Linksys products please look at the Linksys public web site at: [www.linksys.com/gpl/](http://www.linksys.com/gpl/) or Schedule 2 below as applicable.

BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE PRODUCT CONTAINING THE SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THE SOFTWARE LICENSE AGREEMENTS BELOW. IF YOU DO NOT AGREE TO ALL OF THESE TERMS, THEN YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE. YOU MAY RETURN UNUSED SOFTWARE (OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, THE UNUSED PRODUCT) FOR A FULL REFUND UP TO 30 DAYS AFTER ORIGINAL PURCHASE, SUBJECT TO THE RETURN PROCESS AND POLICIES OF THE PARTY FROM WHICH YOU PURCHASED SUCH PRODUCT OR SOFTWARE.

## Software Licenses:

The software Licenses applicable to software from Linksys are made available at the Linksys public web site at: [www.linksys.com](http://www.linksys.com) and [www.linksys.com/gpl/](http://www.linksys.com/gpl/) respectively. For your convenience of reference, a copy of the Linksys Software License Agreement and the main open source code licenses used by Linksys in its products are contained in the Schedules below.

### Schedule 1 Linksys Software License Agreement

THIS LICENSE AGREEMENT IS BETWEEN YOU AND CISCO-LINKSYS LLC OR ONE OF ITS AFFILIATES CISCO SYSTEMS-LINKSYS (ASIA) PTE LTD. OR CISCO-LINKSYS K.K. ("LINKSYS") LICENSING THE SOFTWARE INSTEAD OF CISCO-LINKSYS LLC. BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE PRODUCT CONTAINING THE SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THESE TERMS, THEN YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE. YOU MAY RETURN UNUSED SOFTWARE (OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, THE UNUSED PRODUCT) FOR A FULL REFUND UP TO 30 DAYS AFTER ORIGINAL PURCHASE, SUBJECT TO THE RETURN PROCESS AND POLICIES OF THE PARTY FROM WHICH YOU PURCHASED SUCH PRODUCT OR SOFTWARE.

**License.** Subject to the terms and conditions of this Agreement, Linksys grants the original end user purchaser of the Linksys product containing the Software ("You") a nonexclusive license to use the Software solely as embedded in or (where authorized in the applicable documentation) for communication with such product. This license may not be sublicensed, and is not transferable except to a person or entity to which you transfer ownership of the complete Linksys product containing the Software, provided you permanently transfer all rights under this Agreement and do not retain any full or partial copies of the Software, and the recipient agrees to the terms of this Agreement.

"Software" includes, and this Agreement will apply to (a) the software of Linksys or its suppliers provided in or with the applicable Linksys product, and (b) any upgrades, updates, bug fixes or modified versions ("Upgrades") or backup copies of the Software supplied to You by Linksys or an authorized reseller, provided you already hold a valid license to the original software and have paid any applicable fee for the Upgrade.

**Protection of Information.** The Software and documentation contain trade secrets and/or copyrighted materials of Linksys or its suppliers. You will not copy or modify the Software or decompile, decrypt, reverse engineer or disassemble the Software (except to the extent expressly permitted by law notwithstanding this provision), and You will not disclose or make available such trade secrets or copyrighted material in any form to any third party. Title to and ownership of the Software and documentation and any portion thereof, will remain solely with Linksys or its suppliers.

**Collection and Processing of Information.** You agree that Linksys and/or its affiliates may, from time to time, collect and process information about your Linksys product and/or the Software and/or your use of either in order (i) to enable Linksys to offer you Upgrades; (ii) to ensure that your Linksys product and/or the Software is being used in accordance with the terms of this Agreement; (iii) to provide improvements to the way Linksys delivers technology to you and to other Linksys customers; (iv) to enable Linksys to comply with the terms of any agreements it has with any third parties regarding your Linksys product and/or Software and/or (v) to enable Linksys to comply with all applicable laws and/or regulations, or the requirements of any regulatory authority or government agency. Linksys and/or its affiliates may collect and process this information provided that it does not identify you personally. Your use of your Linksys product and/or the Software constitutes this consent by you to Linksys and/or its affiliates' collection and use of such information and, for EEA customers, to the transfer of such information to a location outside the EEA.

