ProConnect® II Series

Layer 2 Management 4-Port Gigabit Ethernet Switch

Use this guide to install:
PC22604

User Guide

LINKSYS®

Table of Contents

Introduction

ProConnect II Layer 2 Management 4-Port Gigabit Ethernet Switch

Maximize your network potential with this high-speed, high-reliability, manageable and stackable switch. The ProConnect® II Layer 2 Management 4-Port Gigabit Ethernet Switch from Linksys delivers a combination of wire-speed Ethernet, Fast Ethernet, and Gigabit solutions, all in one surprisingly affordable package. Perfect for demanding enterprise environments, this switch's intelligent design and built-in SNMP provide maximum network control, regulating traffic and eliminating server bottlenecks. Its web browser-based management interface and upgrade capability makes it ideal for busy network administrators. The Switch is rack mountable and includes four Expansion Slots that accept optional Gigabit Modules (fiber or copper) to let you grow your network as your needs grow. Three Port Trunking groups eliminate bottlenecks, and you can stack up to eight switches and manage them as one. So when you're ready to bring your network up to speed, get Linksys reliability, manageability, stackability, and expandability -- with the ProConnect® II Layer 2 Management 4-Port Gigabit Ethernet Switch.

- Four 10/100 auto-MDI/MDI-X ports and Four Gigabit Expansion Slots - speeds up to 1000Mbps

- Optimizes your network traffic with 802.1q VLAN support and 802.1p traffic prioritization

- Stacking support for up to eight switches lets your network grow

- Manageable via Console, Telnet, web browser, and SNMP/RMON

- 256K Packet Buffer and 32K MAC address entries

- IEEE 802.1Q VLAN support for up to 128 groups

- IGMP Multicast Filtering and Snooping

- Supports 3 Port Trunking groups that include up to 4 10/100 ports and up to 2 ports for the Gigabit modules

- IEEE 802.1d Spanning Tree support for redundant connections

1

Getting to Know the Switch

The RJ-45 Ports

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

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 the *Twisted-Pair Cabling* section.

LEDs

Act	Green. Lights to indicate that the switch is successfully connecting to the network. Blinks to indicate the switch is actively receiving or sending the data over the port.
10	Amber. Lights to indicate that the port is operating at 10 Mbps.
100	Green. Lights to indicate that the port is operating at 100 Mbps.
1000	Green. Lights to indicate that the port is operating at 1000 Mbps.
FDX/COL	Amber. Lights to indicate that the port is operating in full-duplex mode. Blinks to indicate that the connection is experiencing collisions.
Fan	Red. Lights to indicate that the fans are not active.
TEMP	Red. Lights to indicate that the switch exceeds its operational temperature.
Power	Green. Lights to indicate that the switch has power.

The Gigabit Expansion Ports

The Switch is equipped with four expansion ports that provide for the installation of up to four expansion modules. 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, you will need to install an EFPC2SC or EFP2GE Gigabit expansion module and use Category 5e cabling or fiber optic cabling. for more information on fiber optic cabling, refer to the *Fiber Optic Cabling* section.

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.

The Back Panel

Power   Where the AC power cord connects.

FAN   Radiates the heat inside the system.

Buzzer   Warns you if the system overheats. To disable the warn-
                    ing system, use a pen point or similar object to push in
                    the button and the buzzer will not sound if the system
                    overheats.

Installing the Switch

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 Considerations

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:

• Make sure that the switch is accessible and that the cables can be connected easily.

• Keep cabling away from sources of electrical noise, power lines, and fluorescent lighting fixtures.

• Position the Switch away from water and moisture sources.

• To ensure adequate air flow around the Switch, be sure to provide a minimum clearance of two inches (50 mm).

• Do not stack free-standing Switches more than four units high.

Desk Top or Shelf Mounting the Switch

1. Place the Switch on a desktop or shelf near an AC power source and following the guidelines of the preceding paragraph, Positioning the Switch.

2. Connect one end of a standard network cable to one of the 10/100/1000 RJ-45 ports on the front of the Switch.

3. Connect the other end of the cable to the network device, such as a printer, server, workstation or router.

4. Connect one end of the power cable to the switch and the other end into a standard electrical outlet. When the Switch receives power, the Power LED will remain solid Green.

The installation is complete.

Rack-Mounting the Switch

The Switch can be installed in a standard 19-inch rack.

Before you begin, disconnect all cables from the Switch.

1. Place the Switch right side up and with the front panel facing you.

2. Position a mounting bracket over the screw holes on one side of the Switch.

3. Secure the mounting bracket by inserting a screw into each of the three screw holes. Use a screwdriver to tighten the screws, ensuring that they are fastened firmly in place.

4. Repeat steps 2 and 3 to install the other mounting bracket on the opposite side of the Switch.

5. Insert the Switch into the 19-inch rack and secure it with suitable screws (not provided). Ensure that the ventilation holes are not obstructed.

The rack-mount installation is complete.
You can now re-connect the cables to the back of the Switch.

Powering On and Resetting the Switch

To power on the Switch, simply connect the power cord to the back of the Switch, then plug the power cord into an electrical outlet. The Switch will boot up within approximately 30 seconds.

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

Power On Self Test

When you power-on the switch, it performs a Power-On Self Test (POST). During the POST, the Switch's CPU:
- Performs a series of diagnostic procedures to make sure the basic system is functioning with integrity.
- Decompresses the main switching software run-time image from the flash ROM into DRAM area.
- Begins executing the main switching software. During the POST process if the Esc key is pressed, a COMMAND LINE prompt appears.

Download Runtime Software from Console Port	This option downloads the runtime system image to the Switch through the Switch's Console port. Before you select this option, make sure: • A host system is running a terminal emulation program that supports the Kermit file transfer protocol. • The host system's hard drive has the required binary file that will be downloaded to the switch.
Configure the System	This option lets you modify any configurable parameter in the switch's flash ROM before the switch system boots.
Run Manufacturing Diagnostics	This option downloads the manufacturer's diagnostics. This option has the same download requirements as the runtime software applied. When the file transfer is completed, the target system jumps to the entry point of the diagnostic program and starts executing the diagnostic code. The Main Menu of the diagnostic program appears, where you can initiate tests or obtain system information. Note that user intervention is not required when a test runs, unless an error occurs. If an error occurs during testing, you are given the choice of continuing the diagnostics or skipping the error.

Uplinking the Switch

All four ports on the Switch can act as uplink ports, allowing you to uplink to other switches or hubs using a standard Ethernet connection.

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

Installing the Gigabit Expansion Modules

Use the following instructions to install the Gigabit Expansion Modules:

Before you begin, power off the Switch by disconnecting all cables from the Switch.

1. Place the Switch right side up, with the front panel facing you.

2. Use a screwdriver to remove the desired Expansion Module cover plate (labeled "Module 1", "Module 2", "Module 3", "Module 4"). Set the screws aside for step 4.

3. Insert the Gigabit Expansion Module (must be purchased separately) into the selected Gigabit Expansion Port, ensuring that it is seated firmly in place.

4. Secure the module in place using the screws and a screwdriver.

**The Gigabit Expansion Module installation is complete.
You can now re-connect the cables to the back of the Switch.**

EFPC2GE - Gigabit Ethernet
EFPC2SC - Gigabit Fiber Optic

Switch Management

Overview

The Switch offers an easy-to-use, menu-driven console interface. Using this interface, you can perform various switch configuration and management activities, including:

- Configuring system and port parameters
- Assigning an IP address to the Switch
- Configuring routing properties
- Configuring ARP
- Configuring DHCP
- Setting VLAN policies
- Setting packet filtration
- Configuring STP and SNMP parameters
- Upgrading firmware

There are four methods of managing the Switch:

- Local Console Management using the serial port
- Remote Console Management using telnet
- Using an SNMP Management Station
- Web-Browser

Local Console Management

You can manage the Switch locally by connecting the switch to a PC or workstation with terminal emulation software, such as Hyperterminal, using the serial port.

Before you log on to the Switch, make sure that the Switch's Console port settings are as follows:

```
BAUD RATE:         115200
FLOW:              None
PARITY:            None
STOP BITS:         1
DATA BITS:         8

EMULATION:         ANSI
CURSOR EMULATION:  VT100
```

Remote Console Management

You can manage the Switch remotely by having a remote host establish a Telnet connection to the switch via an Ethernet or modem link.

To use this management method:

- The host must run a SLIP protocol if a modem is used
- The Switch must have an IP address. The default IP address is 192.168.1.254.
- Remote Telnet Login must be enabled on the Switch.

The Remote Console Management interface is identical in appearance and functionality to the Local Console Management interface. If you are using Microsoft's Telnet, the terminal setting should be set to VT100/ANSI.

SNMP Management

You can manage the Switch across a LAN using an SNMP Network Management Station with a graphical user interface. This management method allows you to monitor statistical counters and set switch parameters from the remote Network Management Station.

To use this management method:

- The network must use the IP protocol
- The Switch must be configured on the network with a proper IP address
- SNMP must be enabled on the Switch.

Assigning an IP Address to the Switch

To manage the Switch remotely using Telnet or with an SNMP Management Station, you must assign an IP address to the Switch. To assign an IP address to the Switch, refer to the **Configuring the Switch** section.

Logging On to the Switch

When you log on to the Switch for the first time, a sign-in string appears and you are prompted for a *console login name* and *password*. The factory default login name is set as "**admin**" and the password is blank. You can create a password after you log on.

Configuring the Switch

Overview

The Switch features a menu-driven console interface for switch configuration. The Switch can be configured locally through the console port using terminal emulation software, such as Hyperterminal, or remotely via a Telnet connection.

Web-Based Configuration and Management

This **User Guide** provides instructions on how to configure and manage the Switch using the console interface. If you wish to manage the switch through a web connection, you can do so by connecting to the Switch's IP Address using your web browser.

Although the web-based management menu will differ in appearance from the console-based management menu, you will still have access to all the same configuration and management features.

Logging On

When logging on to the Switch, you will receive the following screen prompt:

```
Linksys ProConnect II 2604 Gigabit Switch
Screen Name:

System Name: PC22604
Console Login:admin
Password:
```

Enter the default *login, **admin,*** and leave the password blank, pressing **Enter** after each entry (as shown in the image below).
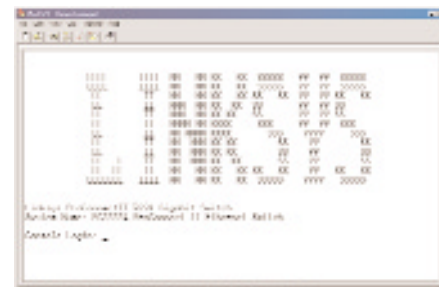
Basic Management Activities

After you log on to the Switch, the *Switch Management* screen will appear.
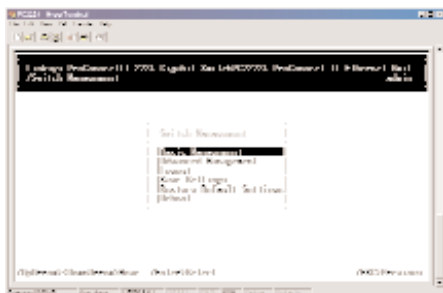
The *Switch Management screen* consists of a series of menus. Each menu has several options, which are listed vertically. A highlight in each menu lets you select the option you wish to choose; pressing the **Enter** key activates the highlighted option.

To navigate through the Console Interface use the *Up Arrow* or *Down Arrow* keys to move up or down, 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. Note that the bottom of the window always has a listing of the appropriate key strokes.

Basic management activities consist of General, LAN port, and console port tasks. To perform basic management activities:

1. From the Switch Management screen, highlight *Basic Management* and press **Enter**. The *Basic Management* screen will appear.
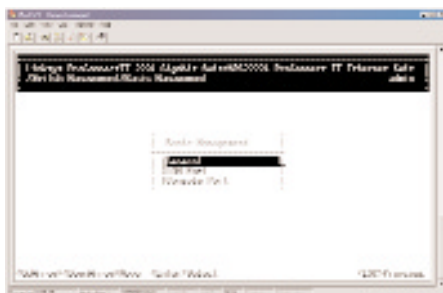
2. From the *Basic Management* screen, highlight the desired option and press the **Enter** key:

- **General** allows you to change the system name, contact, location, administration and guest passwords, statistics collection, reboot-on-error, remote Telnet login, and remote HTTP login.

- **LAN Port** allows you to configure line speed and flow control, Admin Control, and view the physical address of the Switch.

- **Console Port** allows you to change the console baud rate, flow control method, modem control, and setup string; enable or disable SLIP; and configure the SLIP address and SLIP subnet mask.

General Management Configuration

Select *General* from the *Basic Management* screen. The *General* screen will appear with the *System Name* highlighted.
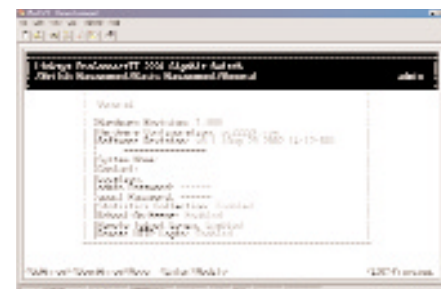
Use the following procedure to configure the general management options:

Changing the System Name
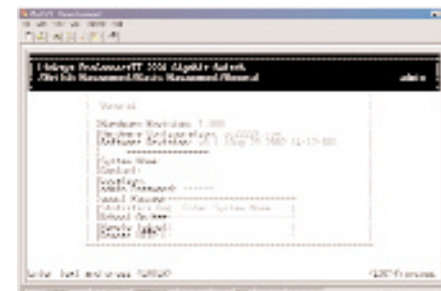
1. From the *General* screen, highlight *System Name* and press the **Enter** key. The *Enter System Name* screen appears.

2. Enter a system name (16 characters max.). If you make a mistake, use the **Backspace** key to delete the error.

3. Press **Enter** to return to the *General* screen.

Changing the Contact

To change the contact:

1. From the General screen, highlight Contact and press the Enter key. The Enter Contact screen appears.
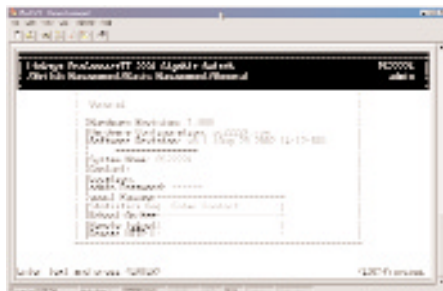
2. Enter a contact name. If you make mistakes, use the Backspace key to delete the error.

