LINKSYS®
A Division of Cisco Systems, Inc.

24-Port 10/100 + 2-Port Gigabit Switch

with WebView and Power over Ethernet

User Guide

WIRED

Model No. **SRW224P**

CISCO SYSTEMS

Copyright and Trademarks

WARNING: This product contains chemicals, including lead, known to the State of California to cause cancer, and birth defects or other reproductive harm. ***Wash hands after handling.***

How to Use This User Guide

This User Guide has been designed to make understanding networking with the Switch easier than ever. Look for the following items when reading this User Guide:

This checkmark means there is a note of interest and is something you should pay special attention to while using the Switch.

This exclamation point means there is a caution or warning and is something that could damage your property or the Switch.

This question mark provides you with a reminder about something you might need to do while using the Switch.

In addition to these symbols, there are definitions for technical terms that are presented like this:

word: *definition.*

Also, each figure (diagram, screenshot, or other image) is provided with a figure number and description, like this:

Figure 0-1: Sample Figure Description

Figure numbers and descriptions can also be found in the “List of Figures” section in the “Table of Contents”.

Table of Contents

List of Figures

Chapter 1: Introduction

Welcome

Thank you for choosing the 24-port 10/100 + 2-Port Gigabit Switch with WebView and Power over Ethernet. This Switch will allow you to network better than ever.

This new Linksys rackmount Switch delivers non-blocking, wire speed switching for your 10 and 100 megabit network clients, plus multiple options for connecting to your network backbone. Twenty-four 10/100 ports wire up your workstations, while the two integrated 10/100/1000BaseTX ports connect to other switches and the backbone at Gigabit speeds. And the mini-GBIC ports allow future expansion through alternate transmission media like optical fiber.

All the 10/100 ports on this Switch support IEEE 802.3af standard (802.3af) Power-over-Ethernet (PoE) capabilities. Each port can detect connected 802.3af-compliant network devices, such as IP phones or wireless access points, and automatically supply the required DC power.

The Switch can provide DC power to a wide range of connected devices, eliminating the need for an additional power source and cutting down on the amount of cables attached to each device. 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-PoE devices.

The Switch features WebView monitoring and configuration via your web browser, making it easy to manage the 128 VLANs and up to 4 lagging groups. Or if you prefer, you can use the integrated console port to configure the Switch. The non-blocking, wire-speed switching forwards packets as fast as your network can deliver them.

All ports have automatic MDI/MDI-X crossover detection. Each port independently and automatically negotiates for best speed and whether to run in half- or full-duplex mode. Head-of-line blocking prevention keeps your high-speed clients from bogging down in lower-speed traffic and fast store-and-forward switching prevents damaged packets from being passed on into the network.

Use the instructions in this User Guide to help you connect the Switch, set it up, and configure it to bridge your different networks. These instructions should be all you need to get the most out of the 24-port 10/100 + 2-Port Gigabit Switch with WebView and Power over Ethernet.

What's in this Guide?

This user guide covers the steps for setting up and using the Switch.

- Chapter 1: Introduction
  This chapter describes the Switch's applications and this User Guide.
- Chapter 2: Getting to Know the Switch
  This chapter describes the physical features of the Switch.
- Chapter 3: Connecting the Switch
  This chapter describes how to connect the Switch.
- Chapter 4: Configuration using the Console Interface
  This chapter instructs you on how to use the Switch's console interface for configuring the Switch.
- Chapter 5: Configuring the Switch through the Web Utility
  This chapter shows you how to configure the Switch using the Web Utility.
- Appendix A: Fast Ethernet and Gigabit Ethernet
  This appendix describes the various types of ethernet.
- Appendix B: Cabling
  This appendix discusses different types of cabling.
- Appendix C: Glossary
  This appendix gives a brief glossary of terms frequently used in networking.
- Appendix D: Specifications
  This appendix provides the Switch's technical specifications.
- Appendix E: Warranty Information
  This appendix supplies the Switch's warranty information.
- Appendix F: Regulatory Information
  This appendix supplies the Switch's regulatory information.
- Appendix G: Contact Information
  This appendix provides contact information for a variety of Linksys resources, including Technical Support.

Chapter 2: Getting to Know the Switch

The Front Panel

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

Figure 2-1: Front Panel

LEDs

System — A green LED indicates that power is being supplied to the Switch. A solid, amber LED indicates that the Switch's power-on-self-test (POST) is in progress, but when this blinks amber that indicates that the POST has failed.

Link/Act — A green LED indicates a functional network link through the corresponding port (1 through 26) with an attached device. A blinking LED indicates that the Switch is actively sending or receiving data over that port.

PoE — A green LED indicates a powered device is connected to the corresponding port (1 through 24).

Speed — A green LED indicates a link to the corresponding port (Gigabit ports 25 and 26) is operating at 1000Mbps. No light indicates either no link or a link operating at a speed of 10/100Mbps.

Ports

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

Gigabit1 (25)/Gigabit 2 (26) The Switch is equipped with two Gigabit RJ-45 ports that are shared with two mini-GBIC ports. If a Gigabit mini-GBIC port is being used, the associated RJ-45 port cannot be used. They link to high-speed network peripheral system or clients at speeds of up to 1000Mbps.

Console The Console port is where you connect a serial cable from a PC's serial port.

The Back Panel

The power port is located on the back panel.

Figure 2-2: Back Panel

Power The Power port is where you will connect the power cord.

The Side Panel

A security slot, where you can attach a lock to protect the Switch, is located on a side panel.

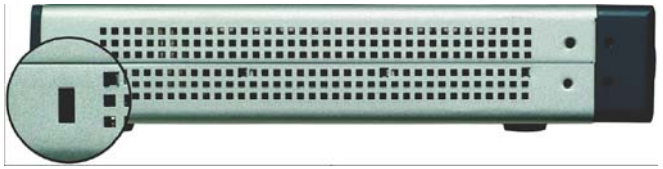

Figure 2-3: Side Panel

RJ-45 Ports

The Switch is equipped with 24 auto-sensing RJ-45 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 a network cable. You will need to use Category 5 (or better) cable. For more information on twisted-pair cabling, refer to *Appendix B: Cabling*.

The Gigabit Expansion Ports

The Switch is equipped with two Gigabit Ethernet ports that have shared mini-GBIC ports, 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 *Appendix B: Cabling*

The Console Port

The Switch is equipped with a serial port labeled CONSOLE (located on the front 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 for more information about products that work with the Switch.

Chapter 3: Connecting the Switch

Overview

This chapter will explain how to connect network devices to the Switch. The following diagram shows a typical network configuration.

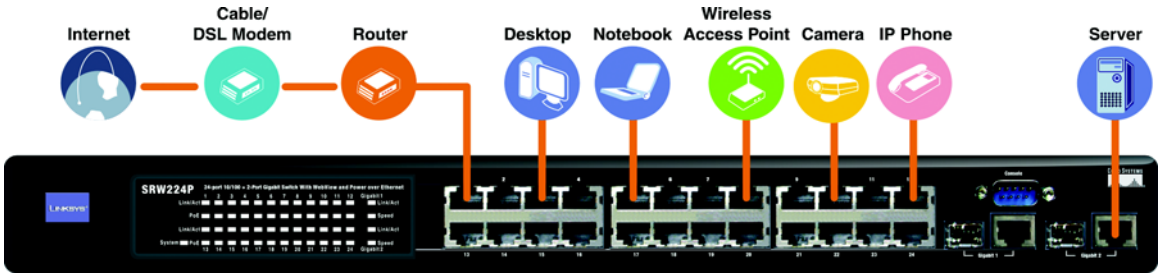

Figure 3-1: Typical Network Configuration

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

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)

*A hub refers to any type of 100Mbps hub. A 10Mbps hub connected to another 10Mbps hub can span up to 100 meters (328 feet).

Pre-Installation Considerations

Fast Ethernet Considerations

If you will be using the Switch for Fast Ethernet (100Mbps) applications, you must observe the following guidelines:

Full-Duplex

As previously mentioned, the Switch provides full-duplex support for its RJ-45 ports. Full-duplex operation allows data to be sent and received simultaneously, doubling a port's potential data throughput.

If you will be using the Switch in full-duplex mode, the maximum cable length using Category 5 cable is 328 feet (100 meters).

Positioning the Switch

Before you choose a location for the Switch, observe the following guidelines:

1. Make sure that the Switch is accessible and that the cables can be connected easily.
2. Keep cabling away from sources of electrical noise, power lines, and fluorescent lighting fixtures.
3. Position the Switch away from water and moisture sources.
4. To ensure adequate air flow around the Switch, be sure to provide a minimum clearance of two inches (50mm).
5. Do not stack free-standing Switches more than four units high.
6. Connect Network Devices

Hardware Installation

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. Connect a Category 5 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 802.3af-compliant PoE devices are connected to the Switch's 10/100 ports, the Switch automatically supplies the required power.
5. If you are using the Gigabit port, connect a Category 5e Ethernet network cable to the Gigabit port on the Switch, and connect the other end to a Gigabit server or other network device.
6. If you are using a mini-GBIC port, then connect a mini-GBIC module to the mini-GBIC port. For detailed instructions, refer to the module's documentation.
7. Connect the supplied power cord to the Switch's power port, and plug the other end into an electrical outlet. When connecting power, always use a surge protector.
8. Power on the devices connected to the Switch. Each active port's corresponding LED will light up on the Switch.

IMPORTANT: Make sure to use the power cord that is supplied with the Switch. Use of a different power cord could damage the Switch.

NOTE: If you need to reset the Switch, remove the power cord from the back of the Switch and then reconnect it.

Placement Options

There are two ways to 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 high rack for rack-mount placement.

Desktop Placement

1. Attach the rubber feet to the recessed areas on the bottom of the Switch.
2. Place the Switch on a desktop near an AC power source.
3. Keep enough ventilation space for the Switch and check the environmental restrictions mentioned in *Appendix D: Specifications* as you are placing the Switch.
4. Connect the Switch to network devices according to the Hardware Installation instructions above.

Figure 3-2: Attaching the Switch's Rubber Feet

Rack-Mount Placement

To rack-mount the Switch in any standard 19-inch rack, follow the instructions described below.

1. Place the Switch on a hard flat surface with the front panel faced towards your front side
2. Attach a rack–mount bracket to one side of the Switch with the supplied screws.

Figure 3-3: Attaching Brackets to the Switch

3. Secure the brackets tightly.
4. Follow the same steps to attach the other bracket to the opposite side.
5. After the brackets are attached to the Switch, use suitable screws to securely attach the brackets to any standard 19-inch rack.

IMPORTANT: Make sure to use the power cord that is supplied with the Switch. Use of a different power cord could damage the Switch.

Figure 3-4: Mounting the Switch

6. Connect the Switch to network devices according to the Hardware Installation instructions above.

Uplinking the Switch

To uplink the Switch, connect one end of a Cat5 (or better) cable into one of the 24 10/100 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.

The hardware installation is complete. Proceed to Chapter 4: Configuration using the Console Interface, for directions on how to set up the Switch.

Chapter 4: Configuration using the Console Interface

Overview

The Switch features a menu-driven console interface for basic configuration. You can easily manage your network from the screens through the console port. Before you can use the console interface, you will need to configure the HyperTerminal application.

Configuring the HyperTerminal Application

1. Click the **Start** button. Select **Accessories** and then select **Communications**. **HyperTerminal** should be one of the options listed in the next menu. Select **HyperTerminal** to run the utility program.
2. Enter a name for this connection. In the example shown, the name of connection is SRW224P. Select an icon for the application. Click **OK**.
3. Select a port to communicate with the Switch. Select **COM1** or **COM2**.
4. Set the serial port settings, as follows, then click **OK**. These settings should be:
   - Bits per Second: **38400**
   - Databits: **8**
   - Parity: **None**
   - Stop bits: **1**
   - Flow control: **None**

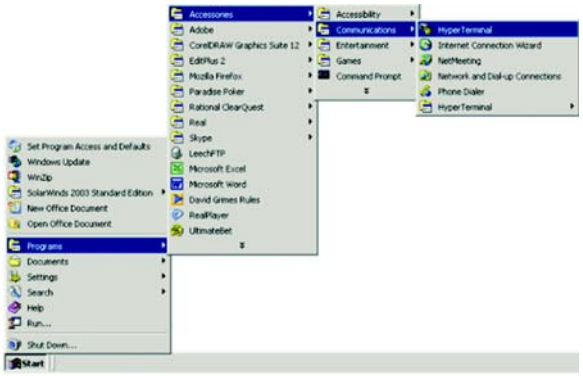

Figure 4-1: Finding Hyperterminal

Figure 4-2: Connection Description

Figure 4-3: Password Screen

Configuring the Switch through the Console Interface

Login

When you finish configuring HyperTerminal, the Login screen will appear. The first time you open the console interface, use the default username **admin**, and leave the password blank. You can set a new password later from the Password Setting screen.

Switch Screens

The console interface screens consist of a series of menus. Each menu has several options, which are listed vertically. A highlight in each menu lets you select the option you wish to choose; pressing the Enter key activates the highlighted option.

To navigate through the Console Interface use the Up Arrow or Down Arrow keys to move up or down, or use the number keys to select the respective option (for example, press the *5* key to highlight help) use the **Enter** key to select, and the **Esc** key to return to the previous selection; menu options and any values entered or present will get highlighted. The bottom of the window always has a listing of the appropriate key strokes.