**Software Upgrades etc.** If the Software enables you to receive Upgrades, you may elect at any time to receive these Upgrades either automatically or manually. If you elect to receive Upgrades manually or you otherwise elect not to receive or be notified of any Upgrades, you may expose your Linksys product and/or the Software to serious security threats and/or some features within your Linksys product and/or Software may become inaccessible. There may be circumstances where we apply an Upgrade automatically in order to comply with changes in legislation, legal or regulatory requirements or as a result of requirements to comply with the terms of any agreements Linksys has with any third parties regarding your Linksys product and/or the Software. You will always be notified of any Upgrades being delivered to you. The terms of this license will apply to any such Upgrade unless the Upgrade in question is accompanied by a separate license, in which event the terms of that license will apply.

**Open Source Software.** The GPL or other open source code incorporated into the Software and the open source license for such source code are available for free download at <http://www.linksys.com/gpl>. If You would like a copy of the GPL or other open source code in this

Software on a CD, Linksys will mail to You a CD with such code for \$9.99 plus the cost of shipping, upon request.

**Term and Termination.** You may terminate this License at any time by destroying all copies of the Software and documentation. Your rights under this License will terminate immediately without notice from Linksys if You fail to comply with any provision of this Agreement.

**Limited Warranty.** The warranty terms and period specified in the applicable Linksys Product User Guide shall also apply to the Software.

**Disclaimer of Liabilities.** IN NO EVENT WILL LINKSYS OR ITS SUPPLIERS BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, REGARDLESS OF CAUSE (INCLUDING NEGLIGENCE), ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE 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 under this Agreement 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.

**Export.** Software, including technical data, may be subject to U.S. export control laws and regulations and/or export or import regulations in other countries. You agree to comply strictly with all such laws and regulations.

**U.S. Government Users.** The Software and documentation qualify as "commercial items" as defined at 48 C.F.R. 2.101 and 48 C.F.R. 12.212. All Government users acquire the Software and documentation with only those rights herein that apply to non-governmental customers.

**General Terms.** This Agreement will be governed by and construed in accordance with the laws of the State of California, without reference to conflict of laws principles. The United Nations Convention on Contracts for the International Sale of Goods will not apply. If any portion of this Agreement is found to be void or unenforceable, the remaining provisions will remain in full force and effect. This Agreement constitutes the entire agreement between the parties with respect to the Software and supersedes any conflicting or additional terms contained in any purchase order or elsewhere.

## END OF SCHEDULE 1

## Schedule 2

If this Linksys product contains open source software licensed under Version 2 of the "GNU General Public License" then the license terms below in this Schedule 2 will apply to that open source software. The license terms below in this Schedule 2 are from the public web site at <http://www.gnu.org/copyleft/gpl.html>

---

### GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

### **Preamble**

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software—to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

### **TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION**

**0.** This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

**1.** You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

**2.** You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

**3.** You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

**4.** You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

**5.** You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

**6.** Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

**7.** If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

**8.** If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

**9.** The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

**10.** If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

## **NO WARRANTY**

**11.** BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE

STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

**12.** IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

**END OF TERMS AND CONDITIONS**

**END OF SCHEDULE 2**

**Schedule 3**

If this Linksys product contains open source software licensed under the OpenSSL license then the license terms below in this Schedule 3 will apply to that open source software. The license terms below in this Schedule 3 are from the public web site at <http://www.openssl.org/source/license.html>

---

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

OpenSSL License

```
-----
/*
=====
===
```

Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

=====  
 This product includes cryptographic software written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)). This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

Original SSLeay License

-----

Copyright (C) 1995-1998 Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com))

All rights reserved.

This package is an SSL implementation written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

**END OF SCHEDULE 3**

# Contacts

For additional information or troubleshooting help, refer to the User Guide on the CD-ROM. Additional support is also available by phone or online.