3. Press the Enter key to return to the General screen.

Changing the Location

1. From the *General* screen, move the cursor to *Location* and press the **Enter** key. The *Enter Location* screen will appear.
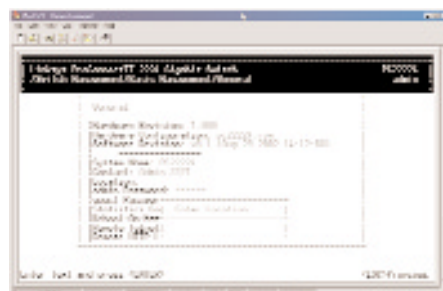
2. Enter a location name. If you make a mistake, use the **Backspace** key to delete the error.

3. Press **Enter** to return to the *General* screen.

14

Changing the Administration Password

1. Use the *Down Arrow* key to highlight *admin Password* and press the **Enter** key. The *Enter Old Password* screen will appear.
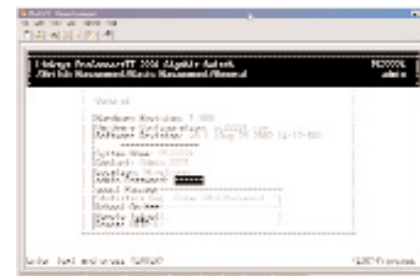
2. Enter the current password. Each character you type appears as an asterisk (*). If you make a mistake, use the **Backspace** key to delete the error.

3. Press **Enter**. The *Enter New Password* screen will appear.

4. Enter the new password. For security, each password character you type appears as an asterisk (*). The password is case-sensitive, can be no more than 16 characters (only alphanumeric characters and the underscore "_" character can be used).

15

5. Press **Enter**. A screen will prompt you to re-enter the new password.

6. Re-enter the new password you typed in step 4 and press **Enter**. The *Password Changed* message will appear, confirming that the new password is in effect.
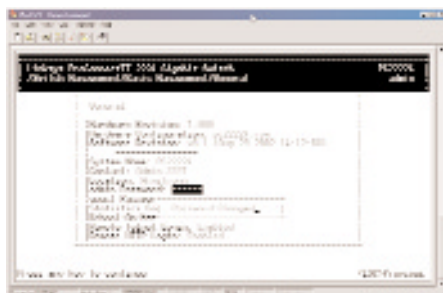
7. Press **Enter** to remove the message and return to the *General* screen. The admin password will appear as asterisks in the *admin Password* field.

Changing the Guest Password

1. Use the *Down Arrow* key to highlight *guest Password* and press the **Enter** key. The *Enter New Password* screen will appear.
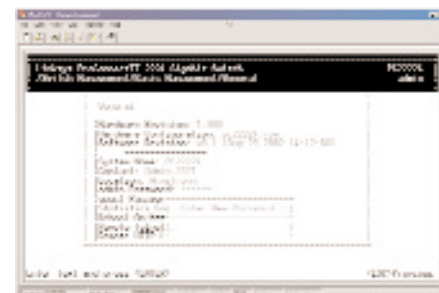
2. Enter a new guest password. If you make a mistake, use the **Backspace** key to delete the error. The password is case-sensitive, can be no more than 16 characters (only alphanumeric characters and the underscore "_" character can be used).

3. Press **Enter** to return to the *General* screen.

Statistic Collection

1. From the *General* screen, highlight *Statistic Collection* and press the **Enter** key. The following screen will appear.
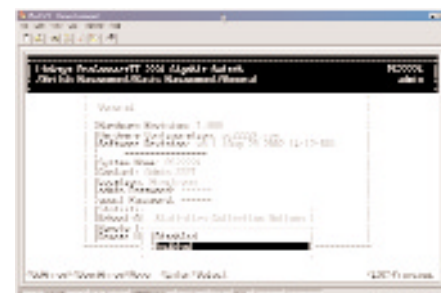
2. Highlight one of the following choices:

  Disabled (prevents active statistic collection for each port)

  Enabled (allows active statistic collection for each port)

3. Press **Enter** to return to the *General* screen.

Reboot-on-Error

1. From the *General* screen, highlight *Reboot-On-Error* and press the **Enter** key. The following screen will appear.
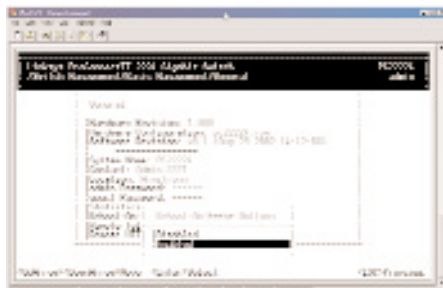
2. Highlight one of the following choices:

   Disabled (prevents the Switch from automatically resetting when a fatal error is detected. This setting is useful when a persistent problem needs to be reported)

   Enabled (allows the Switch to automatically reset when a fatal error is detected)

3. Press **Enter** to return to the *General* screen.

Remote Telnet Login

1. From the *General* screen, highlight *Remote Telnet Login* and press the **Enter** key. The following screen will appear.
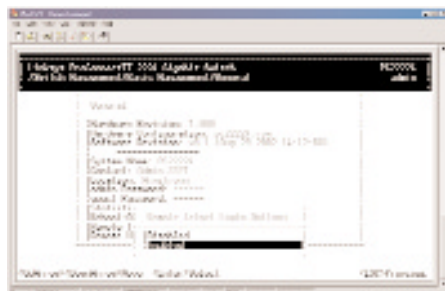
2. Highlight one of the following choices:

   Disabled (prevents remote Telnet logins to the Switch)

   Enabled (allows remote Telnet logins to the Switch. This is the default setting)

3. Press **Enter** to return to the *General* screen.

Remote Http Login

To enable or disable the function of Remote Http Login:

1. From the General screen, highlight Remote Http Login and press the Enter key. The following screen will appear:
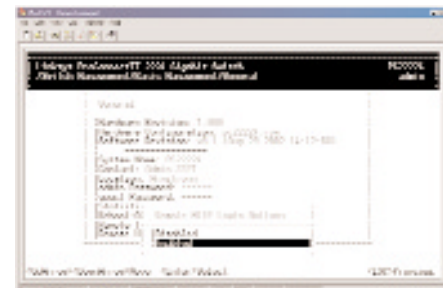
2. Highlight one of the following choices:

   Disable prevents remote HTTP login to the switch.

   Enable allows remote HTTP login to the switch.

3. Press the Enter key to go back to the General screen.

Returning to the Basic Management Screen

After completing the general management activities, press the **Esc** key to exit the *General* screen and return to the *Basic Management* screen. You can then select another option from the *Basic Management* screen or press **Esc** to return to the *Switch Management* screen.

LAN Port Configuration

Select *LAN Port* from the *Basic Management* screen. The *LAN Port Configurations* screen will appear, with *Speed & Flow Control* highlighted.

Use the procedures in this section to configure the *LAN Port Configuration* options for one or more ports, including:

• *Speed & Flow Control*
• *Administration Control*
• *Physical Address*

Changing the Speed and Flow Control

1. From the *LAN Port Configurations* screen, highlight *Speed & Flow Control* and press the **Enter** key. A screen similar to the following will show the current line speed settings for all ports. If an expansion module is installed in the switch, it will also be listed.

2. You configure each port individually. To configure an individual port, highlight it and press **Enter**. The *Port Setting Options* screen will appear

3. Proceed to the appropriate section:

   To set the line speed, proceed to *the* **Setting the Line Speed** section

   To set the flow control, go to the section on **Changing the Flow Control.**

Setting the Line Speed

1. Press **Enter** with the *Speed & Flow Control* value highlighted . The *Speed & Flow Control Options* menu will appear.
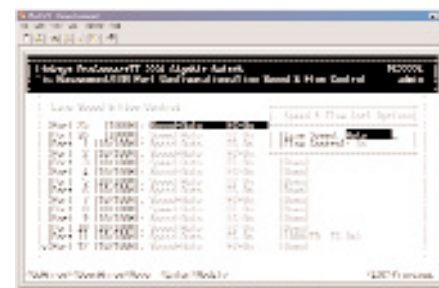
2. Highlight the line *Speed Option* you want to select for the port. *Auto* allows the Switch to automatically determine the line speed and duplex mode. All the other selections force the Switch to use a specific line speed and duplex mode.

3. Press **Enter**. You will return to the *Speed & Flow Cntl Options* screen and the line speed setting you selected appears next to *Line Speed*.

4. To configure the flow control for this port, proceed to **Changing the Flow Control**.

5. To configure the line speed for additional ports, press **Esc** to remove the *Speed & Flow Cntl Options* screen. Then highlight the port you want to configure and repeat steps 1 through 4.

6. When you finish, press the **Esc** key from the *Line Speed & Flow Control* screen to return to the *LAN Port Configurations* screen.

Changing the Flow Control

1. With the *Speed & Flow Cntl Options* screen displayed, press the *Down Arrow* key to highlight *Flow Control* and press **Enter**. The *Flow Cntl Options* screen will appear.
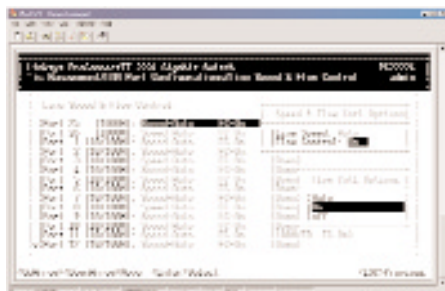
2. Highlight the desired flow control option for the port. *Auto* allows the Switch to automatically determine whether or not to use flow control. *On* enables flow control at all times. *Off* disables flow control at all times.

3. Press **Enter**. You will return to the *Speed & Flow Cntl Options* screen, and the selected flow control setting will appear next to *Flow Control*.

4. To configure the flow control for additional ports, press **Esc** to remove the *Speed & Flow Cntl Options* screen. Highlight the desired port then press **Enter**. Highlight *Speed* and *Flow Control*, then press **Enter.** Repeat steps 1 through 3 for each additional port.

5. When you are finished, press the **Esc** key from the *Line Speed & Flow Control* screen to return to the *LAN Port Configurations* screen.

Admin Control

1. From the *Port Settings Options* menu, select **Admin Control** and press the **Enter** key.

2. The *Admin Status Options* menu will appear.

3. Select **Up** to allow administration of the Switch per port or **Down** to disallow.

Displaying Physical Port Address

The following procedure describes how to display the physical address of the Switch.

1. From the *LAN Port Configurations* screen, highlight *Physical Address* and press the **Enter** key. A screen similar to the following (see next page) will appear.

Returning to the Basic Management Screen

After completing the general management activities, press the **Esc** key to exit the *General* screen and return to the *Basic Management* screen. You can then select another option from the *Basic Management* screen or press **Esc** to return to the *Switch Management* screen.

Console Port Configuration

Select *Console Port* from the *Basic Management* screen, the *Console Port Configurations* screen will appear, with the *Baud Rate* value highlighted.
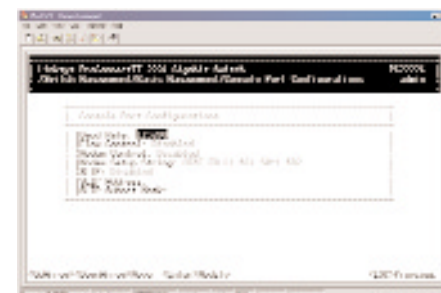
Use the procedures in this section to configure the *Console Port Configurations* options for one or more settings, including:

*   Specifying *Baud Rate*

*   Specifying *Flow Control*

*   Enable or Disable *Modem Control*

*   Enter *Modem Setup String*

*   Enable or Disable *SLIP*

*   Specify a *Slip Address*

*   Specify a *SLIP Subnet Mask*

22

23

Changing the Console Baud Rate

1. From the *Console Port Configurations* screen, highlight *Baud Rate* and press the **Enter** key. A screen similar to the following will show the current console baud rate.
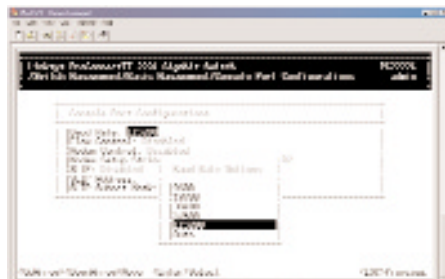
2. Highlight the baud rate you want to select for the console. *Auto* allows the Switch to autosense the baud rate between 9600 bps and 115,200 bps. If you choose *Auto*, it will choose the rest of your configuration selections. Then, when you exit the configuration program, press the **Enter** key one or more times until the prompt *Linksys Switch Login Password* appears on your computer screen. All other selections force a specific console baud rate.

3. Press **Enter**. You will return to the *Console Port Configurations* screen and the selected console port baud rate will appear in the *Baud Rate* field.

Selecting a Flow Control Method

1. From the *Console Port Configurations* screen, highlight *Flow Control* and press the **Enter** key. A screen similar to the following will show the current console flow control method.
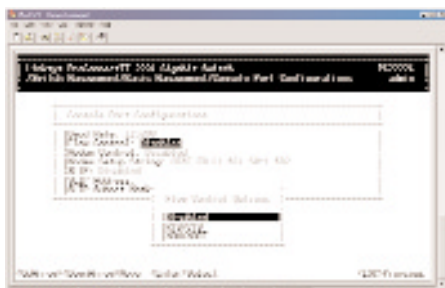
2. Highlight the desired flow control method for the console and press **Enter**. You will return to the *Console Port Configurations* screen and the selected flow control method will appear in the *Flow Control* field.

Enabling or Disabling Modem Control Options

1. From the *Console Port Configurations* screen, highlight *Modem Control* and press the **Enter** key. A screen similar to the following will show whether a console modem connection is enabled or disabled.
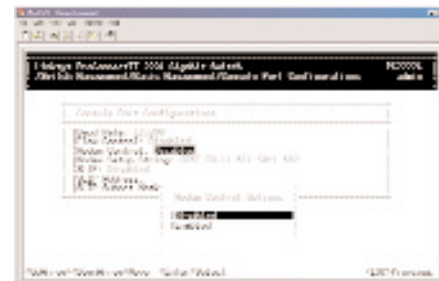
2. Highlight *Enabled* or *Disabled* in the *Modem Control Options* field to either enable or disable a modem connection to the console port.

3. Press **Enter**. You will return to the *Console Port Configurations* screen and the modem control option you selected will appear in the *Modem Control* field.

Specifying a Modem Setup String

If you enabled a modem connection to the console port, use the following procedure to specify a modem setup string.