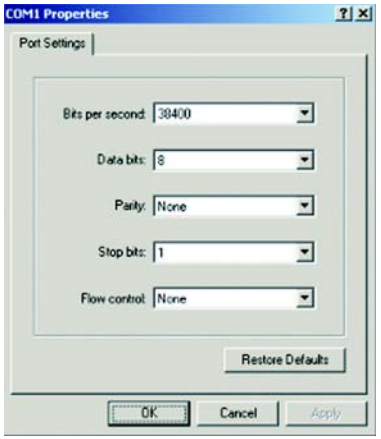

Figure 4-4: COM1 Properties

Figure 4-5: Login

Switch Main Menu

The Main Menu screen displays six menu choices: System Configuration Menu, Port Status, Port Configuration, PoE Configuration, Help, and Logout.

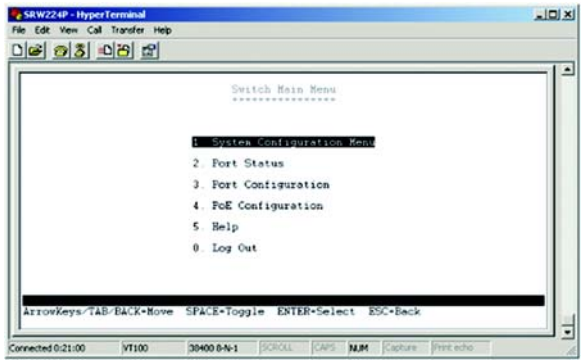

Figure 4-6: Switch Main Menu

System Configuration Menu

System Configuration Menu displays:

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

Figure 4-7: System Configuration Menu

System Information

In System Information, you can check the Versions and General Information.

Figure 4-8: System Information

Versions

The version screen displays the Boot Version, Software Version, Loader Version and the Hardware Version.

Boot Version. This file runs when the Switch is turned on. It loads the operating system for the Switch.

Software Version. This file contains the programming code that runs the Switch.

Loader Version. This file loads the software from storage memory to main memory.

Hardware Version. The current hardware setup of the Switch.

Figure 4-9: Versions

General Information

The General Information screen displays the System Description, System Up Time, System Mac Address, System Contact, System Name and System Location

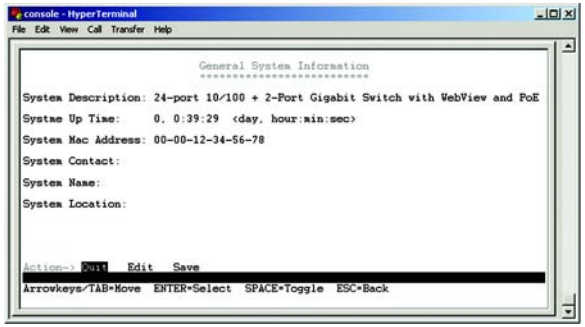

Figure 4-10: General Information

Management Settings

The Management Settings screen displays two menu choices: Serial Port Configuration and CPU Performance

Serial Port Configuration

The Serial Port Configuration screen displays the current setting for the baud rate. The baud rate can be changed by selecting **edit** then using the spacebar to toggle through the different baud rates. Use the **save** action to set the new baud rate.

Figure 4-11: Serial Port Configuration

CPU Performance

The CPU performance screen displays the percentage of processor power being used by the Switch.

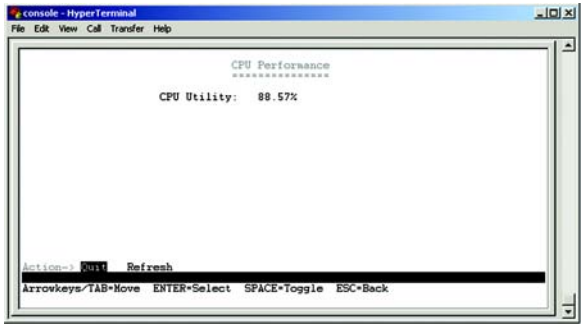

Figure 4-12: CPU Performance

User and Password Settings

The User & Password Settings screen displays user account information on the Switch. The default account is the administrator account. To add a new user, use the arrow keys to select **edit** then enter the username of the new account and assign a password to the account. The password must be re-entered into the **Again Password** column to cofirm the password.

To save the new user account information, use the arrow key to select **save** and press enter.

NOTE: While only five accounts can be configured through the Switch's console interface, up to 16 can be configured with the Switch's web interface.

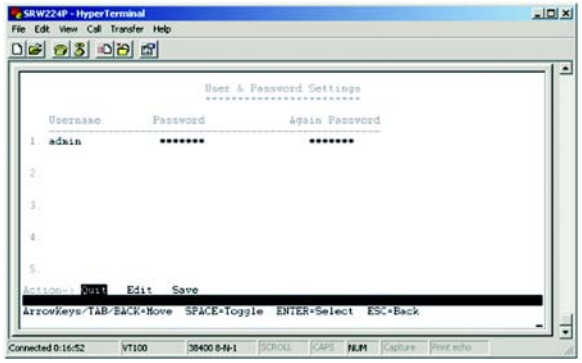

Figure 4-13: User and Password Settings

IP Configuration

The IP Configuration screen displays four menu choices: IP Address Settings, HTTP, SNMP and Network Configuration.

Figure 4-14: IP Configuration

IP Address Settings

The IP Address Settings screen allows you to set the IP information for the Switch.

IP Address. This sets the Switch's IP Address. The default setting is 192.168.1.254.

Subnet Mask. This combined with the IP Address defines the Switch's network address.

Default Gateway. This defines the IP Address for the default gateway of the network.

Management VLAN. 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. However, 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.

Figure 4-15: IP Address Configuration Screen

HTTP

The HTTP screen allows you to set the Hyper Text Transfer Protocol information for the Switch.

HTTP Server. Enable or Disable the Switch's HTTP server function.

HTTP Server port. Set the TCP port which 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 witch HTTPS packets are sent and received from.

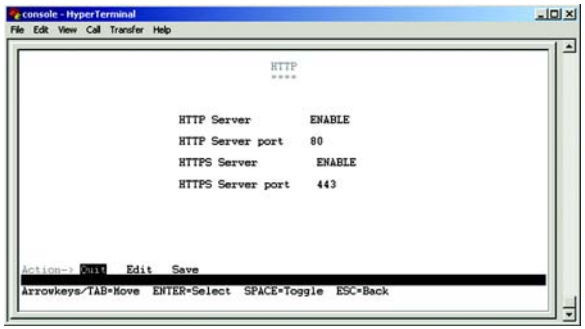

Figure 4-16: HTTP

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

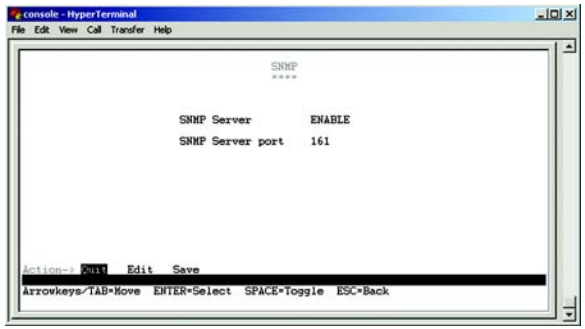

Figure 4-17: SNMP

Network Configuration

The Network Configuration Screen allows you to use PING to test network connectivity. Enter the IP address of the interface or device you wish to PING and select the **Execute** action.

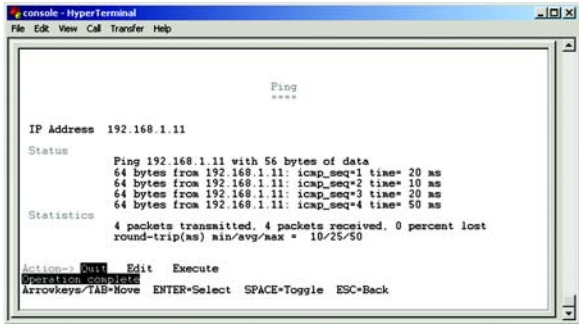

Figure 4-18: Network Configuration/PING

File Management

The File Management screen allows you to upload and download files to the Switch using TFTP.

Source File. Specify the location of the file to transfer. Select TFTP if the file is on a TFTP server, Image if the file is a local image file, or startup-config if the file is a local configuration file.

Destination File. Specify where the file is to be transferred. Select TFTP if the file is to be uploaded to a TFTP server, Image if the file is to be downloaded as a image file, startup-config if the file is a configuration file, or boot if the file is a boot file.

File Name. Enter the name of the file to be uploaded or downloaded.

IP Address. Enter the IP address of the TFTP server that will transfer the file.

Figure 4-19: File Management

Restore System Default Setting

To restore the Switch back to the factory default settings, select Restore System Default Setting and press **Enter**. A confirmation message will appear stating that All User Configuration data will be reset to Default. Continue? [y/n]. Press the "y" key to continue or the "n" key to cancel the action.

Figure 4-20: Restore System Default Settings

Reboot System

If you would like to reboot the Switch, select **Reboot System** and press **Enter**.

Figure 4-21: Reboot System

Back to Main Menu

Select **Back to Main Menu** if you want to return to the main menu.

Figure 4-22: Back to Main Menu

Port Status

This screen allows you to view the status of a port. The Port, Enable, Link Status, Spd/Dpx, and Flow Control are displayed.

Ports 1 through 24 are ethernet RJ-45 ports and ports 25 and 26 are Gigabit RJ-45 ports, Giga1 and Giga2. Each Gigabit port has a shared mini-Gbic port. If there is a connection to one of the mini-Gbic ports then the corresponding Gigabit RJ-45 port cannot be used.

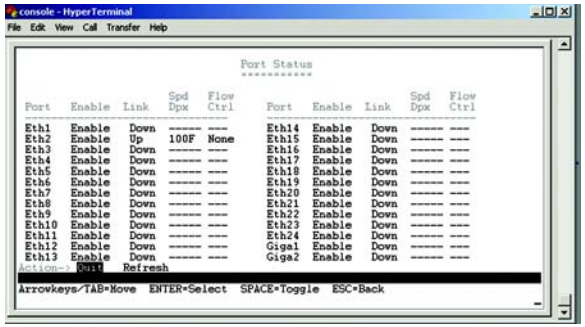

Figure 4-23: Port Status

Port Configuration

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

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

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

- **10half** - Supports 10 Mbps half-duplex operation
- **10full** - Supports 10 Mbps full-duplex operation
- **100half** - Supports 100 Mbps half-duplex operation
- **100full** - Supports 100 Mbps full-duplex operation
- **1000full** (Gigabit only)- Supports 1000 Mbps full-duplex operation
  (Default: Autonegotiation 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.

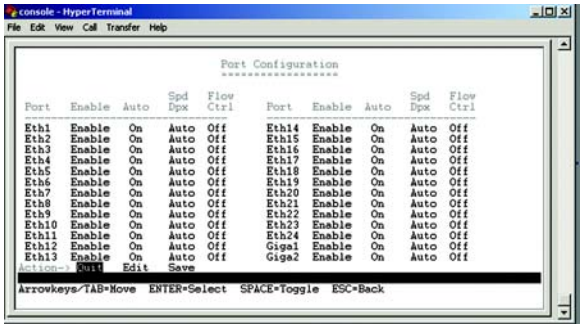

Figure 4-24: Port Configuration

PoE Configuration

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

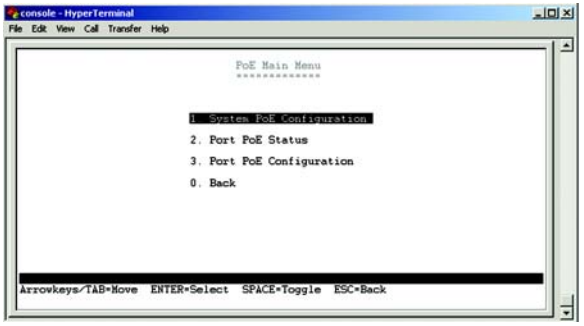

Figure 4-25: PoE Main Menu

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.

Figure 4-26: Power Configuration

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.

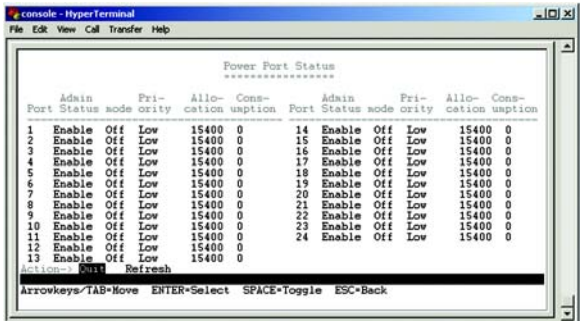

Figure 4-27: Power Port Status

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. Use the Save action to save the new settings.

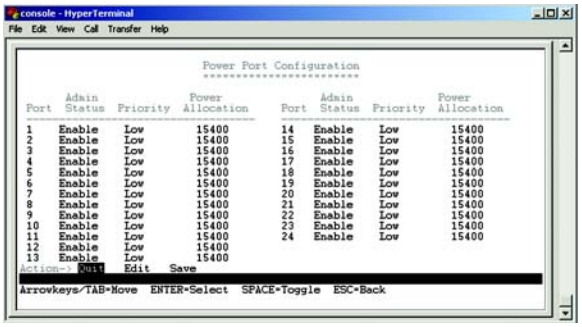

Figure 4-28: Power Port Configuration

Logout

Select Logout to log out of the console configuration utility.