## US/Canada Contacts

24-Hour Technical Support

800-326-7114

RMA (Return Merchandise Authorization)

<http://www.linksys.com/warranty>

Website

<http://www.linksys.com>

FTP Site

<ftp://ftp.linksys.com>

Support

<http://www.linksys.com/support>

Sales Information

800-546-5797 (800-LINKSYS)

## EU Contacts

Website

<http://www.linksys.com/international>

Product Registration

<http://www.linksys.com/registration>

# 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 requires 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 using 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 from 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 4: Using the Console Interface for Configuration** to configure HyperTerminal to connect to the Switch.

```

console - HyperTerminal
File Edit View Call Transfer Help

--- Performing Power-On Self Tests (POST) ---
Timer Test ..... PASS
UART Loopback Test ..... PASS
POE UART Loopback Test ..... PASS
DRAM Test ..... PASS
Switch Int Loopback Test ..... PASS
Done All Pass.
----- DONE -----

File Name                               S/Up Type Size      Create Time
-----
$logfile_1                               0 3         64      1193046:28:15
Factory_Default_Config.cfg               0 5         354     24:00:28
SRW2024F_boot_v1021.bix                  1 1      1286876 24:02:43
SRW2024F_image.bix                       1 2     3371724 24:26:35
certificate                               0 8        18040 24:00:21
startup-config                           1 5         3350 24:10:06
startup1.cfg                             0 5         2921 24:00:39

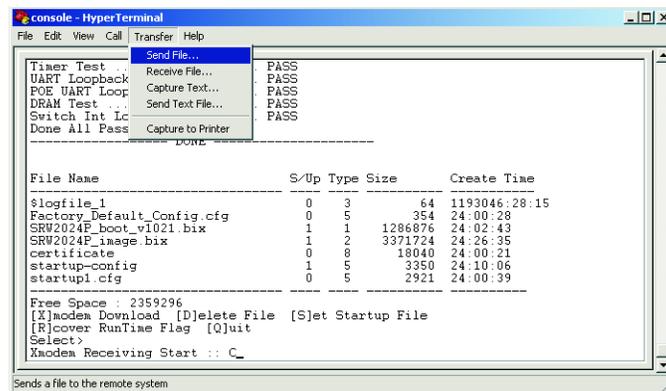
Free Space : 2359296
[X]modem Download [D]elete File [S]et Startup File
[R]cover RunTime Flag [Q]uit
Select>

Connected 3:30:20 | VT100 | 38400 8-N-1 | SCROLL | CAPS | NUM | Capture | Print echo

```

4. Power on the Switch and watch for the POST done message: *Done All Pass.*
5. When the POST done message appears, press and hold Ctrl and press the U key 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

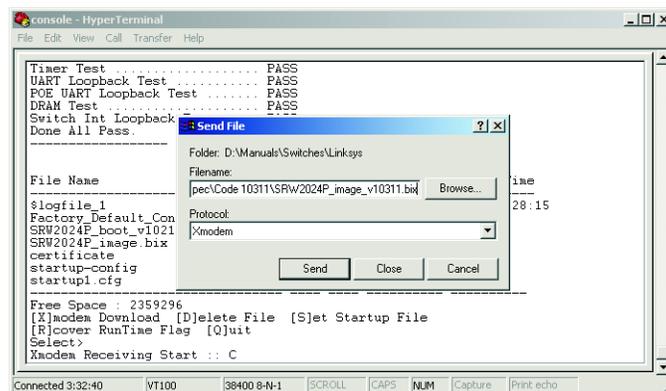
“Xmodem file send” window displays the progress of the download procedure. Note: The download file must be a valid binary software file from Linksys for the target switch.



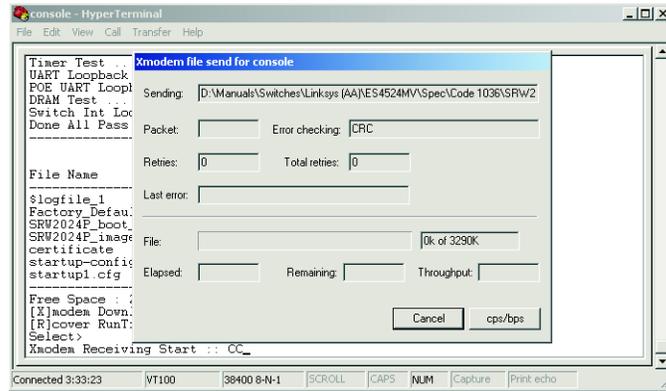
- After the file has been downloaded, you are prompted with “Update Image File:” to specify the type of code file. Press <R> for runtime code, <D> for diagnostic code, or,<L> for loader code.