1. From the *Console Port Configurations* screen, highlight *Modem Setup String* and press the **Enter** key. A screen similar to the following will show the current modem setup string option.
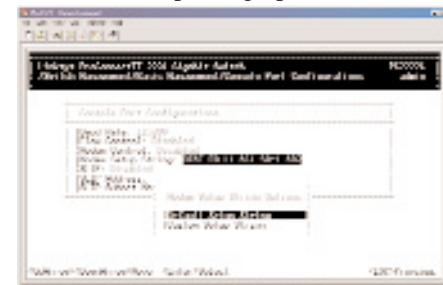
2. Highlight the desired modem setup string option.

> *Note: Switch setup, when accessed through a modem or SLIP account, is the sole responsibility of the user. Technical support is not provided for setup of modem or SLIP.*

3. Press the **Enter** key. If you highlight *Default Setup String*, you will return to the *Console Port Configurations* screen and the default modem string will appear in the *Modem Setup String* field. If you highlight *Custom Setup String*, enter the custom string in the *Enter Modem Setup String* screen and press **Enter** again. You will return to the *Console Port Configurations* screen and the custom setup string will appear in the *Modem Setup String* field.

Enabling or Disabling SLIP

1. From the *Console Port Configurations* screen, highlight *SLIP* and press the **Enter** key. A screen similar to the following will show the current SLIP setting.
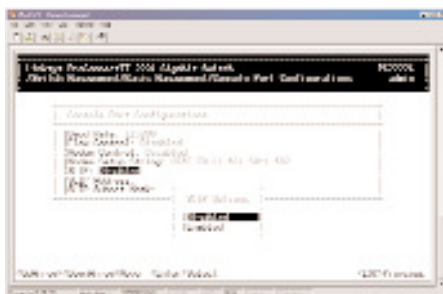
2. Highlight *Enabled* or *Disabled* to either enable or disable SLIP, then press **Enter**. You will return to the *Console Port Configurations* screen and the selected SLIP option will appear in the *SLIP* field.

> ⚠️ **Note:** *if you enable SLIP, a warning window will appear telling you to disable SLIP if you encounter problems. By enabling SLIP, the switch cannot be directly accessed through the console port with the provided serial cable.*

Specifying a SLIP Address

If you enabled SLIP, use the following procedure to enter an address that has a network part different than the network address of the Switch (for more information, contact your network administrator).

1. From the *Console Port Configurations* screen, highlight *SLIP Address* and press **Enter**. The following screen (see next page) will appear.

---
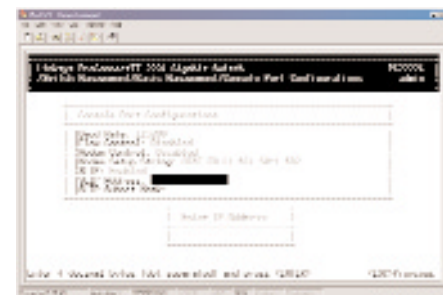
2. Enter the SLIP address. The address consists of numbers separated by periods (e.g., 192.168.1.105).

3. After you enter the SLIP address, press the *Enter* key. You will return to the *Console Port Configurations* screen and your entry will appear in the *SLIP Address* field.

Specifying a SLIP Subnet Mask

If you are using SLIP, enter a suitable SLIP subnet mask.

1. From the *Console Port Configurations* screen, highlight *SLIP Subnet Mask* and press **Enter**. The *Enter IP Subnet Mask* screen will appear.
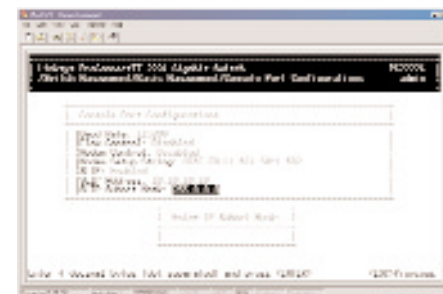
2. Enter the SLIP subnet mask. The subnet mask consists of numbers separated by periods (e.g., 255.255.255.0).

3. After you enter the SLIP subnet mask, press the **Enter** key. You will return to the *Console Port Configurations* screen and your entry will appear in the *SLIP Subnet Mask* field.

Returning to the Basic Management Screen

After completing the general management activities, press the **Esc** key to exit the *Console Port* screen and return to the *Basic Management* screen. You can then select another option from the *Basic Management* screen or press **Esc** to return to the *Switch Management* screen.

Advanced Management Activities

Advanced management activities consist of the Layer 2 switching database, IP networking, Bridging, Static Filtering, Spanning Tree, SNMP, Stacking, Other Protocols, Port Trunking, Port Mirroring, QOS Setup, and File Transfer.

To perform advanced management activities:

1. From the *Switch Management* screen, highlight *Advanced Management* and press **Enter**. The *Advanced Management* screen will appear.
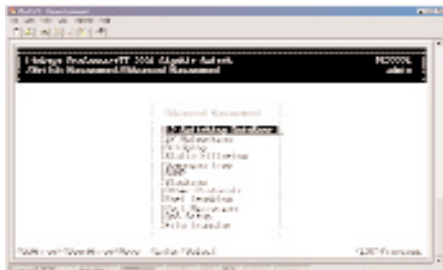
2. In the *Advanced Management* screen, highlight the desired option and press the **Enter** key.

The following options are available:

*   *L2 Switching DataBase* lets you view and change VLAN and PVID, IP multicast group, MAC address, and Port Perspectives.

*   *IP Networking* allows you to view or change IP settings, ARP and routing table parameters, RIP parameters, DHCP gateway settings, and ping settings.

*   *Bridging* lets you view and change the aging period for a MAC address and set the *Flood Limits* for all ports.

*   *Static Filtering* allows you to view, add, delete, or search all source or destination addresses to be filtered.

*   *Spanning Tree* lets you view and change parameters relating to the spanning tree protocol.

*   *SNMP* allows you to view, enable, and change all SNMP-related information.

*   *Stacking* allows you to set up the stack configuration.

*   *Other Protocols* lets you view and change GVRP and IGMP settings.

*   *Port Trunking* allows you to assign a range of ports to trunking groups.

*   *Port Mirroring* lets you mirror one port to another.

*   QoS Setup allows for the configuration of Quality of Service.

*   *File Transfer* allows you to upgrade your Switch software.

Switching Database Configuration

Select *L2 Switching DataBase* from the *Advanced Management* screen and press **Enter**. The *L2 Switching DataBase* screen will appear, with *VLAN & PVID Perspective* highlighted.
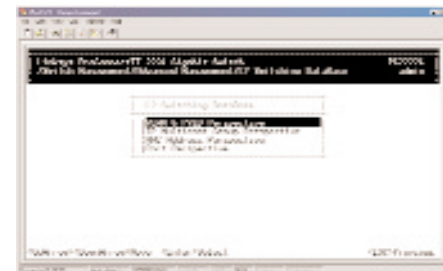
The Switch can be viewed from the four perspectives in the *L2 Switching DataBase* screen.

*   *VLAN & PVID Perspective*

*   *IP Multicast Group Perspective*

*   *MAC Address Perspective*

*   *Port Perspective*

These four views allow a network administrator to manage and monitor VLANs and their associated MAC addresses and ports effectively from different views.

VLAN & PVID PERSPECTIVE

This section describes the default VLAN and how to obtain a VLAN perspective.

Default VLAN

The IEEE 802.1Q standard defines VLAN ID #1 as the default VLAN. The default VLAN includes all the ports as the factory default. The default VLAN's egress rule restricts the ports to be all untagged, so it can, by default, be easily used as a simple 802.1D bridging domain. The default VLAN's domain shrinks as untagged ports are defined in other VLANs.

Obtaining a VLAN Perspective

The following procedure describes how to obtain a VLAN perspective. For convenience, the VLAN ID appears as both decimal and hexadecimal values side by side in the *VLAN Perspective* screen.

1. From the *L2 Switching DataBase* screen, highlight *VLAN & PVID Perspective* and press the **Enter** key. The *VLAN & PVID Perspective* screen will appear. Select VLAN settings.
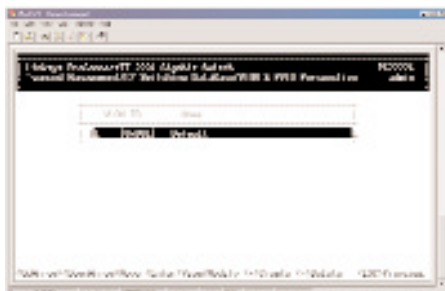
From this screen you will be able to:

*   Create a new VLAN

*   Delete a VLAN ID

*   View VLAN activities

*   View or change a VLAN Configuration

To return to the *VLAN & PVID Perspective* screen, press the **Esc** key.

Creating a New VLAN

1. From the *VLAN Perspective* screen in, hold down the **Shift** key and press the "+" key. The *New VLAN Settings* screen will appear.
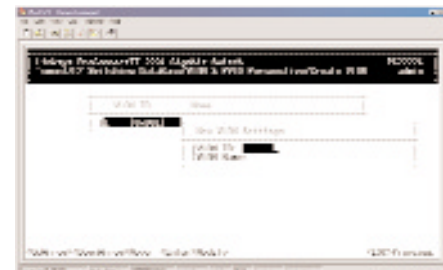
2. With the *VLAN ID* field highlighted, press the **Enter** key. The *Enter New VLAN ID* screen will appear.
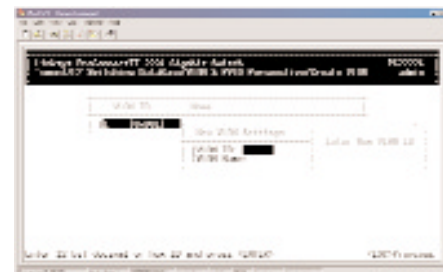
3. Enter a new VLAN ID as either a decimal or hexadecimal ID value from 1 to 4094 (0xFFE).

4. Press **Enter**. The VLAN ID appears next to *VLAN ID* in the *New VLAN Settings* screen.

5. To enter an optional VLAN name, perform the following steps (the VLAN name is used to identify the VLAN at the local switch).

    a) Press the **Down Arrow** key to move to *VLAN Name*.

    b) Press **Enter**. The *Enter New VLAN Name* screen will appear.

c) Enter a name for the new VLAN (up to 31 alphanumeric characters).

d) Press **Enter**. The VLAN name appears next to *VLAN Name* in the *New VLAN Settings* screen.

6. Press the **Esc** key. A screen similar to the following will appear.

This screen will allow you to add or delete switch port to a VLAN.

Adding New Switch Ports

To add new switch ports to the newly created VLAN:

1. Hold down the **Shift** key and press "**+**" to display the *Port Options* screen.

2. In the *Port Options* screen, highlight either *Untagged Ports* or *Tagged Ports* and press the **Enter** key.If you highlight *Untagged Ports*, the screen window reads *Select Untagged Ports*, as in the following screen. Ports not allowed to be used in specific VLANs are labeled *Forbidden Ports*.

If you highlight *Tagged Ports*, the screen window reads *Select Tagged Ports*, as in the following screen.

3. In the *Select Untagged Ports* or *Select Tagged Ports* screen, use the **Up Arrow** and **Down Arrow** keys to highlight an individual port.

4. Press **Enter**. An asterisk appears to the right of the selected port. Repeat this step for each new port you want to add.

5. After selecting the new ports you want to add, press **Esc**. A screen will show the selected ports and whether they are tagged or untagged.

6. If you added untagged ports and want to now add tagged ports, or vice versa, repeat steps 1 through 4 and in step 2 select the appropriate port option. To remove a port, highlight the desired port and press "**-**".

32

33

7. Press Esc to return to the *VLAN Perspective* screen. You may then select another option from the *VLAN Perspective* screen or press **Esc** to return to the *L2 Switching DataBase* screen.

The VLAN IDs and names you added will appear in the *VLAN Perspective* screen. In the following screen, the Zuma and lana VLAN IDs have been added.

Deleting a VLAN ID

Use the following procedure to delete a VLAN ID from the *VLAN Perspective* field.

1. Use the **Up Arrow** and **Down Arrow** keys to highlight the VLAN ID you want to delete.

2. Press the "**-**" (hyphen) key. A message will ask whether you are sure you want to delete the VLAN ID.

3. With *Yes* highlighted, press the **Enter** key to delete the VLAN ID, or to retain it, press the **Esc** key or highlight *No* and press **Enter**.

Viewing VLAN Activities

The following procedure describes how to use the *VLAN Perspective* screen to view activities for a particular VLAN. Using this procedure, you can view:

• Active ports.
• Active MAC addresses associated with a VLAN.
• A transient address, if any.
• Filtering and port information.

To view VLAN activities:

1. From the *VLAN Perspective* screen , highlight an existing VLAN and press the **Enter** key.

2. The *VLAN Info* screen appears, with the highlight on *VLAN Activities*. Press the **Enter** key.

This screen shows all active MAC addresses and VLAN domains for the VLAN you selected.

• MAC addresses are those that have been sending frames from this VLAN to the switch within the last aging period.

• VLAN domain shows the domains in this VLAN from which active MAC addresses have been learned within the last aging period.

You can use the **Tab** key to move between the *MAC Addresses* and *VLAN Domain* screens.

Searching for MAC Addresses

To search for MAC addresses:

1. In the *VLAN MAC Address* screen, press **S**. The *Enter MAC Addr To Search* screen will appear.

2. Enter a MAC address in the *Enter MAC Addr To Search* screen and press the **Enter** key. If the address is found, it is highlighted in the *MAC Addresses* screen.

Obtaining Additional Information

To obtain additional information about an active MAC address:

1. In the *MAC Addresses* screen, scroll to the desired address.

2. Press the **Enter** key. A *VLAN/IP Multicast Group Membership* screen similar to the following will appear.

3. Press **Esc** to remove the *VLAN/IP Multicast Group Membership* screen.

Scrolling Through Domains

When the *VLAN Domain* screen is active, you can use the **Up Arrow** and **Down Arrow** keys to scroll through the list of domains associated with the selected VLAN.

Exiting the VLAN Screens

When you finish performing VLAN activities, press the **Esc** key until you return to the desired screen.

Viewing VLAN Settings

Using the *VLAN Configuration* screen, you can view VLAN settings.

1. From the *VLAN Perspective* screen, highlight an existing VLAN and press the **Enter** key. A screen similar to the following will appear, with the high-light on *VLAN Activities*.
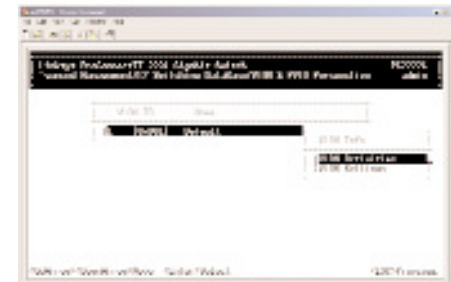
2. Press the **Up Arrow** or **Down Arrow** key to highlight *VLAN Settings*.