Figure 4-29: Logout

Chapter 5: Configuring the Switch through the Web Utility

Overview

Open your web browser and enter **192.168.1.254** into the address field. Press the **Enter** key and the Password screen will appear. The first time you open the Web-Based Utility, use the default username **admin**, and leave the password blank. Click the **OK** button. You can set a new password later from the *Security* tab's *System Password* screen.

NOTE: The default IP address is 192.168.1.254. If the IP address has been changed using DHCP or the console interface, enter the assigned IP address.

The first screen that appears displays the System Description screen for the Sys.Info tab. There are 14 tabs that run across the top of the screen: Sys.Info, IP Conf, Switch Conf., QoS, DiffServ, Security, SNTP, Statistics, PoE, Spanning Tree, SNMP, IGMP, Maintenance and Help. Each tab contains further screens, described in this chapter, to help you configure and manage the Switch.

Figure 5-1: Address Field

Figure 5-2: Password Screen

Figure 5-3: Sys. Info - System Description

System Information

The System Information tab includes links to the following screens.

- System Description
- System Mode
- Forwarding Database
- Time Synchronization
- CPU Performance
- Logout

System Description

The System Description screen displays the following information.

Model Name. This displays the switch's name.

System name. Assign a name to the switch system, up to 255 characters long.

System Location. Assign a name to the system location, up to 255 characters long.

System Contact. Enter the name of the administrator responsible for the system, up to 255 characters long.

System up time. Length of time the management agent has been up.

IP Address. The IP Address assigned to the Switch is displayed. (The default IP address is 192.168.1.254.)

Base MAC Address. The MAC Address of the switch is displayed.

Hardware version. The current hardware version is displayed.

Software version. The current software version is displayed.

Click the **Submit** button after you have verified that the information is correct.

Figure 5-4: Sys. Info - System Information

System Mode

The System Mode screen displays the following information.

Jumbo Frames. Shows if jumbo frames are enabled.

This switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames up to 9216 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 will limit the maximum threshold for broadcast storm control to 64 packets per second. The current setting for jumbo frames can be displayed with the show system command.

Use the drop-down menu to **Enable** or **Disable** the transmitting and receiving of Jumbo Frames for this switch.

Figure 5-5: Sys. Info - System Mode

Forwarding Database

The Forwarding Database screen displays the following information.

Aging Status. This feature, when enabled, discards dynamic MAC addresses after a set amount of time.

Aging Interval. 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.

Click **Submit** to save the changes.

To query a Dynamic IP address click on the Dynamic address icon.

To query a Static IP address click on the Static address icon.

Figure 5-6: Sys. Info - Forwarding Database

Address Table Settings

Switches store the addresses for all known devices. This information is used to pass 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.

Dynamic Address

The 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.

Interface. Indicates a port or lag.

MAC Address. Physical address associated with this interface.

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

Address Table Sort Key. You can sort the information displayed based on MAC address, VLAN or interface (port or lag).

Dynamic Address Counts. The number of addresses dynamically learned.

Current Dynamic Address Table. Lists all the dynamic addresses.

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

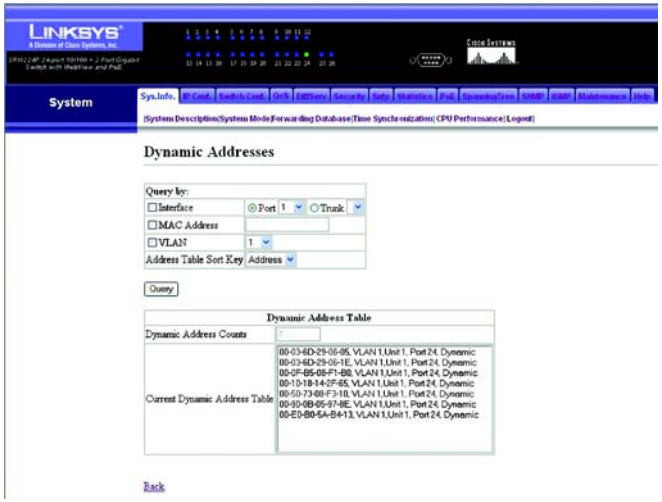

Figure 5-7: Dynamic Address Screen

Static address

A static address can be assigned to a specific interface on this 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 8,000 Static Address Counts.

Current Static Address Table. Lists all the static addresses.

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

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

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

Specify the interface, the MAC address and VLAN, then click **Add Static Address**.

Figure 5-8: Static Address Screen

Time Synchronization

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 three time server IP addresses. The switch will attempt to poll each server in the configured sequence.

Figure 5-9: Sys. Info - Time Synchronization Screen

The Time Synchronization screen displays the following information.

SNTP Client. Configures the switch to operate as an SNTP client. This requires at least one time server to be specified in the SNTP Server field. (Default: Disabled)

Current Time. Displays the current time.

Name. Assign a name for the time setting.

Hours. Set the hours for the clock.

Minutes. Set the minutes for the clock.

Direction. SNTP uses Coordinated Universal Time (or UTC, formerly Greenwich Mean Time, or GMT) based on the time at the Earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (after) or west (before) of UTC.

Click the SNTP Client checkbox to Enable SNTP Client. Uncheck it to disable it.

Set the name, hours and minutes using the text fields.

Set the Direction by choosing the Before-UTC or After-UTC.

Click **Submit** to save the changes.

CPU Performance

The CPU Performance screen displays the current percentage of processor power being used by the switch.

Figure 5-10: Sys. Info - CPU Performance

Logout

To logout, click the **Logout** hyper-link. Then click **OK** to proceed or **Cancel** to cancel. Then click **Yes** to close the window or **No** to cancel.

Figure 5-11: Sys. Info - Logout

IP Config

The IP Config tab includes a link to the following screen.

- IP Address

IP Address

To manually configure IP settings, you need to set an IP address and subnet mask that is compatible with your network. You may also need to establish a default gateway between the switch and management stations that exist on another network segment.

An IP address may be used for management access to the switch over your network. You may also need to establish a default gateway between the switch and management stations that exist on another network segment.

The IP Address screen displays the following information

IP Address Mode. Specifies whether IP functionality is enabled via manual configuration (Static), Dynamic Host Configuration Protocol (DHCP), or Boot Protocol (BOOTP). If DHCP/BOOTP is enabled, IP will not function until a reply has been received from the server. Requests will be broadcast periodically by the switch for an IP address. (DHCP/BOOTP values can include the IP address, subnet mask, and default gateway.)

Host Name. Specifies the name of the switch. Enter the name into the textfield provided, up to 255 characters long. (Default: None)

IP Address. Address of the VLAN interface that is allowed management access. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. (Default: 192.168.1.254)

Mask. This mask identifies the host address bits used for routing to specific subnets.
(Default: 255.255.255.0)

Default Gateway. IP address of the gateway router between this device and management stations that exist on other network segments. (Default: 0.0.0.0)

Current Management Interface. ID of the configured VLAN (1-4094, no leading zeroes). By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address.

Figure 5-12: IP Config - IP Address

Select the IP Address Mode using the drop-down menu. Selecting **Static** will allow you to enter a static IP address, subnet mask and default gateway using the text field provided. Selecting **BOOTP** or **DHCP** disables these text boxes and auto assigns an IP address.

Enter a name for each IP address using the textfield provided and the Current Management Interface using the drop-down menu box.

Click **submit** to save the changes.

Click **Restart DHCP** to assign a new IP address using DHCP.

Switch Config

The Switch Config tab includes links to the following screens.

- Port Configuration
- VLAN
- VLAN Port
- LAG Configuration
- Port Mirroring
- LACP

Port Configuration

You can manually configure the speed, duplex mode, and flow control used on specific ports, or use auto-negotiation to detect the connection settings used by the attached device. Use the full-duplex mode on ports whenever possible to double the throughput of switch connections. Flow control should also be enabled to control network traffic during periods of congestion and prevent the loss of packets when port buffer thresholds are exceeded. The switch supports flow control based on the IEEE 802.3x standard.

This screen displays the current connection status, including link state, speed/duplex mode, flow control, and auto-negotiation.

The Port Configuration screen displays the following information for each port on the switch.

Name. Enter a name for the port, up to 64 characters long.

Port Type. Indicates the port type. (100BASE-TX, 1000BASE-T, or SFP)

Admin Status. Shows if the interface is enabled or disabled.

Operating Status. Indicates if the link is Up or Down.

Speed Duplex. Shows the current speed and duplex mode. (Auto, or a fixed choice)

Figure 5-13: Switch Config - Port Configuration

Flow Control. Indicates the type of flow control currently in use. (IEEE 802.3x, Back-Pressure or None)

Auto Negotiation. Shows if auto-negotiation is enabled or disabled.

LAG Member. Shows if port is a LAG member.

Click **Port Configuration** to edit the port settings.

Click **Port Broadcast Control** to edit the port broadcast threshold.

Edit Port Configuration

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

This screen allows you to edit the following information for each port on the switch.

Name. Allows you to label an interface. (Range: 1-64 characters)

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

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

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

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

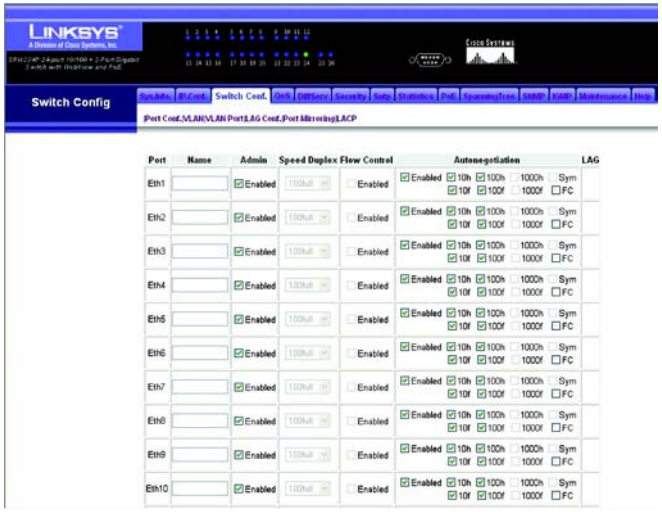

Figure 5-14: Edit Port Configuration Screen

- 100full - Supports 100 Mbps full-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.)
- FC - Supports 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)

LAG. Indicates if a port is a member of a LAG.

Modify the required interface settings, and click **submit**.

VLAN

A VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment.

VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as videoconferencing).

The VLAN screen displays the following information for each VLAN and each port.

Figure 5-15: Switch Config - VLAN

Selected VLAN. Lists all the current VLAN groups created for this system. Up to 128 VLAN groups can be defined. VLAN 1 is the default untagged VLAN.

Up Time at Creation. This displays the amount of time since this VLAN was created (that is, System Up Time).

Status. Shows if this VLAN is enabled or disabled.

VLAN ID. ID of configured VLAN (1-4094, no leading zeroes).

VLAN Name. Name of the VLAN (1 to 32 characters).

VLAN type. Shows how this VLAN was added to the switch.

- Default: The Switch's default VLAN.
- Static: Added as a static entry.

Member Information. Shows the VLAN interface members.

Tagging Information. Shows the tagging information for each port.

To display a particular VLAN, select the **Select VLAN ID** radio button and choose the VLAN ID from the drop-down menu.

To display all VLANs, click the **Show All** radio button.

To create a new VLAN, click **Create VLAN**.

To configure a VLAN, click VLAN Configuration.

Create VLAN

To create a VLAN, enter the VLAN ID and VLAN name, up to 32 characters long. Mark the **Enable** checkbox to activate the VLAN, and click **Create VLAN**.

To edit a VLAN, select a VLAN ID and click the Edit icon (which resembles a pen). Modify the VLAN name and status if required. Select the membership type by marking the appropriate radio button in the list of ports or lags. Click **Submit**.

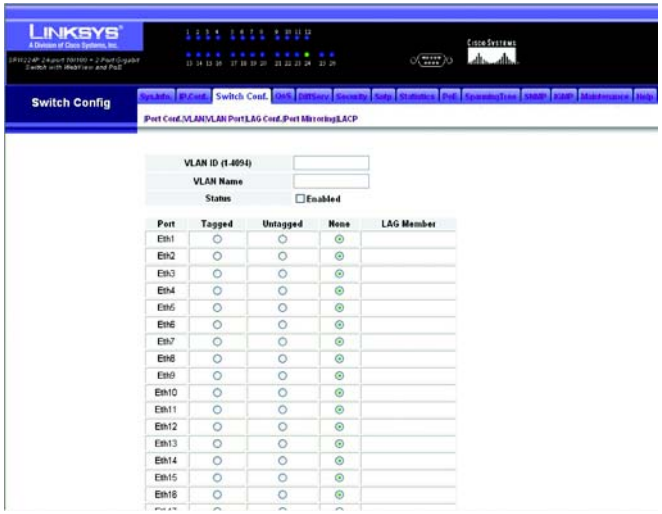

Figure 5-16: Adding/Editing VLAN Screen

Membership Type. Select VLAN membership for each interface by marking the appropriate radio button for a port or LAG:

- Tagged. Interface is a member of the VLAN. All packets transmitted by the port will be tagged, that is, carry a tag and therefore carry VLAN or CoS information.
- Untagged. Interface is a member of the VLAN. All packets transmitted by the port will be untagged, that is, not carry a tag and therefore not carry VLAN or CoS information. Note that an interface must be assigned to at least one group as an untagged port.
- None. Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.