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.

- 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 will reboot 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 Control List)**—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.

**Burst Size**—Indicates the burst size transmitted at a faster than normal rate.

**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** (Committed Burst Size)—Indicates the maximum number of data bits transmitted within a specific time interval.

**CIR** (Committed Information Rate)—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**—Specifies a group of users which retain the same system access rights.

**CoS** (Class of Service)—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** (Dynamic Domain Name System)—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** (Dynamic Host Configuration Protocol)—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** (Domain Name Server)—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** (Digital Subscriber Line)—An always-on broadband connection over traditional phone lines.

**DSCP** (DiffServe Code Point) provides a method of tagging IP packets with QoS priority information.

**Dynamic IP Address**—A temporary IP address assigned by a DHCP server.

**EIGRP** (Enhanced Interior Gateway Routing Protocol)—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 is implemented by the higher speed device refraining from sending packets.

**FTP** (File Transfer Protocol)—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** (General Attributes Registration Protocol)—Registers client stations into a multicast domain.

**Gateway**—A device that interconnects networks with different, incompatible communications protocols.

**GBIC** (GigaBit Interface Converter)—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** (GARP VLAN Registration Protocol)—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** (HyperText Transport Protocol)—The communications protocol used to connect to servers on the World Wide Web.

**HTTPS** (HyperText Transport Protocol Secure)—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 Control Message Protocol)—Allows the gateway or destination host to communicate with the source host. For example, to report a processing error.

**IGMP** (Internet Group Management Protocol)—Allows hosts to notify their local switch or router that they want to receive transmissions assigned to a specific multicast group.

**IP** (Internet Protocol)—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** (Internet Protocol Security)—A VPN protocol used to implement secure exchange of packets at the IP layer.

**ISP** (Internet Service Provider)—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** (Link Aggregated Group)—Aggregates ports or VLANs into a single virtual port or VLAN.

**LAN**—The computers and networking products that make up your local network.

**MAC** (Media Access Control) 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** (MegaBits Per Second)—One million bits per second; a unit of measurement for data transmission.

**MD5** (Message Digest 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** (Media Dependent Interface) A cable used for end stations.

**MDIX** (Media Dependent Interface with Crossover)—A cable used for hubs and switches.

**MIB** (Management Information Base)—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** (Network Management System)—An interface that provides a method of managing a system.

**OID** (Object Identifier)—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** (Packet INternet Groper)—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 over Ethernet** (PoE)—A technology enabling an Ethernet network cable to deliver both data and power.

**QoS** (Quality of Service) -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** (Remote Authentication Dial-In User Service)—A protocol that uses an authentication server to control network access.

**RJ-45** (Registered Jack-45)—An Ethernet connector that holds up to eight wires.

**RMON** (Remote Monitoring)—Provides network information to be collected from a single workstation.

**Router**—A networking device that connects multiple networks together.

**RSTP** (Rapid Spanning Tree Protocol)—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** (Simple Mail Transfer Protocol)—The standard e-mail protocol on the Internet.

**SNMP** (Simple Network Management Protocol)—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** (Secure Socket Layer)—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** (Spanning Tree Protocol)—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-network)—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+** (Terminal Access Controller Access Control System Plus)—Proprietary Cisco enhancement to Terminal Access Controller Access Control System (TACACS). Provides additional support for authentication, authorization, and accounting.

**TCP** (Transmission Control Protocol)—A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

**TCP/IP** (Transmission Control Protocol/Internet Protocol)—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** (Trivial File Transfer Protocol)—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** (User Data Protocol)—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** (Uniform Resource Locator)—The address of a file located on the Internet.

**VLAN** (Virtual Local Area Networks)—Logical subgroups that constitute a Local Area Network (LAN). This is done in software rather than defining a hardware solution.

**WAN** (Wide Area Network)—Networks that cover a large geographical area.

**Wildcard Mask**—Specifies which IP address bits are used, and which bits are ignored. A wildcard 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.