3. Press **Enter**. A screen similar to the following will appear.

4. From this screen, you can add or delete switch ports from any VLAN except the default VLAN. The controls for adding and deleting ports are not displayed for the default VLAN.

Adding Ports

To add ports to a VLAN:

1. After following the previous four steps of *Viewing VLAN Settings*, hold down the **Shift** key and press "+". The *Port Options* screen will appear.

2. Select either *Untagged Ports* or *Tagged Ports*. Ports not allowed to be used in specific VLANs are labeled as *Forbidden Ports.*

To select *Untagged Ports*:

• Highlight *Untagged Ports* and press **Enter**. The *Select Untagged Ports* screen will appear, along with a list of the untagged ports that are not in use. Initially, there are 8 untagged ports you can select; this number decreases as you use untagged ports in your VLANs. In the following example, only untagged port 9 is available.

• To select an individual port, highlight it and press **Enter**. An asterisk will appear next to each port you select (to deselect it, press **Enter** again to remove the asterisk).

To select all ports, highlight *All Ports* and press **Enter**.

• Press **Esc**. The port(s) you selected appear in the previous screen.

To select tagged ports:

• Highlight *Tagged Ports* and press **Enter**. The *Select Tagged Ports* screen will appear, along with a list of the tagged ports.
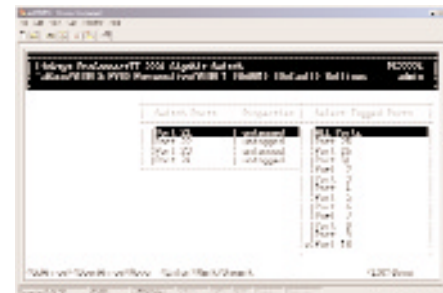
• To select an individual port, highlight it and press **Enter**. An asterisk will appear next to each port you select (to deselect it, press **Enter** again to remove the asterisk).

To select all ports, highlight *All Ports* and press **Enter**.

• Press **Esc**. The port(s) you selected will appear in the previous screen.

3. When you finish, press **Esc** until you return to the desired screen.

Deleting Ports

The following procedure describes how to delete ports from a VLAN. Since there is no precautionary message that appears before you delete a VLAN port, be sure you want to delete the port before you begin.

1. From the screen in step 3 of *Viewing VLAN Settings*, use the **Up Arrow** and **Down Arrow** keys to highlight the port you want to delete.

2. Press the "**-**" (hyphen) key. The port is deleted.

Configuring PVID

The PVID is the VLAN that the port is associated with. By default, all ports are associated with the default VLAN of 1. If you want to configure the PVID, highlight the PVID setting from the *VLAN & PVID Perspective* screen and press the **Enter** key. The following screen will appear:
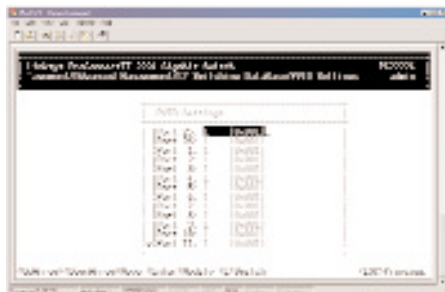
The following steps will show you how to set the PVID.

1. Highlight an individual port you want to configure and press the **Enter** key. The *Enter New PVID* column will appear next to the *PVID Settings* screen.

2. Enter a decimal number in the *Enter New PVID* column. Then press the **Enter** key.

IP MULTICAST GROUP PERSPECTIVE

The IP multicast group perspective provides information associated with an IP multicast group. Use the following procedure to obtain an IP multicast group perspective (prior to this process, set the IGMP in the *Other Protocols* section, step 2.):

1. From the *L2 Switching DataBase* screen, highlight *IP Multicast Group Perspective* and press the **Enter** key. A screen similar to the following will appear.
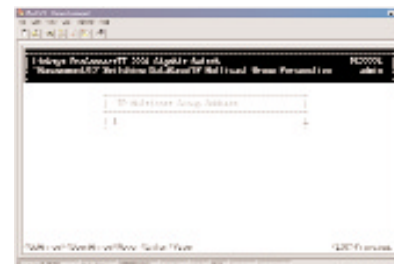
2. To obtain a IP multicast group perspective for one of the addresses in the screen above, use the **Up Arrow** and **Down Arrow** keys to highlight an address and press the **Enter** key. A screen similar to the following will appear.
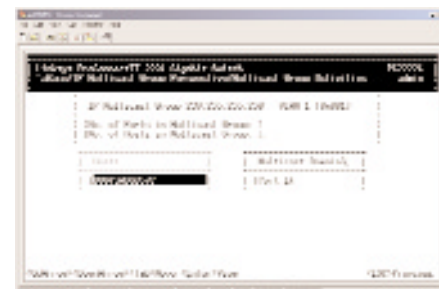
3. To view the VLAN and IP multicast group addresses associated with the MAC address, highlight a host in the *Hosts* screen and press **Enter**. A *VLAN/IP Multicast Group Membership* screen similar to the following will appear.

40

41

4. Use the **Up Arrow** and **Down Arrow** keys to scroll through the *VLAN/IP Multicast Group Membership* screen.

5. When you finish, press **Esc** until you return to the desired screen.

MAC ADDRESS PERSPECTIVE

The MAC address perspective lets you view all characteristics associated with a MAC address, corresponding VLANs, and corresponding ports in the switching database.

To obtain a MAC address perspective:

1. From the *L2 Switching DataBase* screen, highlight *MAC Address Perspective* and press the **Enter** key. You are prompted for a MAC address.
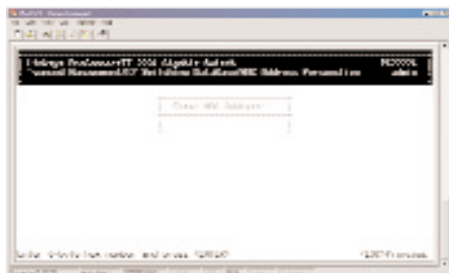
2. Enter the desired MAC address' characteristics, corresponding VLANs, and corresponding ports you want to view.

3. Press **Enter**. A screen similar to the following will appear.

4. Use the **Up Arrow** and **Down Arrow** keys to scroll through the *VLAN/IP Multicast Group Membership* screen.

5. When you finish, press the **Esc** key to return to the desired screen.

42

PORT PERSPECTIVE

The port perspective lets you view VLAN activities, Port Statistics, and MAC Limit.

To obtain a port perspective:

1. From the *L2 Switching DataBase* screen, highlight *Port Perspective* and press the **Enter** key. The *Port Perspective* screen will appear.
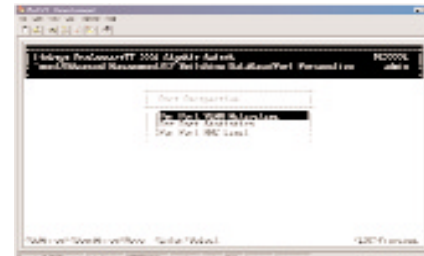
2. To view per-port VLAN activities, highlight *Per Port VLAN Activities*, then press the **Enter** key.

3. To view per-port statistics, highlight *Per Port Statistics*, then press the **Enter** key.

4. To configure the MAC Address learning for each port, highlight *Per Port MAC Limit*.

Per Port VLAN Activities

If you select *Per Port VLAN Activities* from the *Port Perspective* screen, a screen similar to the following *Per Port VLAN Activities* screen appears.

1. Use the **Up Arrow** and **Down Arrow** keys to highlight the desired port number and view the corresponding VLAN activities.

2. Press the **Enter** key. A screen similar to the one on the next page will appear, along with a list of the MAC addresses for the selected VLAN and the corresponding VLAN memberships.

43

Scrolling Through MAC Addresses

Use the following procedure to scroll through the list of active MAC addresses corresponding to the selected port:

1. If the *MAC Addresses* screen is not the current screen, press the **Tab** key until it appears.

2. Use the **Up Arrow** and **Down Arrow** keys to scroll through the list of active MAC addresses for the selected port.

3. To search for a MAC address, press the "**S**" key. When the search prompt appears, enter a MAC address in the *Enter MAC Addr to Search* screen and press the **Enter** key. If the address is found, it will be highlighted in the *Port MAC Addresses* screen.

4. To obtain additional information about a particular MAC address, scroll to the address in the *Port MAC Address* screen and press the **Enter** key. A screen similar to the following will appear, showing detailed information about the selected MAC address.
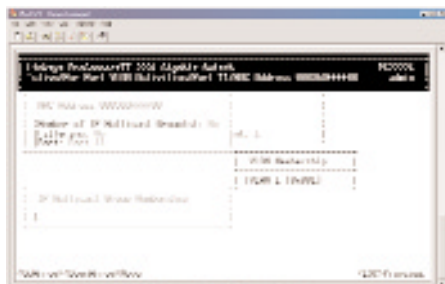
Per Port Statistics

If you select *Per Port Statistics* from the *Port Perspective* screen, a screen similar to the following *Per Port VLAN Activities* will appear.
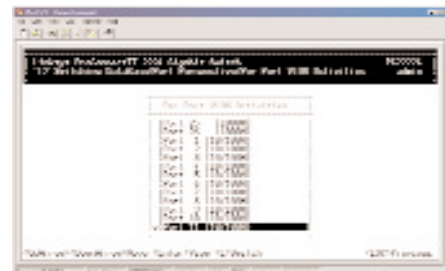
1. To reset counters for all ports, press the "**R**" key. When the following screen appears, highlight *Yes*. Press **Enter** to reset the counters or highlight *No* and press **Enter** to not reset them.

2. To view statistics for a port, use the **Up Arrow** and **Down Arrow** keys to highlight the desired port.

3. Press the **Enter** key. A screen similar to the following will appear, showing the statistics for the port you selected.

4. To reset counters for the port in the screen above, press the "**R**" key. The following screen will appear (see next page).

5. After reviewing this information, press the **Esc** key until you return to the desired screen.

Per Port MAC Limit

If you select Per Port MAC Limit from the Port Perspective screen, a screen similar to the following one appears.
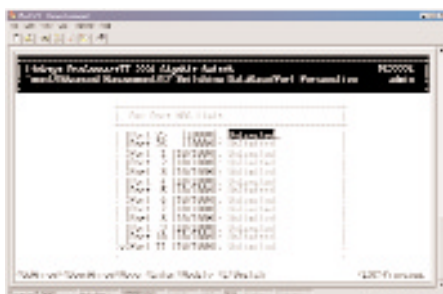
1. To specify MAC learning options for a MAC port, use the Up and Down Arrow keys to highlight a port, then press the Enter key. A MAC Learning Options screen similar to the following appears.
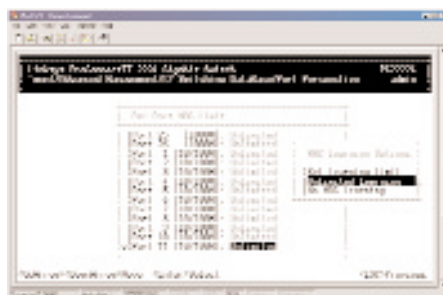
2. Highlight the desired option, and then press the Enter key.

3. If you selected Set Learning Limit, the Enter New Limit screen appears.
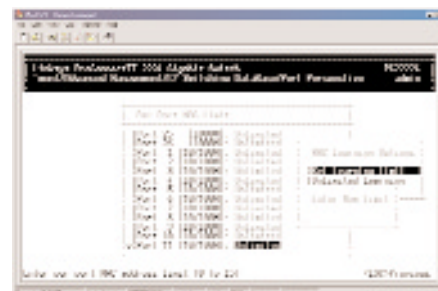
4. Type the new limit, and press the Enter key.

IP Networking

If you select *IP Networking* from the *Advanced Management* screen, the *IP Networking* screen will appear.

From the *IP Networking* screen, you can:

*   View or change *IP and RIP Settings*.

*   View or change *ARP Table* Parameters.

*   View or change *Routing Table* Parameters.

*   View or change *DHCP Gateway Settings*.

*   View or change *Ping* Settings.

IP & RIP SETTINGS

If you select *IP & RIP Settings* from the *IP Networking* screen, an *IP Settings* screen similar to the following will appear, along with a list of the VLAN IDs, IP addresses, subnet masks, and frame types currently defined.

Use the following procedure to modify the settings shown:

1. Use the **Down Arrow** key to highlight the row that contains the parameters you want to change, then press **Enter**. A screen similar to the following will appear, with the the *IP Address* field highlighted.
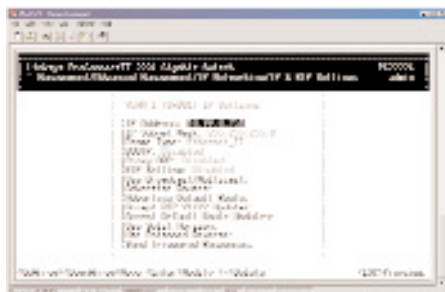
2. Review the settings. To change a setting, highlight it, press the **Enter** key, select the desired setting, and press **Esc**.

3. To delete a setting, highlight the setting and press the "**-**" (hyphen) key. When a message asks you to confirm the deletion, highlight *Yes* and press **Enter** to delete it. Press **Esc** or highlight *No* and press **Enter** to retain it. Note that by deleting the IP Address, any Telnet or Web connection will be disconnected.

4. When you finish, press the **Esc** key until you return to the desired screen.

ARP TABLE SETTINGS

If you select *ARP Table* from the *IP Networking* screen, an *ARP Table* screen similar to the following will appear with the ARP table entries that have already been defined or learned.
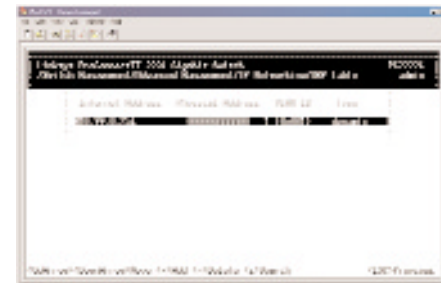
From this screen, you are able to:

• Add static entries to the ARP table.

• Delete static entries to the ARP table.

• Search for entries in the ARP table.

Adding Static ARP Table Entries

Use the following procedure to add static entries to the ARP table:

1. From the *ARP Table* screen, hold down the **Shift** key and press the "+" key. The *Static ARP Specifications* screen will appear, with the *Internet Address* field highlighted.

2. Press the **Enter** key. The *Enter Internet Address* screen (see next page) will appear.

Deleting Static ARP Table Entries

If you no longer need a static entry in the ARP table, use the following procedure to delete it. Since there is no precautionary message that appears before you delete a static ARP table entry, be sure you want to delete the entry before you begin.