VLAN Port

You can configure VLAN behavior for specific interfaces, including the default VLAN identifier (PVID), accepted frame types, ingress filtering and mode.

VLAN identifier (PVID). VLAN ID assigned to untagged frames received on the interface. (Default: 1)

- If an interface is not a member of VLAN 1 and you assign its PVID to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before you can assign its PVID to that group.

Accepted frame types. Sets the interface to accept all frame types, including tagged or untagged frames, or only tagged frames. When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN. (Options: All, Tagged; Default: All)

Ingress filtering. Determines how to process frames tagged for VLANs for which the ingress port is not a member. (Default: Disabled)

- Ingress filtering only affects tagged frames.
- If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).
- If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.
- Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STP. However, they do affect VLAN dependent BPDU frames, such as GMRP.

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

- Trunk – Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. Note that frames belonging to the port's default VLAN (that is, associated with the PVID) are also transmitted as tagged frames.
- General – Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.
- Access – Is the default setting for all ports.

Fill in the required settings for each interface, click **Submit**.

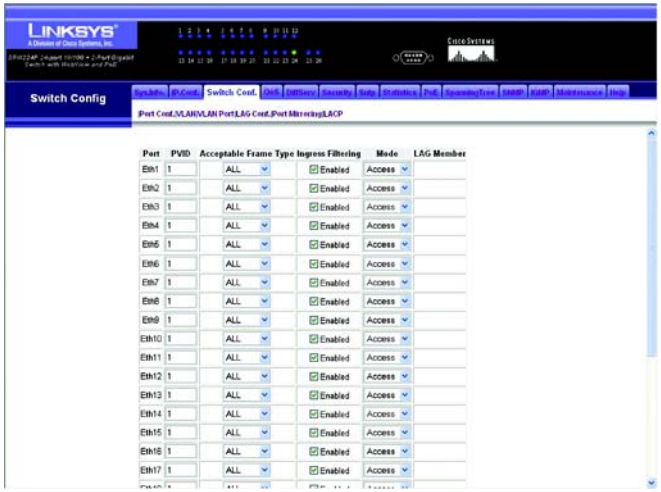

Figure 5-17: Switch Config - VLAN Port

LAG Configuration

You can create multiple links between devices that work as one virtual, aggregate link. An aggregated link offers a dramatic increase in bandwidth for network segments where bottlenecks exist, as well as providing a fault-tolerant link between two devices. You can create up to four lags on the switch. Each lag can contain up to eight ports.

The LAG Configuration screen displays the following information

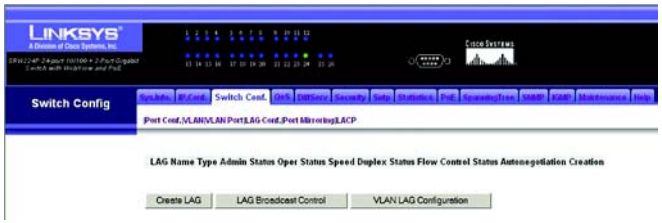

Figure 5-18: Switch Config - LAG Configuration

LagName. Shows you the label assigned to an interface. (Range: 1-64 characters)

Type. Indicates the port type. (100BASE-TX, 1000BASE-T, or SFP)

Admin Status. Shows if the interface is enabled or disabled.

Oper Status. Shows if the link is Up or Down.

Speed Duplex Status. Shows the current speed and duplex mode. (Auto, or fixed choice)

Flow Control Status. Indicates the type of flow control currently in use. (IEEE 802.3x, Back-Pressure or None)

Autonegotiation. Shows if auto-negotiation is enabled or disabled.

Creation. Shows if a lag is manually configured or dynamically set via LACP.

To create a new lag, click **Create Lag**.

To configure broadcast control on a lag, click **Lag Broadcast Control**.

To configure VLAN activity for a specific lag, click **VLAN Lag Configuration**.

Create LAG

Enter a lag ID of 1-4 in the *Lag* field, select any of the switch ports from the scroll-down port list, and click **Add**.

Figure 5-19: Create LAG Screen

LAG Broadcast Control

Set the threshold for any lag, click **Submit**.

Figure 5-20: LAG Broadcast Control Screen

VLAN LAG Configuration

You can configure VLAN behavior for specific lag, including the default VLAN identifier (PVID), accepted frame types, ingress filtering and mode.

Fill in the required settings for each lag, click **Submit**.

Acceptable Frame Type. Sets the interface to accept all frame types, including tagged or untagged frames, or only tagged frames. When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN. (Options: All, Tagged; Default: All)

Mode. Indicates VLAN membership mode for an interface.

- Trunk – Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. Note that frames belonging to the port's default VLAN (that is, associated with the PVID) are also transmitted as tagged frames.
- General – Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.
- Access – Is the default setting for all ports.

Figure 5-21: VLAN LAG Configuration Screen

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.

Monitor port speed should match or exceed source port speed, otherwise traffic may be dropped from the monitor port.

All mirror sessions have to share the same destination port.

When mirroring port traffic, the target port must be included in the same VLAN as the source port.

Set the following attributes for port mirroring using the Port Mirroring screen.

Mirror Sessions. Displays a list of current mirror sessions.

Source Port. The port whose traffic will be monitored.

Type. Allows you to select which traffic to mirror to the target port, Rx (receive), or Tx (transmit).

Target Port. The port that will mirror the traffic on the source port.

Specify the source port, the traffic type to be mirrored, and the target port, then click **Add**.

Figure 5-22: Switch Config - Port Mirroring

LACP

Ports can be statically grouped into an aggregate link (i.e., 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 this 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 four 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.

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

Set Port Partner – This menu sets the remote side of an aggregate link; that is, the ports on the attached device. The command attributes have the same meaning as those used for the port actor. However, configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Set the System Priority, Admin Key, and Port Priority for the Port Actor. You can optionally configure these settings for the Port Partner. (Be aware that these settings only affect the administrative state of the partner, and will not take effect until the next time an aggregate link is formed with this device.) After you have completed setting the port LACP parameters, click **submit**.

To assign ports to the member list, click LACP Membership.

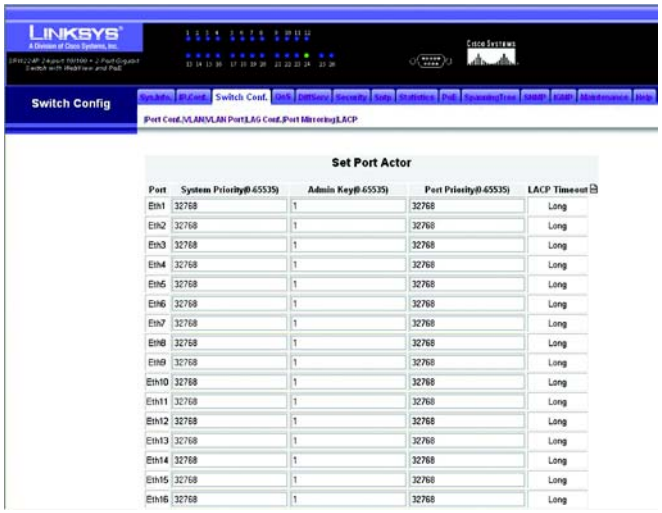

Figure 5-23: Switch Config - LACP

LACP Membership

Select any of the switch ports from the drop-down menu and click **Add**. After you have completed adding ports to the member list, click **submit**.

Figure 5-24: LACP Membership Screen

QoS

The QoS tab includes links to the following screens.

- CoS Settings
- Queue Settings
- CoS to Queue
- IP Precedence/DSCP
- IP Port
- ACL Priority
- Rate Limit

Class of Service 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. This 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.

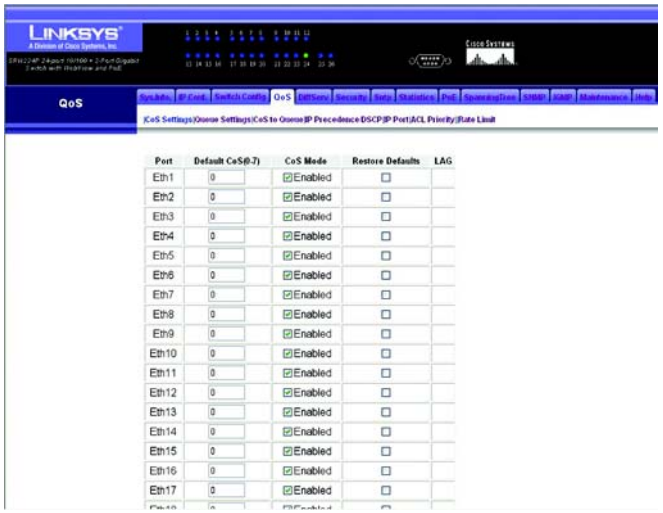

Figure 5-25: QoS - CoS Settings

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.

Table 1:

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

Priority. CoS value. (Range: 0-7, where 7 is the highest priority)

Traffic Type. Output queue buffer. (Range: 0-3, where 3 is the highest CoS priority queue)

Modify the default priority for any interface using the textfield provided. CoS can be enabled or disabled by using the CoS Mode checkbox.

Default settings can be restored using the Restore Defaults checkbox.

Click **submit** to save the changes.

Queue Settings

This switch prioritizes each packet based on the required level of service, using four priority queues with strict or Weighted Round Robin Queuing. It uses IEEE 802.1p and 802.1Q tags to prioritize incoming traffic based on input from the end-station application. These functions can be used to provide independent priorities for delay-sensitive data and best-effort data.

Queue Mode (Global). 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 processed 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. This prevents the head-of-line blocking that can occur with strict priority queuing.

- **WRR**. Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights 1, 2, 4, 6 for queues 0 through 3 respectively.
- **Strict**. Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues.

Set the Queue Mode to Strict or WRR using the Queue Mode drop-down menu then click **submit**.

Enter a weight, select a traffic class (that is, output queue) then click **submit** to save the changes.

Weight Value. Set a new weight for the selected traffic class. However, note that Queue 0 is fixed at a weight of 1, and cannot be configured. (Range: 1-31)

Figure 5-26: QoS - Queue Settings

CoS to Queue

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

Queue. Output queue buffer. (Range: 0-3, where 3 is the highest CoS priority queue)

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

Click **submit** to save the changes.

Figure 5-27: QoS - CoS to Queue

IP Precedence/DSCP

This switch supports several common methods 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 or the number of the TCP port. If priority bits are used, the ToS octet may contain three bits for IP Precedence or 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, this switch maps priority values to the output queues in the following manner:

Figure 5-28: QoS - IP Precedence/DSCP

The precedence for priority mapping is IP Port Priority, IP Precedence or DSCP Priority, and then Default Port Priority.

IP Precedence and DSCP Priority cannot both be enabled. Enabling one of these priority types will automatically disable the other.

The switch allows you to choose between using IP Precedence or DSCP priority. Select one of the methods or disable this feature.

Disabled. Disables both priority services. (This is the default setting.)

IP Precedence. Maps layer 3/4 priorities using IP Precedence.

IP DSCP. Maps layer 3/4 priorities using Differentiated Services Code Point Mapping.

Select Disabled, IP Precedence or IP DSCP from the drop-down menu.

Click **submit** to save the changes.

To select the configuration type, select IP Precedence or IP DSCP from the drop-down menu.

Click **config** to save the changes.

IP Port

You can also map network applications to Class of Service values based on the IP port number (i.e., TCP/UDP port number) in the frame header. Some of the more common TCP service ports include: HTTP: 80, FTP: 21, Telnet: 23 and POP3: 110.

IP Port Priority Status. Enables or disables the IP port priority.

IP Port Priority Table. Shows the IP port to CoS map.

IP Port Number (TCP/UDP). Set a new IP port number, such as HTTP: 80, FTP: 21, Telnet: 23 and POP3: 110.

Class of Service Value. Sets a CoS value for a new IP port. Note that "0" represents low priority and "7" represent high priority.

Set IP Port Priority Status to Enabled by checking the IP Port Priority Global Status checkbox.

Enter the port number for a network application in the IP Port Number box and the new CoS value in the Class of Service box.

Click **Submit** to save the changes.

To remove an IP Port Priority, select the priority to be removed from the table and click **Remove IP Port**.

Figure 5-29: QoS - IP Port

ACL Priority

Use ACL CoS Mapping to set the output queue for packets matching an ACL rule as shown in the following table. Note that the specified CoS value is only used to map the matching packet to an output queue; it is not written to the packet itself.

Table 2:

Queue	0	1	2	3
Priority	1,2	0,3	4,5	6,7

Figure 5-30: QoS - ACL Priority

Port. Port identifier.

Name. Name of ACL.

Type. Type of ACL (IP or MAC).

CoS Priority. CoS value used for packets matching an IP ACL rule. (Range: 0-7)

ACL CoS Priority Mapping. Displays the configured information.

Select an ACL rule, specify a CoS priority, then click **Add**.

To remove an ACL CoS priority mapping click the **Remove** button in the row of the entry you wish to remove.

Rate Limit

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

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

The rate limit screen displays both Fast Ethernet Granularity and Gigabit Granularity.

Rate limit granularity is an additional feature enabling the network manager greater control over traffic on the network. The “rate limit granularity” is multiplied by the “rate limit level” to set the actual rate limit for an interface. Granularity is a global setting that applies to Fast Ethernet or Gigabit Ethernet interfaces.

Use the drop-down menus to change the rate limit for fast ethernet and/or gigabit granularity, click **submit**.

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

To configure input rate limit for each port or lag, click **Port Conf** or **Trunk Conf** in the Input row of the table respectively.

To configure output rate limit for each port or lag, click **Port Conf** or **Trunk Conf** in the Output row of the table respectively.

Figure 5-31: QoS - Rate Limit

Rate Limit Configuration

To configure Port Input Rate Limit, click the Enable checkbox and then set the rate limit level in the textfield provided.

Port Rate Output Limit is configured the same way on the Port Output Rate Limit Configuration screen.

If a port is assigned as a lag member then the rate limit of that port cannot be set in the port configuration screen.

Truck Rate Limit is configured the same way as port rate limit using the trunk Input and output screens.

NOTE: When the rate limit granularity is set to a low value (for 10/100 ports, less than 512 Kbps), the maximum bandwidth available on ports is restricted to a value that is "256 x granularity." This restriction also applies to ports with rate limiting disabled.

DiffServ

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

All switches or routers that access the Internet rely on class information to provide the same forwarding treatment to packets in the same class. Class information can be assigned by end hosts, or switches or routers along the path. Priority can then be assigned based on a general policy, or a detailed examination of the packet. However, note that detailed examination of packets should take place close to the network edge so that core switches and routers are not overloaded.

Switches and routers along the path can use class information to prioritize the resources allocated to different traffic classes. The manner in which an individual device handles traffic in the DiffServ architecture is called per-hop behavior. All devices along a path should be configured in a consistent manner to construct a consistent end-to-end QoS solution.

The DiffServ tab includes links to the following screens.

- DiffServ Class Map
- DiffServ Policy Map
- DiffServ Service Policy

DiffServ Class Map

A class map is used for matching packets to a specified class.

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)

Modify Name and Description. Configures the name and a brief description of a class map. (Range: 1-32 characters for the name; 1-256 characters for the description) Select the entry you wish to change, enter your changes and click the **Modify Name & Description** button.

Edit Rules. Opens "Match Class Settings" for the selected class entry. Modify the criteria used to classify ingress traffic.

Add Class. Opens "Class Configuration". Enter a class name and description and click **Add** to open "Match Class Settings". Enter the criteria used to classify ingress traffic.

Remove Class. Removes the selected class.

Click **Add Class** to create a new class, or select a class and click **Edit Rules** to change the rules of the selected class, or **Remove Class** to delete the class.

Figure 5-32: DiffServ - Diffserv Class Map

Setting Rules

Class Name. List of class maps.

ACL List. Name of an access control list. Any type of ACL can be specified, including standard or extended IP ACLs and MAC ACLs. (Range: 1-16 characters)

IP DSCP. A DSCP value. (Range: 0-63)

IP Precedence. An IP Precedence value. (Range: 0-7)

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

Remove. Deletes the selected criteria from the class.

Figure 5-33: DiffServ Class Map - Setting Rules

Add rules to a selected class using the ACL list drop-down menu and the IP DSCP, IP Precedence and VLAN text fields provided then click **Add**.

Adding a Class

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. Adds the specified class.

Back. Returns to previous screen without making any changes.

Enter the class name and description into the textfields provided in the Add Class screen, then click **Add**.

Figure 5-34: DiffServ Class Map - Adding a Class

DiffServ Policy Map

This function creates a policy map that can be attached to multiple interfaces.

Modify Name and Description. Configures the name and a brief description of a policy map. (Range: 1-32 characters for the name; 1-256 characters for the description)

Edit Classes. Opens "Policy Rule Settings" for the selected class entry. Modify the criteria used to service ingress traffic.

Add Policy. Opens "Policy Configuration". Enter a policy name and description and click **Add** to open "Policy Rule Settings". Enter the criteria used to service ingress traffic.

Remove Policy. Deletes a specified policy.

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

Figure 5-35: DiffServ - Diffserv Policy Map

Adding a Policy

Policy Name. Name of policy map. (Range: 1-32 characters)

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

Add. Adds the specified policy.

Back. Returns to previous screen without making any changes.

Enter the policy name and description into the textfields provided in the Add Policy screen, then click **Add**

Figure 5-36: DiffServ Policy Map - Adding a Policy

Setting Rules

Class Name. Name of class map.

Action. Shows the service provided to ingress traffic by setting a CoS, DSCP, or IP Precedence value in a matching packet.

Meter. The maximum throughput and burst rate.

- Rate (kbps) – Rate in kilobits per second.
- Burst (byte) – Burst in bytes.

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

Remove Class. Deletes a class.

Class Name. Name of class map.

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)

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 (byte) – Burst in bytes. (Range: 64-1522)

Exceed. 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 out of conformance traffic.

Add. Adds the specified criteria to the policy map.

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

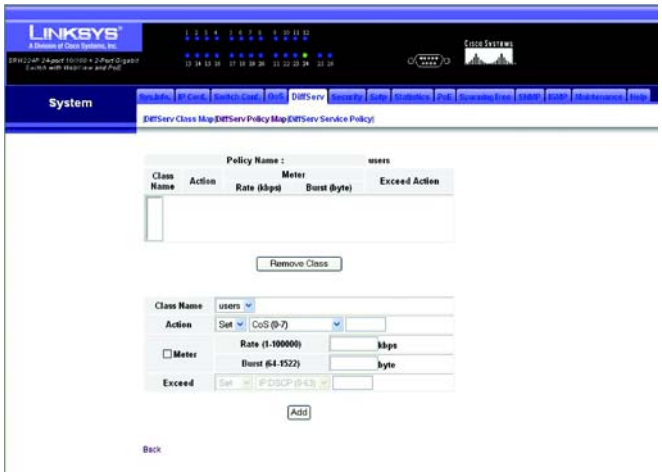

Figure 5-37: DiffServ Policy Map - Setting Rules

DiffServ Service Policy

This function binds a policy map to the ingress queue of a particular interface.

Check **Enabled** and choose a Policy Map for a port from the drop-down menu.

Click **Submit** to save the changes.

Figure 5-38: DiffServ - Diffserv Service Policy

Security

The Security tab includes links to the following screens.

- ACL Conf.
- ACL Port Binding
- 802.1xUsers
- 802.1xPort Conf.
- Radius Server
- Port Security
- Storm Control
- HTTPS Settings
- System Password

ACL Conf.

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

Enter an ACL name in the Name field (with up to 16 characters), select the list type (IP Standard, IP Extended, or MAC), and click **Add** to open the configuration screen for the new list.

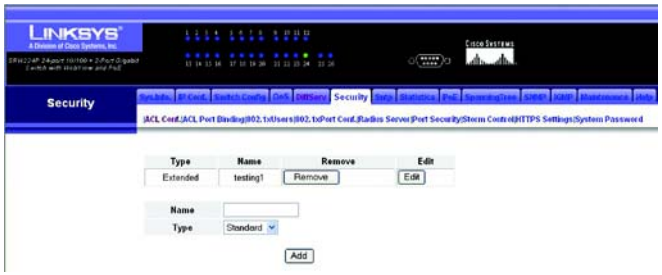

Figure 5-39: Security - ACL Conf

Standard ACL

To configure a standard ACL do the following.

Specify the action (that is, Permit or Deny). Select the address type (Any, Host, or IP). If you select "Host," enter a specific address. If you select "IP," enter a subnet address and the mask for an address range. Then click **Add**.

Figure 5-40: ACL Conf - Adding/Editing Standard ACL

Extended ACL

To configure an extended ACL do the following.

Specify the action (that is, Permit or Deny). Specify the source and/or destination addresses. Select the address type (Any, Host, or IP). If you select "Host," enter a specific address. If you select "IP," enter a subnet address and the mask for an address range. Set any other required criteria, such as service type, protocol type, or TCP control code. Then click **Add**.

Figure 5-41: ACL Conf - Adding/Editing Extended ACL

Action. An ACL can contain any combination of permit or deny rules.

Source Address/Destination Type. Specifies the source or destination IP address. Use "Any" to include all possible addresses, "Host" to specify a specific host address in the Address field, or "IP" to specify a range of addresses with the Address and SubMask fields. (Options: Any, Host, IP; Default: Any)

Source/Destination IP Address. Source or destination IP address.

Source/Destination Subnet Mask. Subnet mask for source or destination address.

Service Type. Packet priority settings based on the following criteria:

- Precedence – IP precedence level. (Range: 0-7)
- TOS – Type of Service level. (Range: 0-15)
- DSCP – DSCP priority level. (Range: 0-63)

Protocol. Specifies the protocol type to match as TCP, UDP or Others, where others indicates a specific protocol number (0-255). (Options: TCP, UDP, Others; Default: TCP)

Source/Destination Port (0-65535). Source/destination port number for the specified protocol type. (Range: 0-65535)

Control Code (0-63). Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)

Control Code Bitmask (0-63). Decimal number representing the code bits to match. The control bitmask is a decimal number (for an equivalent binary bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit "1" means to match a bit and "0" means to ignore a bit. The following bits may be specified:

- 1 (fin) – Finish
- 2 (syn) – Synchronize
- 4 (rst) – Reset
- 8 (psh) – Push
- 16 (ack) – Acknowledgement
- 32 (urg) – Urgent pointer

For example, use the code value and mask below to catch packets with the following flags set:

- - SYN flag valid, use control-code 2, control bitmask 2
- - Both SYN and ACK valid, use control-code 18, control bitmask 18
- - SYN valid and ACK invalid, use control-code 2, control bitmask 18

MAC ACL

To configure a MAC ACL do the following.

Specify the action (that is, Permit or Deny). Specify the source and/or destination addresses. Select the address type (Any, Host, or MAC). If you select “Host,” enter a specific address (for example, 11-22-33-44-55-66). If you select “MAC,” enter a base address and a hexadecimal bitmask for an address range. Set any other required criteria, such as VID, Ethernet type, or packet format. Then click **Add**.

Action. An ACL can contain any combination of permit or deny rules.

Source/Destination Address Type. Use “Any” to include all possible addresses, “Host” to indicate a specific MAC address, or “MAC” to specify an address range with the Address and Bitmask fields. (Options: Any, Host, MAC; Default: Any)

Source/Destination MAC Address. Source or destination MAC address.

Source/Destination Bitmask. Hexidecimal mask for source or destination MAC address.

VID. VLAN ID. (Range: 1-4094)

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).

Figure 5-42: ACL Conf - Adding/Editing MAC ACL

NOTE: MAC addresses specified in MAC ACLs will conflict with any user-defined static MAC addresses.

NOTE: When configuring a MAC ACL that includes the rule "deny any any" for a specific VLAN, the following restrictions apply: Received unicast packets with unknown addresses are not flooded to all ports in the VLAN. All dynamically learned MAC addresses in the specified VLAN are flushed from the switch's MAC address table. Other rules in the MAC ACL allow only specific Host source or destination MAC addresses to be specified.

ACL Port Binding

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

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 ACL to any port, and one MAC ACL globally, 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.

Port – Fixed port or SFP module. (Range: 1-26)

IP. Specifies the IP Access List to enable for a port.

MAC. Specifies the MAC Access List to enable globally.

IN. ACL for ingress packets.

ACL Name. Name of the ACL.

Click **Submit** to save the changes.

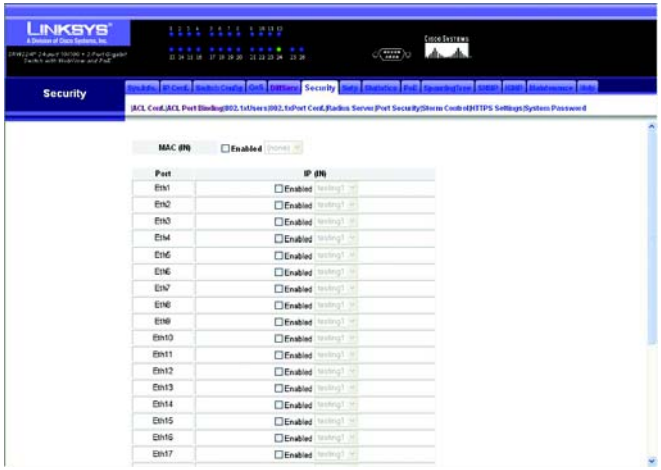

Figure 5-43: Security - ACL Port Binding

802.1xUsers

Network switches can provide open and easy access to network resources by simply attaching a client PC. Although this automatic configuration and access is a desirable feature, it also allows unauthorized personnel to easily intrude and possibly gain access to sensitive network data.

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.

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.

Figure 5-44: Security - 802.1x Users

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

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

To enable 802.1X System Authentication Control, mark the Enable checkbox.

Click **submit** to save the changes.

802.1xPort Conf.

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.

Modify the parameters required using the drop-down menus and textfields provided, and click **Submit**.

Max-Req. 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)

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

TX 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)

Supplicant. This Indicates the MAC address of a connected client.