1. From the *ARP Table* screen, use the **Up Arrow** or **Down Arrow** key to highlight the ARP table entry you want to delete.

2. Press the "**-**" (hyphen) key to delete the entry.

3. To delete additional static ARP table entries, repeat steps 1 and 2.

4. When you finish, press **Esc** to return to the *ARP Table* screen.

Searching for ARP Table Entries

Use the following procedure to search for ARP table entries:

1. From the *ARP Table* screen, press the "**S**" key. The *Search Options* screen will prompt you to select an *Internet Address* or a *Physical Address*.

2. Highlight either *Internet Address* or *Physical Address* and press the **Enter** key. You are prompted for an IP or physical address.

3. Enter the IP or physical address you are searching and press **Enter**. The selected address will be highlighted.

4. When you finish viewing the information, press the **Esc** key until you return to the desired screen.

3. Type an Internet address. The address consists of numbers separated by periods (e.g., 129.32.0.11). When you finish, press **Enter**. The Internet address you typed will appear next to *Internet Address* in the *Static ARP Specifications* screen.

4. Press the **Down Arrow** key to highlight *Physical Address* and press **Enter**. The *Enter Physical Address* screen will appear.

5. Type the corresponding physical address and press **Enter**. The physical address you typed will appear next to *Physical Address* in the *Static ARP Specifications* screen.

6. Press **Esc**. The Internet and physical addresses you typed will appear in the *ARP Table* screen. The following screen shows an example of Internet and physical addresses that have been added.

7. To add more static ARP table entries, repeat steps 1 through 6. When you are finished, press **Esc** to return to the *ARP Table* screen.

50

51

ROUTING TABLE

If you select *Routing Table* from the *IP Networking* screen, a *Routing Table* screen similar to the following will appear.
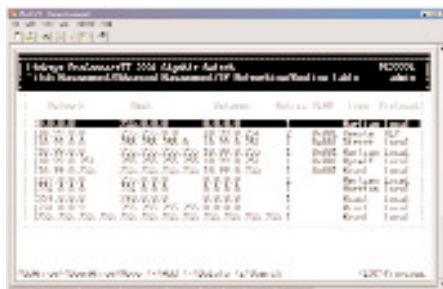
The Routing Table allows you to view, add, delete, or search a particular routing path. Information is displayed in the following columns:

Network	The IP Subnetwork address to which the switch can route packets.
Mask:	The related IP Subnetwork Mask to which the switch can route packets.
Gateway	The IP address of the router at the next hop.
Metric	The number of hops needed between the switch and the destination network.
VLAN	The VLAN within which the gateway or destination resides.
Type	The IP route type for the IP subnetwork. There are six IP route types:

Direct	A directly connected subnetwork.
Remote	A remote IP subnetwork or host address.
Myself	A switch IP address on a specific IP subnetwork.
Bcast	A subnetwork broadcast address.
Mcast	An IP multicast address.
Martian	An illegal IP address to be filtered.

Protocol	Indicates one of the following:

Local	A manually configured routing entry.
NetMgmt	A routing entry set via SNMP.
ICMP	A routing entry obtained via ICMP redirect.
RIP	A routing entry learned via the RIP protocol.
Other	A protocol other than one of the other four listed above.

From the *Routing Table* screen, you are able to:

• Add entries to the Routing table.

• Delete entries from the Routing table.

• Search for entries in the Routing table.

Adding Routing Table Entries

Use the following procedure to add entries to the Routing table:

1. From the *Routing Table* screen, hold down the **Shift** key and press the "+" key. The *Route Options* screen will appear.

2. Select *Default Gateway* or *Static Route*, then press **Enter**.

If you select *Default Gateway*, the following screen (see next page) will appear. Press **Enter** and type an IP address for the default gateway. The address consists of numbers separated by periods (e.g., 129.32.0.11). When you finish, press **Enter**. Proceed to step 3.
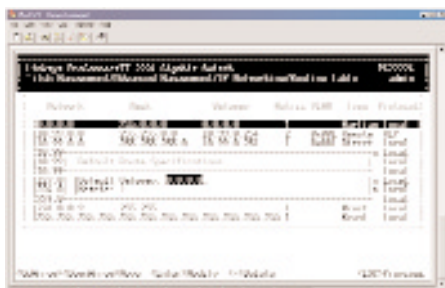
If you select *Static Route*, the following screen will appear. At each field, press **Enter**, type the appropriate parameter, and press **Enter** again. Use the **Up Arrow** and **Down Arrow** keys to move between fields. Proceed to step 3.
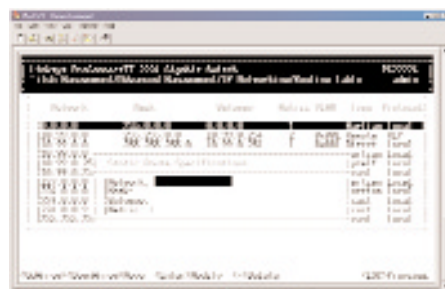
3. After entering default gateway or static route parameters, press **Esc**. The parameters you entered will appear in the *Routing Table* screen.

Deleting Routing Table Entries

If you no longer need an entry in the Routing Table, use the following procedure to delete it. Since there is no precautionary message that appears before you delete a Routing Table entry, be sure you want to delete the entry before you begin.

1. From the *Routing Table* screen, use the **Up Arrow** or **Down Arrow** key to highlight the Routing table entry you want to delete.

2. Press the "**-**" (hyphen) key to delete the entry.

3. To delete additional Routing Table entries, repeat steps 1 and 2. When you finish, press **Esc** to return to the *Routing Table* screen.

Searching for Routing Table Entries

Use the following procedure to search for entries in the Routing Table:

1. From the *Routing Table* screen, press the "**S**" key. The *Enter Network Address* screen will appear.

2. Type the network address you want to search for, then press **Enter**.

DHCP GATEWAY SETTINGS

If you highlight *DHCP Gateway Settings* from the *IP Networking* screen and press the **Enter** key, a *DHCP Gateway Settings* screen similar to the following will appear.

In this screen, the following details are displayed:

VLAN ID shows the IDs of the VLANs that have been defined.

IP Address shows the corresponding IP addresses of the VLANs.

DHCP Relay shows whether the DHCP relay is enabled or disabled.

Max. Hops shows the maximum number of hops that a DHCP request broadcast can be relayed along the DHCP relay path from the DHCP client to the DHCP server.

Delay   shows the number of seconds that must elapse before a DHCP request broadcast is relayed to the next IP subnetwork.

Servers   shows any preferred servers that have been defined.

Relays   shows the outbound IP subnetwork for relaying a DHCP request broadcast.

The following procedure describes how to change the DHCP gateway settings. As part of this procedure, you can specify up to three preferred servers and/or an outbound relay interface.

1. Highlight the appropriate *VLAN ID* and press **Enter**. A screen similar to the following will appear.

2. To add a relay IP, hold down the **Shift** key and press the "+" key. A screen similar to the following will appear.

3. Highlight the appropriate interface, or highlight *All Interfaces*, then press **Esc**. A screen similar to the following (see next page) will appear.

4. With the highlight on *DHCP Gateway*, press **Enter**. The following screen will appear.

5. Highlight *Enabled* and press **Enter** to enable the DHCP gateway.

6. Press the **Down Arrow** key and press **Enter** to configure the maximum-number of hops. When the following screen appears, type the desired number and press **Enter**.

7. Press the **Down Arrow** key and press **Enter** to configure the delay. When the following screen (see next page) appears, type the delay, in seconds, and press **Enter**.

8. Press the **Down Arrow** key and press **Enter** to specify the preferred server. When the following screen appears, type the delay, in seconds, and press **Enter**.

9. To specify up to three more preferred servers, do so in the remaining *Preferred Field* options.

10. When you finish, press **Esc**. The *DHCP Gateway Settings* screen will appear, along with the parameters you specified.

11. To define additional DHCP gateways, repeat steps 1 through 10.

12. When you finish defining DHCP gateways, press **Esc** until you return to the desired screen.

PING SETTINGS

If you select *Ping* from the *IP Networking* screen, a *Ping* screen similar to the following will appear, with the *Host* field highlighted.

Use the following procedure to change the ping settings:

1. Press **Enter**. The *Enter IP Address* screen will appear.

2. Type the IP address of the computer you want to ping.

3. Press **Enter**.

4. Use the **Down Arrow** key to move to *Count* and press **Enter**. The *Enter Packet Count* screen will appear.

58   59

5. Type a packet count number from 1 to 999, or type 0 for an infinite packet count. Press **Enter**.

6. Move to *Size <mbytes>* and press **Enter**. The *Enter Packet Size* screen will appear.

7. Type the packet size, from 0 to 1500, then press **Enter**.

8. Move to *Timeout <sec>* and press **Enter**. The *Enter Timeout* screen will appear.

9. Type a timeout value, from 0 to 999, and press **Enter**.

10. When you finish specifying the ping parameters, press **Esc** to start pinging a remote IP address.

11. Press **Esc** again to return to the *IP Networking* screen.

BRIDGING

If you select *Bridging* from the *Advanced Management* screen, the following *Bridging Parameters* screen will appear.
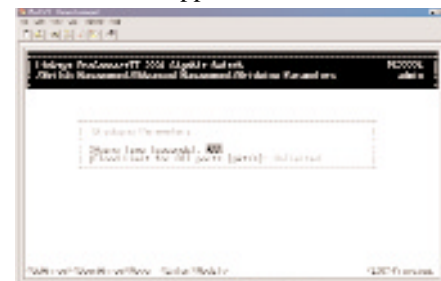
1. To change the aging time, highlight *Aging Time <seconds>* and press **Enter**. The following prompt will ask you to enter a bridge aging period, in seconds. Enter a new aging period and press the **Enter** key.
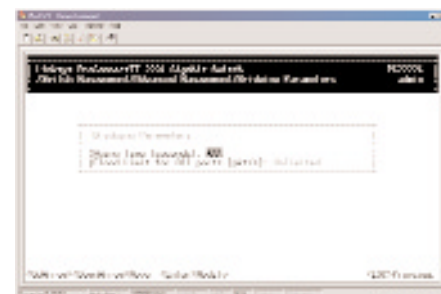
2. To change the flood limit for all ports, highlight *Flood Limit for All ports <pkt/s>*, the following prompt will ask you to enter the flood limit, in packets per second. Enter a a new flood limit and press the **Enter** key. Enter 0 for no limit.
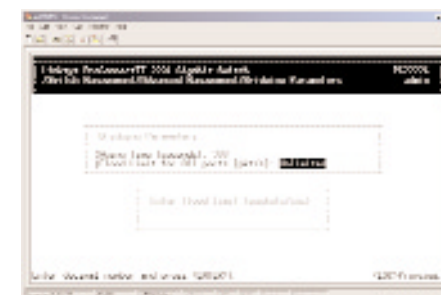
3. Press the **Esc** key until you return to the desired screen.

STATIC FILTERING

If you select *Static Filtering* from the *Advanced Management* screen, the following *Static Filtering* screen will appear, with *Source MAC Address* highlighted.

From the *Static Filtering* screen, you can select *Source MAC Addresses Destination MAC Addresses* and *MAC Address In-Filters* for static filtering by highlighting one of these options and pressing the **Enter** key.

If you select *Source MAC Address* and press **Enter**, the *SRC MAC Out-Filter* screen will appear.

If you select *Destination MAC Address* and press **Enter**, the *DST MAC Out-Filter* screen will appear.

If you select *MAC Address In-Filters*, the *MAC Address In-Filters* screen will appear.

From each of these screens, you are able to:

• Hold down the **Shift** key and press the "+" key to add a specific MAC address to be filtered.

• Press the "**-**" (hyphen) key to delete a specific MAC address from being filtered. Since there is no precautionary message that appears before you delete a specific MAC address, be sure you want to delete the address before you begin.

• Press "**S**" to search through the list of MAC addresses in the static filtering database. The static filtering database maximum capacity is 64.

When you finish, press the **Esc** key until you return to the desired screen.

SPANNING TREE FUNCTIONS

If you select *Spanning Tree* from the *Advanced Management* screen, the *Spanning Tree Protocol* screen will appear.
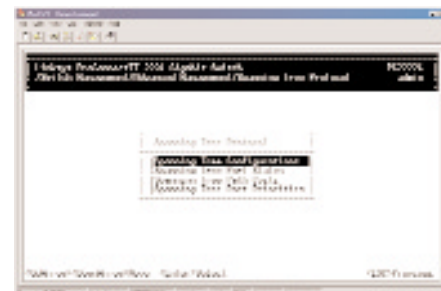
Spanning Tree Protocol Configurations

Highlight *Spanning Tree Configurations* in the *Spanning Tree Protocol* screen and press the **Enter** key. A *Spanning Tree Protocol Configuration* screen similar to the following will appear. The top half of this screen displays read-only values. The bottom half, starting with *Spanning Tree Protocol*, is user configurable. Use the **Up Arrow** and **Down Arrow** keys to highlight a field, then press **Enter** to change the value. When you finish, press the **Esc** key until you return to the desired screen.

Use the following procedure to modify the selections shown:

1. With the *Spanning Tree Protocol* field highlighted, press **Enter**. The following choices will appear (see next page).

2. Select either *Disabled* or *Enabled* and press **Enter**. Your selection will appears next to *Spanning Tree Protocol*.

3. Use the **Down Arrow** key to move to *Bridge Priority* and press **Enter**. The *Enter Bridge Priority* screen will appear.

4. Type a decimal number for the bridge priority and press **Enter**. The decimal value you typed will appear next to *Bridge Priority*.

5. Use the **Down Arrow** key to move to *Hello Time <sec>* and press **Enter**. The *Enter Hello Time* screen will appear.
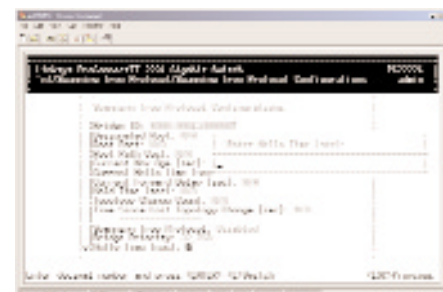
6. Type a decimal number for the hello time and press **Enter**. The decimal value you typed will appear next to *Hello Time*.

7. Press the **Esc** key to return to the *Spanning Tree Protocol* screen.

Spanning Tree Port States

Highlight *Spanning Tree Port States* in the *Spanning Tree Protocol* screen and press the Enter key. A *Spanning Tree Port States* screen similar to the following will appear. This screen displays read-only values. When you finish, press the **Esc** key until you return to the desired screen.