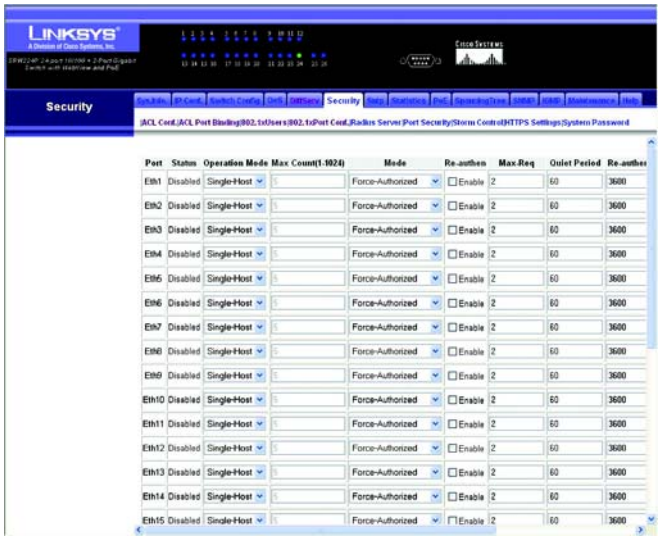

Figure 5-45: Security - 802.1x Port Conf

Radius Server

Remote Authentication Dial-in User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) are logon 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.

RADIUS and TACACS+ logon authentication assign a specific privilege level for each user name/password pair. The user name, password, and privilege level must be configured on the authentication server.

To configure local or remote authentication preferences, specify the authentication sequence (that is, one to three methods), fill in the parameters for RADIUS or TACACS+ authentication if selected.

Secret Text String. Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)

Click **Submit** to save the changes.

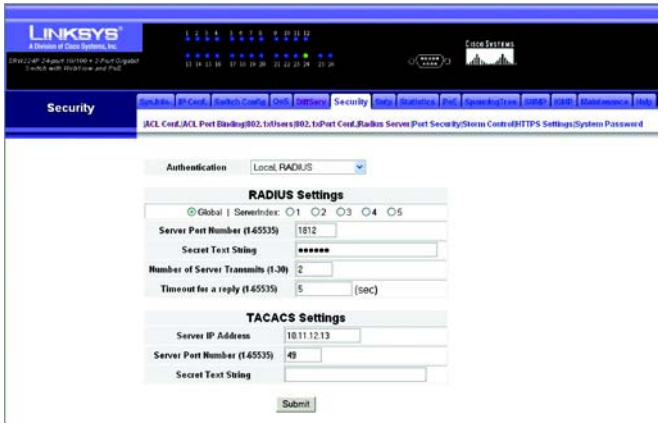

Figure 5-46: Security - RADIUS Server

Port Security

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

To use port security, specify a maximum number of addresses to allow on the port and then let the switch dynamically learn the <source MAC address, VLAN> pair for frames received on the port. When the port has reached the maximum number of MAC addresses the selected port will stop learning. The MAC addresses already in the address table will be retained and will not 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, mark the checkbox in the Status column to enable security for a port, set the maximum number of MAC addresses allowed on a port.

Click **Submit** to save the changes.

Figure 5-47: Security - Port Security

Storm Control

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

Set the threshold using the Threshold text field, to enable storm control on a specified port mark the Enable checkbox for that port. storm control on a specified port.

Click **Submit** to save the changes.

Figure 5-48: Security - Storm Control

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.

Mark the HTTPS Status checkbox to enable HTTPS and specify the port number.

Click **Submit** to save the changes.

Figure 5-49: Security - HTTPS Settings

System Password

The switch supports up to 16 user names and passwords for management access (console and web interfaces). Each user account has an associated access level; either Normal or Privileged. A Normal level user has only read access for most configuration parameters. However, a Privileged user has write access for all parameters governing the switch. The default Normal user name is "guest" with the password "guest." The default Privileged user name is "admin" with no password. You should therefore assign a new password for the "admin" user account or create new Privileged user accounts, and store them in a safe place. Both the default "admin" and "guest" user accounts can be deleted from the system.

To configure a new user account, enter the user name, access level, and password - up to eight characters long - and click **Add**. To change the password for a specific user, enter the user name and new password, confirm the password by entering it again. Up to 16 user accounts can be configured on this switch.

Click **Change** to save the changes.

Figure 5-50: Security - System Password

SNTP

The SNTP tab includes links to the Global Settings screen.

Figure 5-51: SNTP - Global Settings

Global Settings

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.

To receive updates the switch sends unicast packets to the SNTP server.

Set the Polling Interval using the text field provided. Set the IP address of up to three SNTP servers using the text fields provided.

Click **Submit** to save the changes.

Statistics

You can display standard statistics on network traffic from the Interfaces Group and Ethernet-like MIBs, as well as a detailed breakdown of traffic based on the RMON MIB. Interfaces and Ethernet-like statistics display errors on the traffic passing through each port.

The Statistics tab includes links to the following screens.

- Interface Statistics
- Etherlike Statistics
- RMON Statistics

Interface Statistics

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

Figure 5-52: Statistics - Interface Statistics

Etherlike Statistics

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

Figure 5-53: Statistics - Etherlike Statistics

RMON Statistics

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

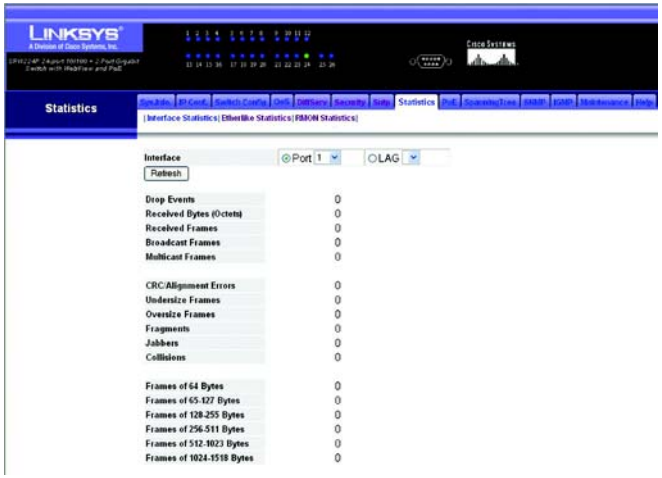

Figure 5-54: Statistics - RMON Statistics

PoE

This switch can provide DC power to a wide range of connected devices, eliminating the need for an additional power source and cutting down on the amount of cables attached to each device. 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.

The PoE tab includes links to the following screens.

- Power Config
- Power Port Config
- Power Port Status
- Power Status

Power Config

A maximum PoE power budget for the switch (power available to all switch ports) can be defined so that power can be centrally managed, preventing overload conditions at the power source. If the power demand from devices connected to the switch exceeds the power budget setting, the switch uses port power priority settings to limit the supplied power.

Specify the desired power budget for the switch.

Click **Submit** to save the changes.

Figure 5-55: PoE - Power Config

Power Port Config

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.

Mark the Enabled checkbox to enable PoE power on selected ports, set the priority using the drop-down menu provided and set the power allocation for each port.

Click **Submit** to save the changes.

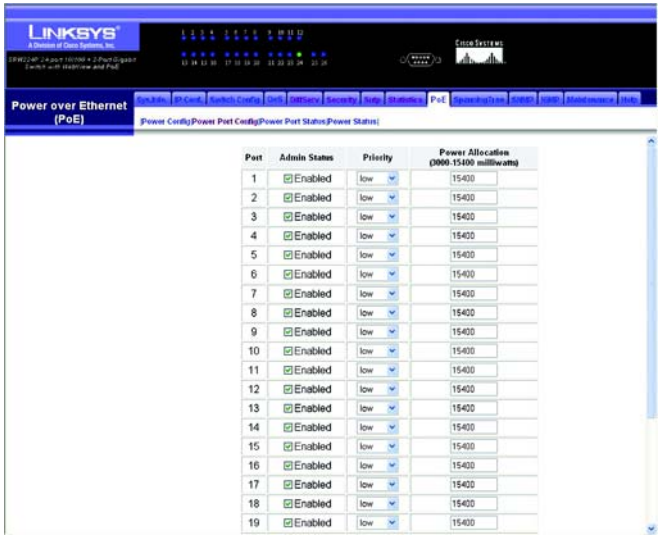

Figure 5-56: PoE - Power Port Config

Power Port Status

Use Power Port Status to display the current PoE power status for all ports.

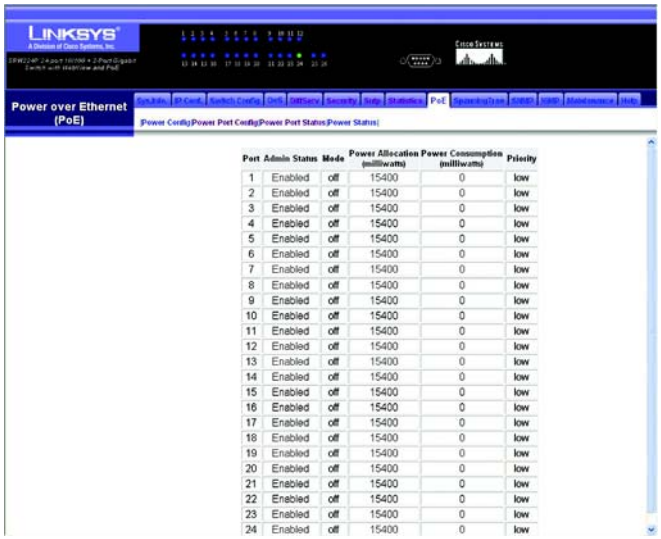

Figure 5-57: PoE - Power Port Status

Power Status

This screen displays the following information.

Maximum Available Power

System Operation Status

Mainpower Consumption

Software Version

Figure 5-58: PoE - Power Status

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 tab includes links to the following screens.

- Information
- Configuration
- Port Info
- LAG Info
- Port Conf
- LAG Conf

Information

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

This screen displays the following information.

Spanning Tree State. Shows if the switch is enabled to participate in an STA-compliant network.

Designated Root. The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.

Bridge ID. A unique identifier for this bridge, consisting of the bridge priority and MAC address (where the address is taken from the switch system).

Root Port. The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.

Max 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 STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to "ports" in this section mean "interfaces," which includes both ports and lags.)

Root Path Cost. The path cost from the root port on this switch to the root device.

Hello Time. Interval (in seconds) at which this device transmits a configuration message.

Configuration Changes. The number of times the Spanning Tree has been reconfigured.

Forward Delay. The maximum time (in seconds) the root 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.

Last Topology Change. Time since the Spanning Tree was last reconfigured.

Figure 5-59: Spanning Tree - Information

Configuration

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

Modify the required attributes for STA.

Click **Submit** to save the changes.

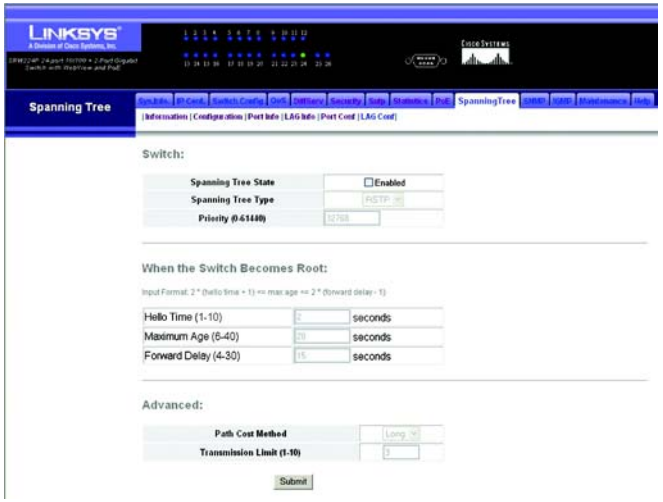

Figure 5-60: Spanning Tree - Configuration

Port/LAG Info

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

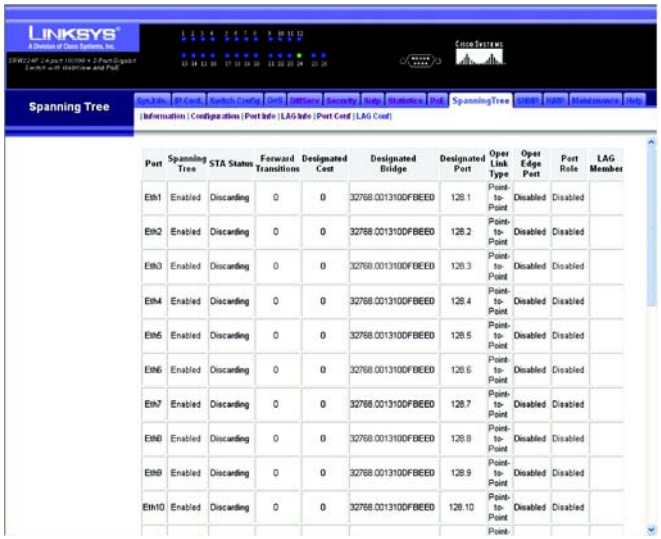

Figure 5-61: Spanning Tree - Port/LAG Info

Port/LAG Conf

You can configure RSTP attributes for specific interfaces, including port priority, path cost, link type, and edge port. You may use a different priority or path cost for ports of the same media type to indicate the preferred path, link type to indicate a point-to-point connection or shared-media connection, and edge port to indicate if the attached device can support fast forwarding. (References to “ports” in this section means “interfaces,” which includes both ports and lags.)

Modify the required attributes.

Click **Submit** to save the changes.