64

65

Use the following procedure to change the administration status:

1. Use the **Up Arrow** and **Down Arrow** keys to highlight the desired port.

2. Press the **Enter** key. The *Admin Status Options* screen will appear.

- To manually enable the selected port, highlight *Up* and press **Esc**.

- To manually disable the selected port, highlight *Down* and press **Esc** (to re-enable the port, repeat steps 1 through 3 and select *Up* in step 3).

3. Enable or disable the selected port (your selection will appear next to the selected port).

4. To change the administration status options for other ports, repeat steps 1 through 3.

5. When you finish, press **Esc**.

Spanning Tree Path Costs

Highlight *Spanning Tree Path Costs* in the *Spanning Tree Protocol* screen and press the **Enter** key. A *Spanning Tree Path Costs* screen similar to the following will appear.

Use the following procedure to change the costs in the *Spanning Tree Path Costs* screen:
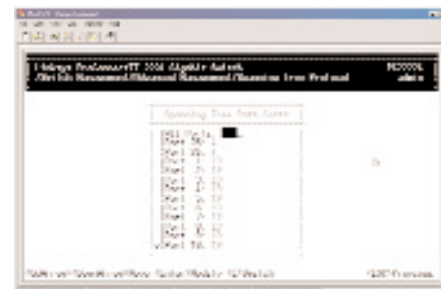
1. Use the **Up Arrow** and **Down Arrow** keys to highlight a specific port or highlight *All Ports*.

2. Press the **Enter** key. The *Enter Path Cost* screen will appear.

3. Enter a new path cost, then press **Enter**. The new Spanning Tree path cost appears next to the selected port.

4. Repeat steps 1 through 3 to change the Spanning Tree path costs for other ports.

5. When you finish, press the **Esc** key until you return to the desired screen.

Spanning Tree Port Priorities

Highlight *Spanning Tree Port Priorities* in the *Spanning Tree Protocol* screen and press the **Enter** key, a *Spanning Tree Port Priorities* screen similar to the following will appear.
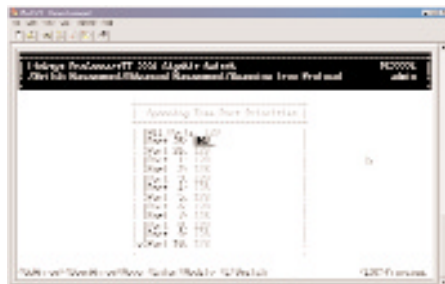
Use the following procedure to modify the settings in the *Spanning Tree Port Priorities* screen:

1. Use the **Up Arrow** and **Down Arrow** keys to highlight the a specific port or highlight *All Ports*.

2. Press **Enter**. The *Enter Port Priority* screen will appear.

3. Type a port priority, from 0 to 255, and press **Enter**. A low value gives the port a greater likelihood of becoming a Root port.

4. To change the priorities of other ports, repeat steps 1 through 3.

5. When you finish, press the **Esc** key until you return to the desired screen.

SNMP FUNCTIONS

If you select *SNMP* from the *Advanced Management* screen, the following *SNMP Configurations* screen will appear, with the SNMP value highlighted.

The *SNMP Configurations* screen lets you view all SNMP-related information. As this screen shows, the factory default SNMP value is *Enabled* and the factory default *Community Name* value is *public*.

Use the following procedure to change a value:

1. With the *SNMP* field highlighted, press the **Enter** key. The following SNMP options will appear.

2. Select *Disabled* or *Enabled* and press **Enter**. Your selection will appear next to *SNMP*.

3. Use the **Down Arrow** key to move to *Get Community Name* and press **Enter**. The *Enter Get Community Name* screen will appear.

4. Type a get community name and press **Enter**. The get community name you typed will appear next to *Get Community Name*.

5. Use the **Down Arrow** key to move to *Set Community Name* and press **Enter**. The *Enter Set Community Name* screen will appear.

6. Type a set community name and press **Enter**. The set community name you typed will appear next to *Set Community Name*.

7. Use the **Down Arrow** key to move to *Trap Community Name* and press **Enter**. The *Enter Trap Community Name* screen will appear.

8. Type a trap community name and press **Enter**. The set community name you typed will appear next to *Trap Community Name*.

9. To specify up to three additional trap community names, repeat steps 7 and 8.

10. To specify a trap host IP address, use the **Down Arrow** key to move to *Trap Host 1 IP Address* and press **Enter**. The *Enter Trap Host 1 IP Address* screen will appear (see next page).

11. Type an IP address for trap host 1. The address consists of numbers separated by periods (e.g., 129.32.0.11).

12. Press **Enter**. The IP address you typed will appear next to *Trap Host 1 IP Address*.

13. To specify up to two additional trap community names, repeat steps 10 through 12.

14. To change the cold start trap setting, press the **Down Arrow** key to move to *Cold Start Trap* and press **Enter**. The Trap Options screen will appear.

15. Select *Disabled* or *Enabled* and press **Enter**. Your selection will appear next to *Cold Start Trap*.

16. Press the **Down Arrow** key to move to *Warm Start Trap* and press the **Enter** key. *The Trap Options* screen will appear.
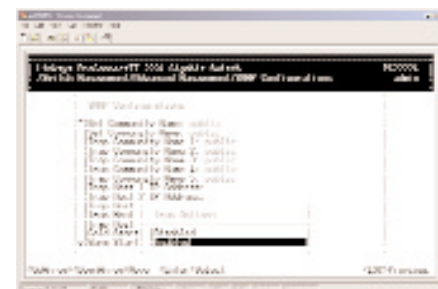
17. Select *Disabled* or *Enabled* and press **Enter**. Your selection will appear next to *Warm Start Trap*.

18. Press the **Down Arrow** key to move to *Link Down Trap* and press the **Enter** key. The *Trap Options* screen will appear.

19. Select *Disabled* or *Enabled* and press **Enter**. Your selection will appear next to *Link Down Trap*.

20. When you finish, press the **Esc** key until you return to the desired screen.

STACKING

Select Stacking from the Advanced Management screen to configure the stacking function. You will receive a Stacking screen as shown in the following.
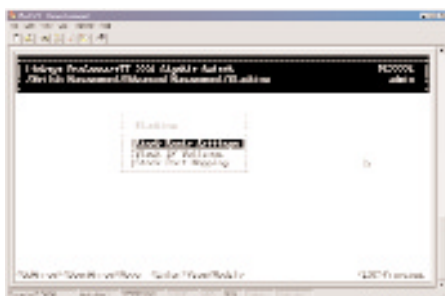
Stacking Basic Setting enables you to set stack ID, stack size, and stack port. Stack IP Settings lets you to set the IP address of the stacked switches. Stack Port Mapping shows information about all ports.

Stacking Basic Setting

Select Stack Basic Settings from the Stacking screen and press the Enter key. The following screen will appear.

• Current Stack Size shows the number of stacked switches. Master Switch ID shows the number of the master switch. The Master Switch must have the lowest switch ID.

• The value of Stack ID, Stack Size, and Switch ID is:
  • 1. Stack ID: 0~65535
  • 2. Stack Size: 2~8
  • 3. Switch ID: 0~65535

1. Before you start to change the stacking parameters, the stacking status must be disabled at first.

2. Highlight the value of Stack ID. Press the Enter key and the column of Enter Stack ID will appear. Set the ID you want. Then press the Enter key.

72

73

3. Use the down arrow key to move to the column of Stack Size. Press the Enter key and the Enter Stack Size column will appear. Type in the value you want to change. Then press the Enter key.

4. Use the down arrow key to move to the column of Switch ID. Press the Enter key and the Enter Switch ID screen will appear. Type in the value you want to change. Then press the Enter key.

5. Use the down arrow key to move to the column of Stack Port. Press the Enter key and the Select Stack Ports screen will appear. Select the port you want to connect to other switches as a stack port. Then press the Enter key. An asterisk mark will appear to the port you select.

Press the ESC key. The selected port will appear in the Stack Port field.

6. Use Up or Down arrow key to highlight the Stacking field. Press the Enter key and the Stack Options will appear. Highlight Enabled and press the Enter key.

7. Repeat step 1~5 to configure other switches to be stacked. Note that the Stack ID should be the same. The Switch IDs should be set different.

8. After enabling the stacking, the current Stack Size and Master Switch ID will be shown as below. The function of stacking is completed.

After stacking is set up, configuration must be executed in the master switch.

OTHER PROTOCOLS

Highlight *Other Protocols* from the *Advanced Management* screen and press the **Enter** key. The *Other Protocol Settings* screen will appear, with the *GVRP* value highlighted.
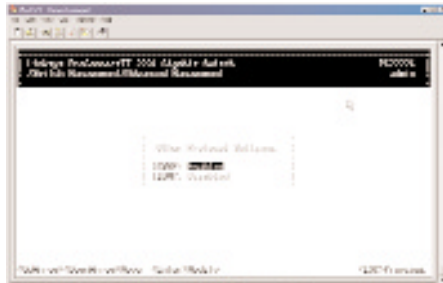
1. To change the GVRP setting, press **Enter** with *GVRP* highlighted. When the following screen appears, highlight the desired setting and press **Enter**.

2. To change the IGMP setting, highlight *IGMP* and press **Enter**. When the following screen appears, highlight the desired setting and press **Enter**.

3. When you finish, press the **Esc** key until you return to the desired screen.

PORT TRUNKING

Using *Port Trunking* from the *Advanced Management* screen, you can associate ports with trunk groups.

1. From the *Advanced Management* screen, highlight *Port Trunking* and press the **Enter** key. The following screen will appear.
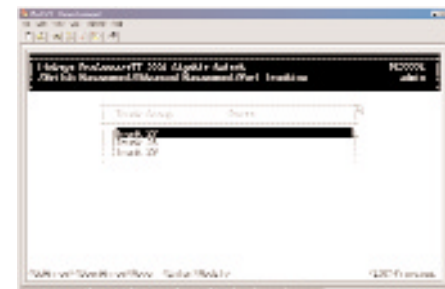
2. Highlight the trunk group to which you want the ports assigned, then press **Enter**. A screen similar to the following (see next page) will appear.
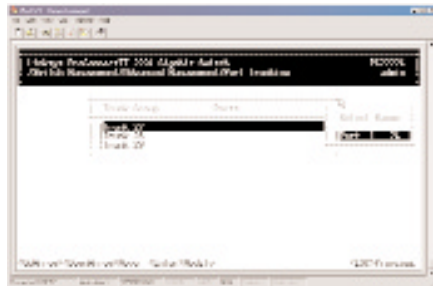
3. Highlight the range of ports you want to associate with the trunk group, then press **Enter**. The port range appears next to the selected trunk group, as in the following screen.
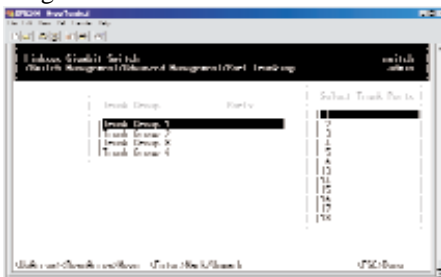
4. For each trunk port you want to select, highlight it and press **Enter**. An asterisk will appear next to the selected port as in the following screen (if you change your mind, highlight the port and press **Enter** again to deselect it and remove the asterisk.)
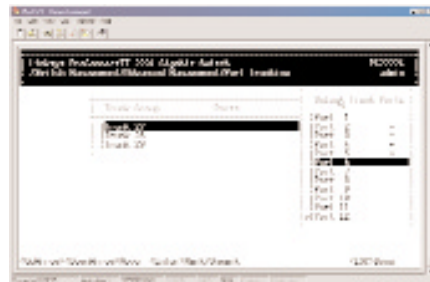
5. When you finish selecting ports, press **Esc**. A screen similar to the following (see next page) will appear, showing the ports associated with the trunk group.
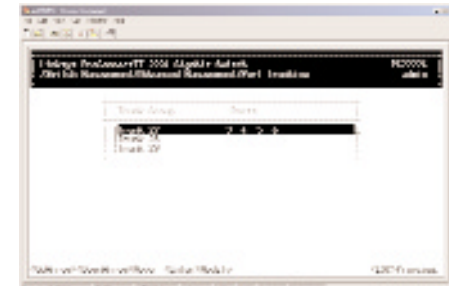
6. To associate additional ports with trunk groups, repeat steps 2 through 5.

7. When you finish, press the **Esc** key until you return to the desired screen.

SETTING QUALITY OF SERVICE PARAMETERS

Using QoS Setup from the Advanced Management screen, you can configure the switch to use various Quality of Service (QoS) parameters.

1. From the Advanced Management screen, highlight QoS Setup and press the Enter key. The QoS menu appears.

2. Refer to the appropriate section for information about setting the QoS parameters in the QoS menu.

- For global settings, refer to "Setting Global Settings".
- For TCP/UDP logical port parameters, refer to "Specifying TCP/UDP Logical Port Settings".
- For QoS parameters, refer to "Specifying the ToS Priority".
- For QoS scheduling algorithm parameters, refer to "Selecting a QoS Profile".
- For port configuration parameters, refer to "Specifying the Port Configuration".
- For rate control parameters, refer to "Rate Control".

Setting Global Settings
To set global settings:

1. From the QoS menu, highlight Global Settings and press the Enter key. The Global Setting menu appears.

2. Press the Enter key. The QoS menu appears.

3. Highlight whether you want QoS status to be enabled or disabled, then press the Enter key. Your selection appears next to QoS Status.

4. With the highlight on Diffserv Expedite Forwarding, press the Enter key. The Diffserv Expedite Forwarding screen appears.

5. Highlight whether you want to enable or disable DiffServ Expedite Forwarding, and then press the Enter key. Your selection appears next to DiffServ Expedite.

6. Press the Down Arrow key to highlight Tos/VLAN Tag.

7. Press the Enter key. The ToS/VLAN Priority Tag menu appears.

8. Highlight the desired setting, then press the Enter key. The setting you select appears next to ToS/VLAN Tag.

9. Press the Down Arrow key to highlight QoS Status.

10. Press the Down Arrow key to highlight WRED Drop Priority Setting. The WRED Drop Priority screen appears.

80

81

11. To change the low-drop percentage, press the Enter key with Low Drop Percentage highlighted. The following screen appears.

13. Highlight the appropriate percentage and press the Enter key.

14. Press the Esc key to return to the WRED Drop Priority screen.

15. To change the high-drop percentage, press the Down Arrow key to high-light High Drop Percentage, then press the Enter key. The following screen appears.