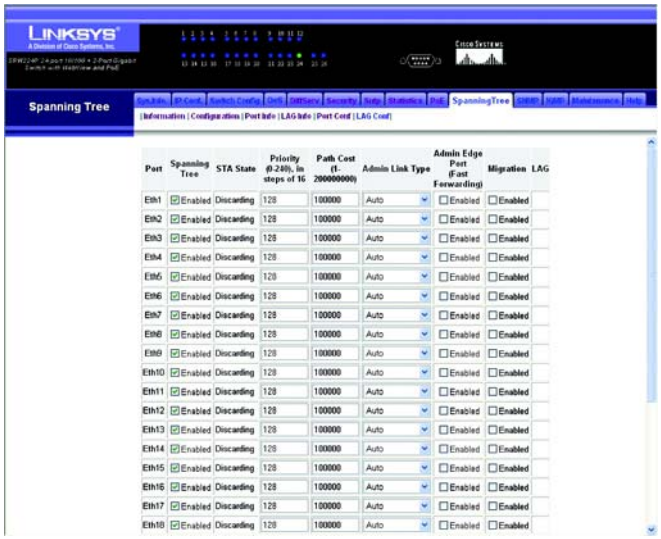

Figure 5-62: Spanning Tree - Information

SNMP

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.

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 this 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.

The SNMP tab displays the SNMP Config screen.

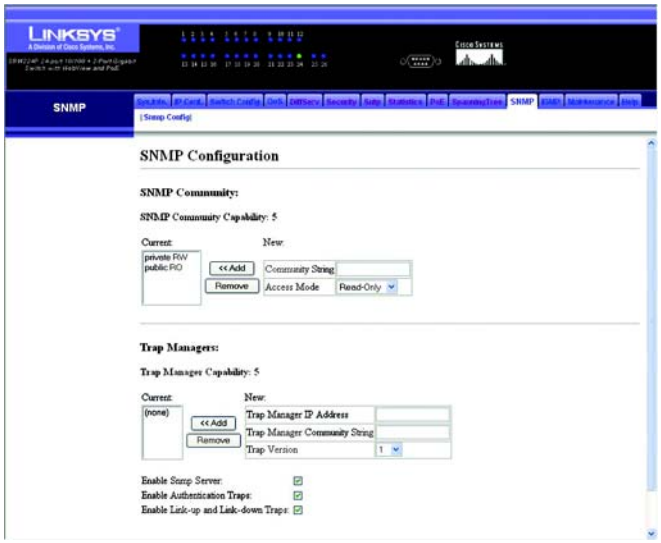

Figure 5-63: SNMP - SNMP Config

SNMP Config

Add up to five new community strings, select the access rights from the Access Mode drop-down menu,. These strings act as passwords. They are case-sensitive and can be up to 32 characters long. Some default strings are "public", specifying read-only access, and "private", allowing read/write access. Once this is entered, click **Add**.

Enter the IP address and community string for each management station that will receive trap messages. Strings are case-sensitive and can be up to 32 characters long. Specify the trap version and click **Add**. Enable SNMP and select the trap types required using the check boxes for Authentication and Link-up/down traps.

Click **Submit** to save the changes.

IGMP

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

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

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

Note that IGMP neither alters nor routes IP multicast packets. A multicast routing protocol must be used to deliver IP multicast packets across different subnetworks.

The IGMP tab includes links to the following screens.

- IGMP Conf
- IGMP Router Info
- IGMP Router Conf
- IP Multicast Reg Table
- IGMP Member Conf

IGMP Conf

Adjust the IGMP settings as required.

IGMP 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).

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

IGMP Query Count. Sets the maximum number of queries 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)

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

IGMP Report Delay. 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)

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

Click **Submit** to save the changes.

Figure 5-64: IGMP - IGMP Conf

IGMP Router Info

Multicast routers that are attached to ports on the switch use information obtained from IGMP, along with a multicast routing protocol such as DVMRP or PIM, 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.

Select a VLAN ID from the drop-down menu to display the ports on this switch attached to a neighboring multicast router/switch for each VLAN ID.

Figure 5-65: IGMP - IGMP Router Info

IGMP Router Conf

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

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

Figure 5-66: IGMP - IGMP Router Conf

IP Multicast Reg Table

You can display the port members associated with a specified 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.

Figure 5-67: IGMP - IP Multicast Reg Table

IGMP Member Conf

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

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

Figure 5-68: IGMP - IGMP Member Conf

Maintenance

The Maintenance tab includes links to the following screens.

- Reset
- File Download
- File Upload
- Restore Defaults
- Save Config
- Integrated Cable Test

Reset

To restart the switch, click the **Reset the Device** link, then click **Yes** to restart the switch. To cancel the restart, click **No** or **Cancel**, then click **OK**.

Figure 5-69: Maintenance - Reset

File Download

Downloads switch firmware or configuration files from a TFTP server. You must specify the file type to transfer, along with TFTP server IP address and file names as required.

Select Firmware of Configuration download using the radio buttons. Enter the IP address of the TFTP server, enter the file name of the software to download and select the destination file name using the drop-down menu, then click **Apply**.

Figure 5-70: Maintenance - File Download

File Upload

Uploads switch firmware or configuration files to a TFTP server. You must specify the file type to transfer, along with TFTP server IP address and file names as required. Saving firmware and configuration files on a TFTP server enables them to be later downloaded to the switch to restore operation.

To Upload a file from the switch select Firmware of Configuration upload using the radio buttons. Enter the IP address of the TFTP server, enter the destination file name and click **Apply**.

Figure 5-71: Maintenance - File Upload

Restore Defaults

To restore default settings, click the **Restore Company Defaults** link. Then click **OK** to proceed or **Cancel** to cancel.

Figure 5-72: Maintenance - Restore Defaults

Save Config

To save the current configuration settings, click the **Save Current Config** link. Then click **OK** to proceed or **Cancel** to cancel.

Figure 5-73: Maintenance - Save Config

Integrated Cable Test

To test the connection quality of cables, click on the test icon for the port.

The following screen will display the last test results. Click the **Submit** button to start the test.

Test results are shown on the Integrated Cable Test Screen.

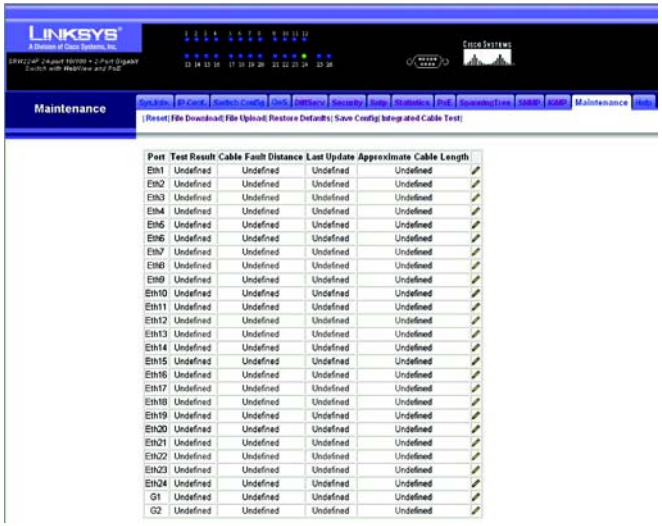

Figure 5-74: Maintenance - Integrated Cable Test

Help

The Help tab includes links to the screens shown in the web-utility and how to navigate them.

Figure 5-75: Help

Appendix A: Fast Ethernet and Gigabit Ethernet

About Fast Ethernet

1. As the demand for desktop video, multimedia development, imaging, and other speed-intensive applications continues to rise, the need for high performance, fault tolerant LAN technology will become more critical.

2. Standard Ethernet, which has been the most popular networking technology to date with a maximum data throughput of 10Mbps (Megabits per second), is becoming insufficient to handle the latest video, multimedia, and other speed-intensive client/server LAN applications.

3. Among the solutions to the problem of network speed, Fast Ethernet has emerged as the most viable and economical. Capable of sending and receiving data at 100Mbps, it is more than fast enough to handle even the most demanding video and other real-time applications.

4. Although there are a number of different competing Fast Ethernet implementations, 100BaseTX is by far the most popular. Operating on two pairs of Category 5 unshielded twisted-pair (UTP) cabling, 100BaseTX supports high speed signaling and is relatively inexpensive. Because it uses four wires for data transmission and the same packet format, packet length, error control, and management information as 10BaseT, 100BaseTX can be made to communicate with slower 10BaseT equipment when routed through a switch.

5. This backwards compatibility is one of 100BaseTX's major advantages over other forms of Fast Ethernet; it allows critical, speed-dependent network segments to be upgraded to 100BaseTX speeds as needed without re-wiring, refitting, and retraining an entire site. Networks can now mix both slow and fast network segments for different users or departments. Publishing, R&D, video, multimedia, or accounting departments can enjoy a 100Mbps pace, while other corporate segments can operate at slower and more affordable 10Mbps speeds.

About 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 5 cabling, with fiber optics more suited for network backbones. As the new Gigabit standard gradually integrates into existing networks, current computer applications will enjoy faster access time for network data, hardware, and Internet connections.

Appendix B: Cabling

Overview

Twisted Pair Cabling and Fiber Optic Cabling are discussed in this appendix.

Twisted Pair Cabling

There are different grades, or categories, of twisted-pair cabling. Category 5 is the most reliable and is highly recommended. Straight-through cables are used for connecting computers to a hub. Crossover cables are used for connecting a hub to another hub (there is an exception: some hubs have a built-in uplink port that is crossed internally, which allows you to link or connect hubs together with a straight-through cable instead).

You can buy pre-made Category 5 cabling, or cut and crimp your own. Category 5 cables can be purchased or crimped as either straight-through or crossover cables. A Category 5 cable has 8 thin, color-coded wires inside that run from one end of the cable to the other. All 8 wires are used. In a straight-through cable, wires 1, 2, 3, and 6 at one end of the cable are also wires 1, 2, 3, and 6 at the other end. In a crossover cable, the order of the wires change from one end to the other: wire 1 becomes 3, and 2 becomes 6. See the diagrams on this page for more detailed information on straight-through and crossover cabling.

To determine which wire is wire number 1, hold the cable so that the end of the plastic RJ-45 tip (the part that goes into a wall jack first) is facing away from you. Face the clip down so that the copper side faces up (the springy clip will now be parallel to the floor). When looking down on the copper side, wire 1 will be on the far left.

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 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 U. S., 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 miniGBIC modules with the Linksys SRW224P. The MGBSX1 and the MGBLH1 require fiber cabling with LC connectors. The MGBT1 requires a Category 5 Ethernet Cable with an RJ-45 connector.

Appendix C: 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.

Bandwidth - The transmission capacity of a given device or network.

Bit - A binary digit.

Boot - To start a device and cause it to start executing instructions.

Broadband - An always-on, fast Internet connection.

Browser - An application program that provides a way to look at and interact with all the information on the World Wide Web.

Byte - A unit of data that is usually eight bits long

DDNS (**D**ynamic **D**omain **N**ame **S**ystem) - Allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (e.g., www.xyz.com) and a dynamic IP address.

Default Gateway - A device that forwards Internet traffic from your local area network.

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) - A networking protocol that allows administrators to assign temporary IP addresses to network computers by "leasing" an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

DNS (**D**omain **N**ame **S**erver) - The IP address of your ISP's server, which translates the names of websites into IP addresses.

Domain - A specific name for a network of computers.

Download - To receive a file transmitted over a network.

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

Ethernet - IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium.

Firewall - A set of related programs located at a network gateway server that protects the resources of a network from users from other networks.

Firmware - The programming code that runs a networking device.

FTP (**F**ile **T**ransfer **P**rotocol) - A protocol used to transfer files over a TCP/IP network.

Full Duplex - The ability of a networking device to receive and transmit data simultaneously.

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

Half Duplex - Data transmission that can occur in two directions over a single line, but only one direction at a time.

HTTP (**H**yper**T**ext **T**ransport **P**rotocol) - The communications protocol used to connect to servers on the World Wide Web.

IP (**I**nternet **P**rotocol) - A protocol used to send data over a network.

IP Address - The address used to identify a computer or device on a network.

MAC (**M**edia **A**ccess **C**ontrol) **Address** - The unique address that a manufacturer assigns to each networking device.

Mbps (**M**ega**B**its **P**er **S**econd) - One million bits per second; a unit of measurement for data transmission.

Network - A series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users.

Packet - A unit of data sent over a network.

Port - The connection point on a computer or networking device used for plugging in cables or adapters.

Power **o**ver **E**thernet (**PoE**) - A technology enabling an Ethernet network cable to deliver both data and power.

PPPoE (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) - A type of broadband connection that provides authentication (username and password) in addition to data transport.

RADIUS (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice) - A protocol that uses an authentication server to control network access.

RJ-45 (**R**egistered **J**ack-**45**) - An Ethernet connector that holds up to eight wires.

Server - Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

SMTP (**S**imple **M**ail **T**ransfer **P**rotocol) - The standard e-mail protocol on the Internet.

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) - A widely used network monitoring and control protocol.

Static IP Address - A fixed address assigned to a computer or device that is connected to a network.

Static Routing - Forwarding data in a network via a fixed path.

Subnet Mask - An address code that determines the size of the network.

Switch - 1. A data switch that connects computing devices to host computers, allowing a large number of devices to share a limited number of ports. 2. A device for making, breaking, or changing the connections in an electrical circuit.

TCP (**T**ransmission **C**ontrol **P**rotocol) - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) - A set of instructions PCs use to communicate over a network.

Telnet - A user command and TCP/IP protocol used for accessing remote PCs.

TFTP (**T**rivial **F**ile **T**ransfer **P**rotocol) - A version of the TCP/IP FTP protocol that has no directory or password capability.

Throughput - The amount of data moved successfully from one node to another in a given time period.

TX Rate - Transmission Rate.