12. Levels 1 and 3 remain fixed at 0% and 100%, respectively, to change the percentage for level 2, highlight Level 2 and press the Enter key. The fol-lowing options appear.

Note
Level 1 is 75% of congestion traffic, Level 2 is 87.5% of congestion traffic, and Level 3 is 100% of congestion traffic.

16. Level 3 remains fixed at 100%. To change the percentage for level 1 or 2, highlight Level 1 or Level 2 and press the Enter key. The following options appear.

Note
Level 1 is 75% of congestion traffic, Level 2 is 87.5% of congestion traffic, and Level 3 is 100% of congestion traffic.

17. Highlight the appropriate percentage and press the Enter key.

18. Press the Esc key to return to the WRED Drop Priority screen.

19. Press the Esc key to return to the QoS screen.

20. Press Esc until you return to the desired screen.

Specifying TCP/UDP Logical Port Settings

To set logical port settings, highlight Logical Port from the QoS menu, and then press the Enter key. The Logical Port menu appears.

The Logical Port menu lets you set parameters for a user-defined port, a well-known port, and a port range.
- To set parameters for a user-defined port, refer to "User-Defined Port".
- To set parameters for a well-known port, refer to "Well-Known Port".
- To set a port range, refer to "Range Port".

User-Defined Port
With the highlight on User Define Port in the Logic Port screen, press the Enter key. The User-Define Port Index screen appears.
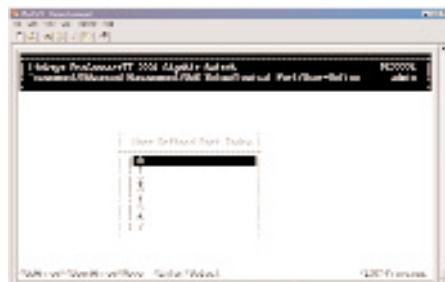
1. Use the Down Arrow key to highlight the appropriate port, and then press the Enter key. The User-Define menu appears for the port you selected.

2. With the highlight on Port Number, press the Enter key. The port Number screen appears under the User Defined port 2 screen.

3. Type a port number, in decimal notation, and press the Enter key. The port number you typed appears next to Port Number.

4. Press the Down Arrow key to highlight Drop Priority, and then press the Enter key. The Drop Priority menu appears.

5. Highlight whether the drop priority should be low or high, and then press the Enter key. Your selection appears next to Drop Priority.

6. Press the Down Arrow key to highlight Transmit Priority, and then press the Enter key. The Transmit Priority menu appears.

7. Highlight the desired transmit priority, then press the Enter key. The transmit priority you selected appears next to Transmit Priority.

8. Use the Down Arrow key to highlight Port Status, and then press the Enter key. The Port Status menu appears.
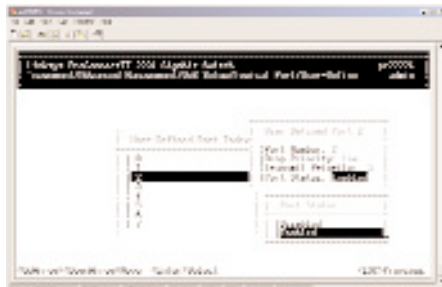
9. Highlight whether the port status should be enabled or disabled, then press the Enter key. Your selection appears next to Port Status.

10. Press the Esc key to return to the User-Define Port Index Screen.

11. To define parameters for another port, repeat steps 3 through 12.

12. When you finish defining parameters, press Esc until you return to the desired screen.

Well-Known Port

To set well-known port settings:

1. From the Logical Port menu, highlight Well-Known Port and press the Enter key. The Well-Known Port Index menu appears.
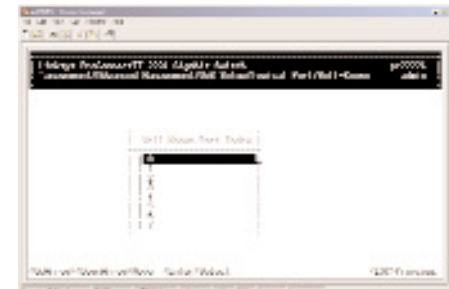
2. The Well-Known Port Index screen works the same way the User-Define Port Index Screen works, except that the well-known port number is pre-configured and cannot be changed. For more information, refer to "User-Defined Port".

Range Port

To select a port range:

1. From the Logic Port menu, press the Down Arrow key to highlight Range Port, and then press the Enter key. The Range Logic Port screen appears.

2. To change the low port number, press the Enter key with the highlight on Low Port Number. When the Low Port Number screen appears, type the low port number, in decimal notation, and press the Enter key. The low port number you typed appears next to Low Port Number.
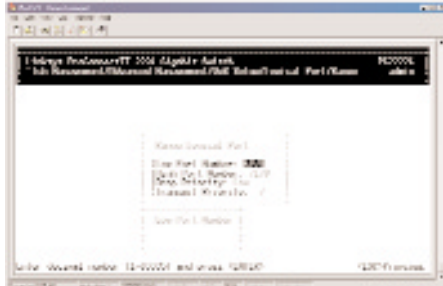
3. To change the high port number, press the Down Arrow key to highlight Down Port Number, then press the Enter key. When the High Port Number screen appears, type the high port number, in decimal notation, and press the Enter key. The high port number you typed appears next to High Port Number.

4. To change the drop priority setting, press the Down Arrow key to highlight Drop Priority, then press the Enter key. When the Drop Priority screen appears, highlight Low or High and press the Enter key. Your selection appears next to Drop Priority.

5. To change the transmit priority setting, press the Down Arrow key to highlight Transmit Priority, then press the Enter key. When the Transmit Priority screen appears, highlight the desired priority and press the Enter key. Your selection appears next to Transmit Priority.

6. Press the Esc key until you return to the desired screen.

Specifying the QoS VLAN Priority

To specify the QoS VLAN priority:

1. From the QoS screen, press the Down Arrow key to highlight VLAN, then press the Enter key. The VLAN Priority Index screen appears.

2. Press the Down Arrow key to highlight a VLAN priority number, and then press the Enter key. The VLAN Priority Setting screen appears.

3. With Drop Priority highlighted, press the Enter key. The Drop Priority screen appears.

4. Highlight either Low or High, and then press the Enter key. Your selection appears next to Drop Priority.

5. Press the Down Arrow key to highlight Transmit Priority, and then press the Enter key. The Transmit Priority screen appears.

6. Highlight the desired transmit priority, then press the Enter key. The transmit priority you selected appears next to Transmit Priority.

7. Press the Esc key to return to the VLAN Priority Index screen.

8. To specify other VLAN priority settings, repeat steps 2 through 7.

9. When you finish, press the Esc key until the appropriate screen appears.

Specifying the ToS Priority

To specify ToS priority:

1. From the QoS screen, press the Down Arrow key to highlight ToS, then press the Enter key. The ToS Priority Index screen appears.

2. Press the Down Arrow key to highlight a ToS priority number.

Note:
The ToS priority number is determined by bit [4:2] of the ToS field in the IP header.

3. Press the Enter key. The ToS Priority Setting screen appears. This screen is similar to the VLAN Priority Setting screen.

4. Perform steps 3 through 9 under "Specifying the QoS VLAN Priority".

Selecting a QoS Profile

To select a QoS profile:

1. From the QoS screen, use the Down Arrow key to highlight Profile, and then press the Enter key. The QoS Profile screen appears.

2. Perform one of the following steps:

• To specify a megabit profile that is used by a 10/100 Megabit port, refer to "Megabit Profile".
• To specify a gigabit profile that is used by a Gigabit port, refer to "Gigabit Profiles".

Megabit Profile

To select a megabit profile:

1. With Megabit Profile highlighted in the QoS Profile screen, press the Enter key. The Megabit Profile screen appears.
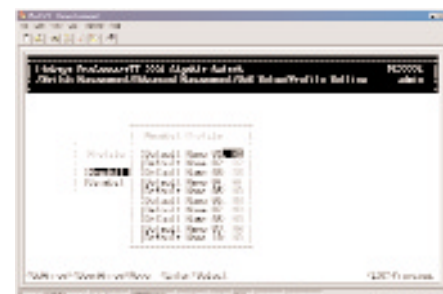
2. Use the Down Arrow key to highlight a profile, then press the Enter key. The Megabit Profile Attributes screen appears.

Note
In the Megabit Profile screen:
A1 = active profile #1, which can be used by any 10/100 Megabit port.
A2 = active profile #2, which can be used by any 10/100 Megabit port.
A3 = active profile #3, which can be used by any 10/100 Megabit port.
A4 = active profile #4, which can be used by any 10/100 Megabit port.
NA = indicates a profile that is not active and cannot be used by any 10/100 Megabit port.

3. To change the profile name, press the Enter key with Profile Name. When Profile Name box appears, enter a profile name and press the Enter key. The name you entered appears next to Profile Name.

4. Ports Using This Profile displays all the ports that are currently using this profile for their QoS scheduling algorithm.

5. To change the bandwidth partition for this profile, use the Down Arrow key to highlight Bandwidth Partitions and press the Enter key. When the BW Partitions screen appears, use the Down Arrow key to highlight a partition and press the Enter key. The bandwidth you entered appears next to Bandwidth Partitions.

Note:
Bandwidth Partition is more accurate for profiles when Delay Sensitive Application is disabled. For profiles that have Delay Sensitive Application enabled, Bandwidth Partition is provided for reference purposes only, because the packet is dispatched based on the delay-bound algorithm.

Note
Ports Using This Profile, Strict Priority, Delay Sensitive Application, and Profile Status are all read-only parameters that cannot be changed.

6. To change the setting for QoS flow control setting, press the Down Arrow key to select QoS with Flow Control and press the Enter key. When the QoS Flow Control screen appears, highlight Disabled or Enabled and press the Enter key. Your selection appears next to QoS with Flow Control.

7. Press the Esc key until you return to the desired screen.

Gigabit Profiles

To select a gigabit profile:

1. Use the Down Arrow key to highlight Gigabit Profile in the QoS Profile screen, then press the Enter key. The Gigabit Profile screen appears.

2. Use the Down Arrow key to highlight a profile, and then press the Enter key. The Gigabit Profile Attributes screen appears.

Note
In the Gigabit Profile screen:
A1 = active profile #1, which can be used by any 10/100/1000 Gigabit port.
A2 = active profile #2, which can be used by any 10/100/1000 Gigabit port.
NA = indicates a profile that is not active and cannot be used by any 10/100/1000 Gigabit port.

3. This screen is similar to the Megabit Profile Attributes screen. To complete this screen, perform steps under 3 through 8 under "Megabit Profile".

Specifying the Port Configuration

To specify port configuration parameters:

1. From the QoS screen, use the Down Arrow key to highlight Port Configuration, and then press the Enter key. The Port Configuration screen appears.

Note
Ports 1 through 24 are 10/100 Megabit ports, while ports 25 and 26 are Gigabit ports.

2. Use the Down Arrow key to highlight a port, and then press the Enter key. A screen similar to the following, with parameters for that port, appears.

3. To change the selected port's active profile, press the Enter key with Active Profile highlighted. When the Active Profile screen appears, use the Up and Down Arrow keys to highlight an active profile and press the Enter key. The active profile number that you selected appears next to Active Profile.
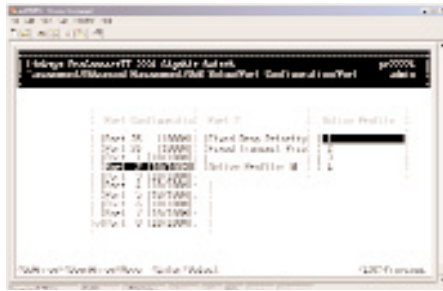
Note

Fixed Drop Priority and Fixed Transmit Priority are read-only parameters that cannot be changed.

4. Press the Esc key until you return to the desired screen.
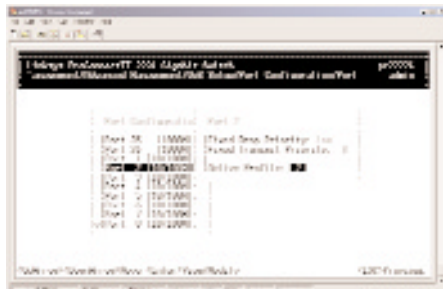
Selecting Rate Control Parameters

To specify rate control parameters:

1. From the QoS screen, use the Down Arrow key to highlight Rate Control, and then press the Enter key. The Rate Control screen appears.

2. Use the Down Arrow key to highlight Rate Control and press the Enter key. The Rate Control Status screen appears.

3. Highlight the desired setting, then press the Enter key. Your selection appears next to Rate Control in the Rate Control screen.

4. To change the port number setting, press the Down Arrow key to highlight Port Number, then press the Enter key. The Port Number screen appears.

5. Highlight the desired port number, then press the Enter key. A screen showing the average rate and traffic type settings for the selected port appears.

6. To change the average rate setting, press the Enter key. The Average Rate screen appears.

7. Highlight the desired rate and press the Enter key. The rate you selected appears next to Average Rate.

8. To change the traffic type, press the Down Arrow key to highlight Traffic Type, then press the Enter key. The Traffic Type screen appears.
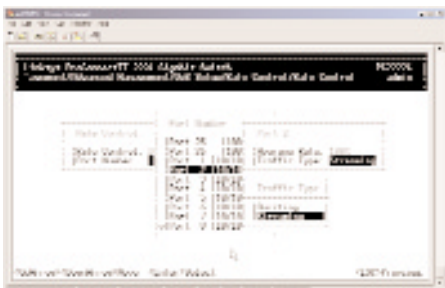
9. Highlight either Bursting or Streaming, then press the Enter key. Your selection appears next to Traffic Type.

10. Press the Esc key until you return to the desired screen.

Sending and Receiving Files

If you select File Transfer from the Advanced Management screen, the following File Transfer screen appears, with the Receive File via TFTP value highlighted. You can use this screen to send and receive files using the TFTP or Kermit protocol.
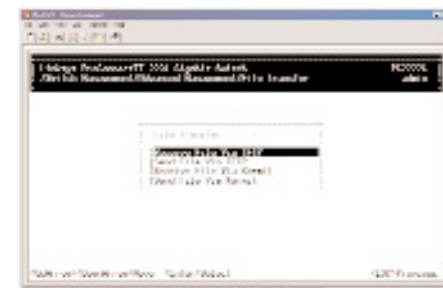
Receiving Files via TFTP

The following procedure describes how to receive files using the TFTP protocol.

Note
The TFTP protocol is used to download upgraded software to the switch. A VLAN with the proper IP address and routing path to the TFTP server must be configured for the switch to access the specified TFTP server.