Upgrade - To replace existing software or firmware with a newer version.

Upload - To transmit a file over a network.

URL (**U**niform **R**esource **L**ocator) - The address of a file located on the Internet.

Appendix D: Specifications

Standards	IEEE Std. 802.3-2002
Ports	24 - 10/100 , 2 - 10/100/1000, 2 - MiniGBIC, 1- Console
Cabling	Type UTP CAT 5e or better
LEDs	System, Link/Act, PoE, Speed, Gigabit 1, Gigabit 2
Dimensions (L x W x H)	16.93" x 1.75" x 13.78" (43cm x 4.45cm x 35cm)
Unit Weight	9.04 lbs (4.1 kg)
Power	Voltage Range 100 ~ 240VAC, Frequency range 47– 63Hz, 225W max
Certifications	FCC Class A, CE, UL
Operating Temp.	0ºC to 50ºC (32ºF to 121ºF)
Storage Temp.	-40ºC to 70ºC (-40ºF to 158ºF)
Operating Humidity	10% to 90% Non-Condensing
Storage Humidity	10% to 95% Non-Condensing

Appendix E: Warranty Information

LIMITED WARRANTY

Linksys warrants to You that, for a period of five years (the "Warranty Period"), your Linksys Product will be substantially free of defects in materials and workmanship under normal use. Your exclusive remedy and Linksys' entire liability under this warranty will be for Linksys at its option to repair or replace the Product or refund Your purchase price less any rebates. This limited warranty extends only to the original purchaser.

If the Product proves defective during the Warranty Period call Linksys Technical Support in order to obtain a Return Authorization Number, if applicable. BE SURE TO HAVE YOUR PROOF OF PURCHASE ON HAND WHEN CALLING. If You are requested to return the Product, mark the Return Authorization Number clearly on the outside of the package and include a copy of your original proof of purchase. RETURN REQUESTS CANNOT BE PROCESSED WITHOUT PROOF OF PURCHASE. You are responsible for shipping defective Products to Linksys. Linksys pays for UPS Ground shipping from Linksys back to You only. Customers located outside of the United States of America and Canada are responsible for all shipping and handling charges.

ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY 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 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 warranty gives You specific legal rights, and You may also have other rights which vary by jurisdiction.

This warranty does not apply if the Product (a) has been altered, except by Linksys, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Linksys, or (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Linksys does not warrant that the Product will be free of vulnerability to intrusion or attack.

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 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.

Please direct all inquiries to: Linksys, P.O. Box 18558, Irvine, CA 92623.

Appendix F: Regulatory Information

FCC STATEMENT

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

You may use unshielded twisted-pair (UTP) for RJ-45 connections - Category 3 or better for 10 Mbps connections, Category 5 or better for 100 Mbps connections, Category 5, 5e, or 6 for 1000 Mbps connections. For fiber optic connections, you may use 50/125 or 62.5/125 micron multimode fiber or 9/125 micron single-mode fiber.

INDUSTRY CANADA (CANADA)

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled “Digital Apparatus,” ICES-003 of the Department of Communications.

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans la norme sur le matériel brouilleur: “Appareils Numériques,” NMB-003 édictée par le ministère des Communications.

Safety Compliance

Warning: Fiber Optic Port Safety

When using a fiber optic port, never look at the transmit laser while it is powered on. Also, never look directly at the fiber TX port and fiber cable ends when they are powered on.

Avertissment: Ports pour fibres optiques - sécurité sur le plan optique

Ne regardez jamais le laser tant qu'il est sous tension. Ne regardez jamais directement le port TX (Transmission) à fibres optiques et les embouts de câbles à fibres optiques tant qu'ils sont sous tension.

Warnhinweis: Faseroptikanschlüsse - Optische Sicherheit

Niemals ein Übertragungslaser betrachten, während dieses eingeschaltet ist. Niemals direkt auf den Faser-TX-Anschluß und auf die Faserkabelenden schauen, während diese eingeschaltet sind.

Please read the following safety information carefully before installing the switch:

WARNING: Installation and removal of the unit must be carried out by qualified personnel only.

"The unit must be connected to an earthed (grounded) outlet to comply with international safety standards.

"Do not connect the unit to an A.C. outlet (power supply) without an earth (ground) connection.

"The appliance coupler (the connector to the unit and not the wall plug) must have a configuration for mating with an EN 60320/IEC 320 appliance inlet.

"The socket outlet must be near to the unit and easily accessible. You can only remove power from the unit by disconnecting the power cord from the outlet.

"This unit operates under SELV (Safety Extra Low Voltage) conditions according to IEC 60950. The conditions are only maintained if the equipment to which it is connected also operates under SELV conditions.

France and Peru only

This unit cannot be powered from IT† supplies. If your supplies are of IT type, this unit must be powered by 230 V (2P+T) via an isolation transformer ratio 1:1, with the secondary connection point labeled Neutral, connected directly to earth (ground).

† Impédance à la terre

Power Cord Set	
U.S.A. and Canada	The cord set must be UL-approved and CSA certified.
	The minimum specifications for the flexible cord are: - No. 18 AWG, not longer than 2 meters, or 16 AWG. - Type SV or SJ - 3-conductor.
	The cord set must have a rated current capacity of at least 10 A
	The attachment plug must be an earth-grounding type with NEMA 5-15P (15 A, 125 V) or NEMA 6-15P (15 A, 250 V) configuration.
Denmark	The supply plug must comply with Section 107-2-D1, Standard DK2-1a or DK2-5a.
Switzerland	The supply plug must comply with SEV/ASE 1011.
U.K.	The supply plug must comply with BS1363 (3-pin 13 A) and be fitted with a 5 A fuse which complies with BS1362.
	The mains cord must be <HAR> or <BASEC> marked and be of type HO3VVF3GO.75 (minimum).
Europe	The supply plug must comply with CEE7/7 ("SCHUKO").
	The mains cord must be <HAR> or <BASEC> marked and be of type HO3VVF3GO.75 (minimum).
	IEC-320 receptacle.

Veuillez lire à fond l'information de la sécurité suivante avant d'installer le Switch:

AVERTISSEMENT: L'installation et la dépose de ce groupe doivent être confiés à un

personnel qualifié.

Ne branchez pas votre appareil sur une prise secteur (alimentation électrique) lorsqu'il n'y a pas de connexion de mise à la terre (mise à la masse).

Vous devez raccorder ce groupe à une sortie mise à la terre (mise à la masse) afin de respecter les normes internationales de sécurité.

Le coupleur d'appareil (le connecteur du groupe et non pas la prise murale) doit respecter une configuration qui permet un branchement sur une entrée d'appareil EN 60320/IEC 320.

La prise secteur doit se trouver à proximité de l'appareil et son accès doit être facile. Vous ne pouvez mettre l'appareil hors circuit qu'en débranchant son cordon électrique au niveau de cette prise.

L'appareil fonctionne à une tension extrêmement basse de sécurité qui est conforme à la norme IEC 60950. Ces conditions ne sont maintenues que si l'équipement auquel il est raccordé fonctionne dans les mêmes conditions.

France et Pérou uniquement:

Ce groupe ne peut pas être alimenté par un dispositif à impédance à la terre. Si vos alimentations sont du type impédance à la terre, ce groupe doit être alimenté par une tension de 230 V (2 P+T) par le biais d'un transformateur d'isolement à rapport 1:1, avec un point secondaire de connexion portant l'appellation Neutre et avec raccordement direct à la terre (masse).

	Cordon électrique - Il doit être agréé dans le pays d'utilisation
Etats-Unis et Canada:	Le cordon doit avoir reÁu líhomologation des UL et un certificat de la CSA.
	Les spe'cifications minimales pour un cable flexible sont AWG No. 18, ouAWG No. 16 pour un cable de longueur infe'rieure a` 2 me'tres. - type SV ou SJ - 3 conducteurs
	Le cordon doit Ítre en mesure díacheminer un courant nominal díau moins 10 A.
	La prise femelle de branchement doit être du type à mise à la terre (mise à la masse) et respecter la configuration NEMA 5-15P (15 A, 125 V) ou NEMA 6-15P (15 A, 250 V).
Danemark:	La prise m,le díalimentation doit respecter la section 107-2 D1 de la norme DK2 1a ou DK2 5a.
Suisse:	La prise m,le díalimentation doit respecter la norme SEV/ASE 1011.
Europe	La prise secteur doit être conforme aux normes CEE 7/7 ("SCHUKO"). LE cordon secteur doit porter la mention <HAR> ou <BASEC> et doit Ítre de type HO3VVF3GO.75 (minimum).

Bitte unbedingt vor dem Einbauen des Switches die folgenden Sicherheitsanweisungen durchlesen:

WARNUNG: Die Installation und der Ausbau des Geräts darf nur durch Fachpersonal erfolgen.

Das Gerät sollte nicht an eine ungeerdete Wechselstromsteckdose angeschlossen werden.

Das Gerät muß an eine geerdete Steckdose angeschlossen werden, welche die internationalen Sicherheitsnormen erfüllt.

Der Gerätestecker (der Anschluß an das Gerät, nicht der Wandsteckdosenstecker) muß einen gemäß EN 60320/IEC 320 konfigurierten Geräteeingang haben.

Die Netzsteckdose muß in der Nähe des Geräts und leicht zugänglich sein. Die Stromversorgung des Geräts kann nur durch Herausziehen des Gerätenetzkabels aus der Netzsteckdose unterbrochen werden.

Der Betrieb dieses Geräts erfolgt unter den SELV-Bedingungen (Sicherheitskleinstspannung) gemäß IEC 60950. Diese Bedingungen sind nur gegeben, wenn auch die an das Gerät angeschlossenen Geräte unter SELV-Bedingungen betrieben werden.

	Stromkabel. Dies muss von dem Land, in dem es benutzt wird gepr¸ft werden:
Schweiz	Dieser Stromstecker mu? die SEV/ASE 1011Bestimmungen einhalten.
Europe	Das Netzkabel mu? vom Typ HO3VVF3GO.75 (Mindestanforderung) sein und die Aufschrift <HAR> oder <BASEC> tragen. Der Netzstecker muß die Norm CEE 7/7 erfüllen ("SCHUKO").

Warnings and Cautionary Messages

Warning: This product does not contain any serviceable user parts.

Warning: When connecting this device to a power outlet, connect the field ground lead on the tri-pole power plug to a valid earth ground line to prevent electrical hazards.

Warning: This switch uses lasers to transmit signals over fiber optic cable. The lasers are compliant with the requirements of a Class 1 Laser Product and are inherently eye safe in normal operation. However, you should never look directly at a transmit port when it is powered on.

Caution: Wear an anti-static wrist strap or take other suitable measures to prevent electrostatic discharge when handling this equipment.

Caution: Do not plug a phone jack connector in the RJ-45 port. This may damage this device.

Caution: Use only twisted-pair cables with RJ-45 connectors that conform to FCC standards.

Caution: The PoE (Power over Ethernet), which is to be interconnected with other equipment that must be contained within the same building including the interconnected equipmentís associated LAN connections.

Note: When selecting a fiber SFP device, considering safety, please make sure that it can function at a temperature that is not less than the recommended maximum operational temperature of the product. You must also use an approved Laser Class 1 SFP transceiver.

Hinweis: Bei der Wahl eines Glasfasertransceivers muß für die Beurteilung der Gesamtsicherheit beachtet werden, das die maximale Umgebungstemperatur des Transceivers für den Betrieb nicht niedriger ist als die für dieses Produkts. Der Glasfasertransceiver muß auch ein überprüftes Gerät der Laser Klasse 1 sein.

Environmental Statement

The manufacturer of this product endeavours to sustain an environmentally-friendly policy throughout the entire production process. This is achieved though the following means:

Adherence to national legislation and regulations on environmental production standards.

Conservation of operational resources.

Waste reduction and safe disposal of all harmful un-recyclable by-products.

Recycling of all reusable waste content.

Design of products to maximize recyclables at the end of the product's life span.

Continual monitoring of safety standards.

End of Product Life Span

This product is manufactured in such a way as to allow for the recovery and disposal of all included electrical components once the product has reached the end of its life.

Manufacturing Materials

There are no hazardous nor ozone-depleting materials in this product.

Documentation

All printed documentation for this product uses biodegradable paper that originates from sustained and managed forests. The inks used in the printing process are non-toxic.

Purpose

This guide details the hardware features of the switch, including Its physical and performance-related characteristics, and how to install the switch.

Audience

This guide is for system administrators with a working knowledge of network management. You should be familiar with switching and networking concepts.

Zielgruppe Dieser Anleitung ist fuer Systemadministratoren mit Erfahrung im Netzwerkmangement. Sie sollten mit Switch- und Netzwerkkonzepten vertraut sein.

Appendix G: Contact Information

Need to contact Linksys? Visit us online for information on the latest products and updates to your existing products at:	http://www.linksys.com or ftp.linksys.com
Can't find information about a product you want to buy on the web? Do you want to know more about networking with Linksys products? Give our advice line a call at:	800-546-5797 (LINKSYS)
Or fax your request in to:	949-823-3002
If you experience problems with any Linksys product, you can call us at:	800-326-7114
Don't wish to call? You can e-mail us at:	support@linksys.com
If any Linksys product proves defective during its warranty period, you can call the Linksys Return Merchandise Authorization department for obtaining a Return Authorization Number at: (Details on Warranty and RMA issues can be found in the Warranty Information section in this Guide.)	949-823-3000