1. Press the Enter key. The Receive File Via TFTP screen appears.

2. If the name of the file you intend to receive is different than the default one shown, press the Enter key. When the Enter File Name screen appears, type the name of the file you intend to receive and press the Enter key. The name you typed appears next to File Name.

3. Use the Down Arrow key to highlight IP Address, then press the Enter key. When the Enter IP Address screen appears, type the IP address from where the file will be obtained. The address consists of numbers separated by periods. For example: 192.168.1.100

4. Press the Enter key. The IP address appears next to IP Address.

5. When you finish, press the Esc key. A prompt asks whether you want to transfer the file now.

6. Highlight Yes and press the Enter key to transfer the file now, or press the Esc key or highlight No and press the Enter key to not transfer the file at this time.

Sending Files via TFTP

The following procedure describes how to send files using the TFTP protocol.

Note
The TFTP protocol is used to download upgraded software to the switch. A VLAN with the proper IP address and routing path to the TFTP server must be configured for the switch to access the specified TFTP server.

1. On the File Transfer screen, highlight Send File Via TFTP and press the Enter key. The Send File Via TFTP screen appears.
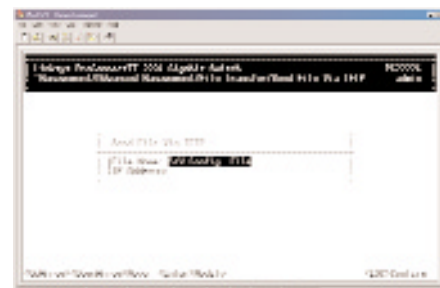
2. If the file type you intend to send is different than the default file one shown, press the Enter key. The Select File Type screen appears.

3. Highlight the file type you want to send and press the Enter key. The file type you selected appears next to File Name.

4. Use the Down Arrow key to highlight IP Address, then press the Enter key. When the Enter IP Address screen appears, type the IP address from where the file will be obtained. The address consists of numbers separated by periods. For example: 192.168.1.100

5. Press the Enter key. The IP address appears next to IP Address.

6. When you finish, press the Esc key. A prompt asks whether you want to transfer the file now.

7. Highlight Yes and press the Enter key to transfer the file now, or press the Esc key or highlight No and press the Enter key to not transfer the file at this time.

Receiving Files via Kermit

To receive files using the Kermit protocol:

1. From the File Transfer screen, highlight Receive File Via Kermit and press the Enter key. A prompt asks whether you want to transfer the file now.

2. Highlight Yes and press the Enter key to transfer the file now, or press the Esc key or highlight No and press the Enter key to not transfer the file at this time.

Sending Files via Kermit

To send files using the Kermit protocol:

1. From the File Transfer screen, highlight Send File Via Kermit and press the Enter key. The Select File Type screen appears.

2. Highlight the file type you want to send and press the Enter key. A prompt asks whether you want to transfer the file now.

3.   Highlight Yes and press the Enter key to transfer the file now, or press the Esc key or highlight No and press the Enter key to not transfer the file at this time.

SNMP and RMON Management

Overview

This section describes the Switch's Simple Network Management Protocol (SNMP) and Remote Monitoring (RMON) capabilities.

RMON is an abbreviation for the Remote Monitoring MIB (Management Information Base). RMON is a system defined by the Internet Engineering Task Force (IETF) document RFC 1757, which defines how networks can be monitored remotely. RMONs typically consist of two components: an RMON probe and a management workstation:

• The RMON probe is an intelligent device or software agent that continually collects statistics about a LAN segment or VLAN. The RMON probe transfers the collected data to a management workstation on request or when a pre-defined threshold is reached.

• The management workstation collects the statistics that the RMON probe gathers The workstation can reside on the same network as the probe, or it can have an in-band or out-of-band connection to the probe.

The Switch provides RMON capabilities that allow network administrators to set parameters and view statistical counters defined in MIB-II, Bridge MIB, and RMON MIB. RMON activities are performed at a Network Management Station running an SNMP network management application with graphical user interface.

SNMP Agent and MIB-2 (RFC1213)

The SNMP Agent running on the switch manager CPU is responsible for:

• Retrieving MIB counters from various layers of software modules according to the SNMP GET/GET NEXT frame messages.

• Setting MIB variables according to the SNMP SET frame message.

• Generating an SNMP TRAP frame message to the Network Management Station if the threshold of a certain MIB counter is reached or if other trap conditions (see next page) are met:

• Warm start
• Cold start
• Link up
• Link down
• Authentication failure
• Rising alarm
• Falling alarm
• Topology change

MIB-2 defines a set of manageable objects in various layers of the TCP/IP protocol suites. MIB-2 covers all manageable objects from layer 1 to layer 4 and, as a result, is the major SNMP MIB supported by all vendors in the networking industry. The Switch supports a complete implementation of SNMP Agent and MIB-2.

RMON MIB (RFC 1757) and Bridge MIB (RFC 1493)

The Switch provides hardware-based RMON counters in the switch chipset. The switch manager CPU polls these counters periodically to collect the statistics in a format that complies with the RMON MIB definition.

RMON GROUPS SUPPORTED

The Switch supports the following RMON MIB groups defined in RFC1757:

• RMON Statistics Group maintains utilization and error statistics for the switch port being monitored.

• RMON History Group gathers and stores periodic statistical samples from the previous Statistics Group.

• RMON Alarm Group allows a network administrator to define alarm thresholds for any MIB variable. An alarm can be associated with Low Threshold, High Threshold, or both. A trigger can trigger an alarm when the value of a specific MIB variable exceeds a threshold, falls below a threshold, or exceeds or falls below a threshold.

• RMON Event Group allows a network administrator to define actions based on alarms. SNMP Traps are generated when RMON Alarms are triggered. The action taken in the Network Management Station depends on the specific network management application.

BRIDGE GROUPS SUPPORTED

The Switch supports the following four groups of Bridge MIB (RFC1493):

• **The dot1dBase Group** a mandatory group that contains the objects applicable to all types of bridges.

• **The dot1dStp Group** contains the objects that denote the bridge's state, with respect to the Spanning Tree Protocol. If a node does not implement the Spanning Tree Protocol, this group will not be implemented. This group is applicable to any transparent only, source route, or SRT bridge that implements the Spanning Tree Protocol.

• **The dot1dTp Group** contains objects that describe the entity's transparent bridging status. This group is applicable to transparent operation only and SRT bridges.

• **The dot1dStatic Group** contains objects that describe the entity's destination-address filtering status. This group is applicable to any type of bridge which performs destination-address filtering.

Appendix

About Fast Ethernet

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.

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.

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.

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.

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.

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 tetrabits 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 in different with two main connector types. The most commonly used fiber optic cable is multi-mode fiber cable (MMF), with a 62.5 micron fiber optic core. Single-mode fiber cabling is somewhat more efficient than multi-mode but far more expensive, due to its smaller optic core that helps retain the intensity of traveling light signals. A fiber connection always require two fiber cables: one transmits data, and the other receives it.

Each fiber optic cable is tipped with a connector that fits into a fiber port on a network adapter, hub, or switch. In the 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.

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 the next 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.
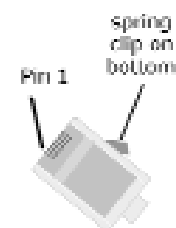
Crimping Your Own Network Cables
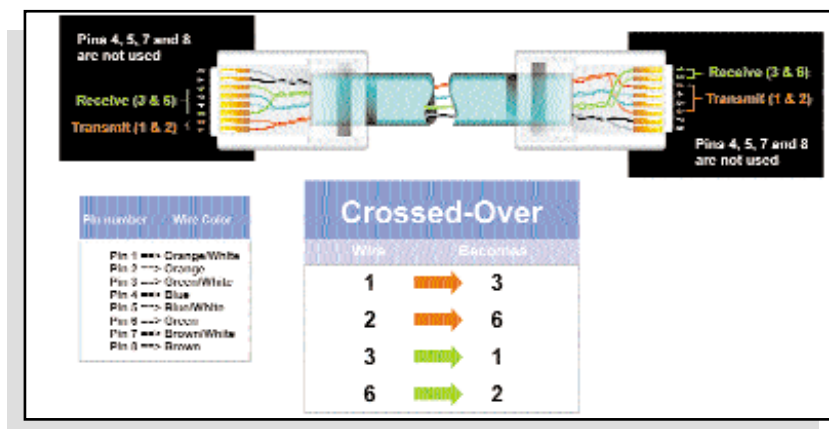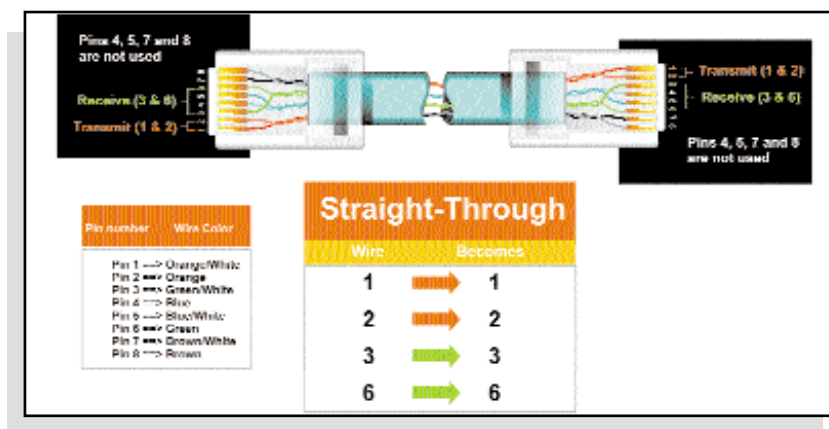
Glossary

10BaseT - An Ethernet standard that uses twisted wire pairs.

100BaseTX - IEEE physical layer specification for 100 Mbps over two pairs of Category 5 UTP or STP wire.

1000BASE-T - provides half-duplex (CSMA/CD) and full-duplex 1000Mb/s Ethernet service over Category 5 links as defined by ANSI/TIA/EIA-568-A. Topology rules for 1000BASE-T are the same as those used for 100BASE-T. Category 5 link lengths are limited to 100 meters by the ANSI/TIA/EIA-568-A cabling standard. Only one CSMA/CD repeater will be allowed in a collision domain.

802.1x - Based on the Extensible Authentication Protocol (EAP), the 802.1x standard is one of the IEEE standards for network authentication and key management. It establishes a framework that supports multiple authentication methods. This standard can be incorporated into any type of network to enhance its security.
For example, a wireless user may use one of the authentication methods to access a wireless network protected by an authentication server. The user, also called the supplicant, sends a request to an access point or wireless router, also called the authenticator. The authenticator sends an identification request back to the user. After the user sends the authenticator the identification message, the authenticator forwards the user's identification message to the authentication server. If the server accepts the identification message, then the user is permitted access to the wireless network. The 802.1x standard can also support encryption key management to strengthen wireless network encryption services.

Adapter - Printed circuit board that plugs into a PC to add to capabilities or connectivity to a PC. In a networked environment, a network interface card (NIC) is the typical adapter that allows the PC or server to connect to the intranet and/or Internet.

Architecture - The total design and implementation of the network. It includes the network's topology, transmission technologies and communications protocols, management and security systems, and any other attributes that give a network a particular set of capabilities and functionalities.

ARP (Address Resolution Protocol) - A TCP/IP protocol used to figure out a host's Ethernet address (MAC address/node ID) from its Internet address.

Automatic Fall-back - A feature provided by some wireless products to increase connection reliability. Automatic fall-back enables a device to dynamically shift between various data transfer rates. It works by decreasing the data transfer rate when interference increases, distance increases, and other factors undermine signal strength and quality.

Auto-MDI/MDIX - On a network hub or switch, an auto-MDI/MDIX port automatically senses if it needs to act as a MDI or MDIX port. The auto-MDI/MDIX capability eliminates the need for crossover cables.

Auto-Sensing - To automatically determine the correct settings. The term is often used with communications and networking. For example, Ethernet 10/100 cards, hubs and switches can determine the highest speed of the node they are connected to and adjust their transmission rate accordingly.

Backbone - The part of a network that connects most of the systems and networks together and handles the most data.

Bandwidth - The transmission capacity of a given facility, in terms of how much data the facility can transmit in a fixed amount of time; expressed in bits per second (bps).

Beacon Interval - A beacon is a packet broadcast by the Access Point to keep the network synchronized. A beacon includes the wireless LAN service area, the AP address, the Broadcast destination addresses, a time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator Message (TIM).

Bit - A binary digit. The value - 0 or 1-used in the binary numbering system. Also, the smallest form of data.

Boot - To cause the computer to start executing instructions. Personal computers contain built-in instructions in a ROM chip that are automatically executed on startup. These instructions search for the operating system, load it and pass control to it.

Bottleneck - A traffic slowdown that results when too many network nodes try to access a single node, often a server node, at once.

Bridge - A device that interconnects different networks together.

Broadband - A data-transmission scheme in which multiple signals share the bandwidth of a medium. This allows the transmission of voice, data and video signals over a single medium. Cable television uses broadband techniques to deliver dozens of channels over one cable.

Browser - A browser is an application program that provides a way to look at and interact with all the information on the World Wide Web or PC. The word "browser" seems to have originated prior to the Web as a generic term for user interfaces that let you browse text files online.

BSS (Basic Service Set) - An infrastructure network connecting wireless devices to a wired network using a single access point.

Buffer - A buffer is a shared or assigned memory area used by hardware devices or program processes that operate at different speeds or with different sets of priorities. The buffer allows each device or process to operate without being held up by the other. In order for a buffer to be effective, the size of the buffer and the algorithms for moving data into and out of the buffer need to be considered by the buffer designer. Like a cache, a buffer is a "midpoint holding place" but exists not so much to accelerate the speed of an activity as to support the coordination of separate activities.

CAT 5 - ANSI/EIA (American National Standards Institute/Electronic Industries Association) Standard 568 is one of several standards that specify "categories" (the singular is commonly referred to as "CAT") of twisted pair cabling systems (wires, junctions, and connectors) in terms of the data rates that they can sustain. CAT 5 cable has a maximum throughput of 100 Mbps and is usually utilized for 100BaseTX networks.

CAT 5e - The additional cabling performance parameters of return loss and far-end crosstalk (FEXT) specified for 1000BASE-T and not specified for 10BASE-T and 100BASE-TX are related to differences in the signaling implementation. 10BASE-T and 100BASE-TX signaling is unidirectional-signals are transmitted in one direction on a single wire pair. In contrast, Gigabit Ethernet is bi-directional-signals are transmitted simultaneously in both directions on the same wire pair; that is, both the transmit and receive pair occupy the same wire pair.

Cookie - Data created by a Web server that is stored on a user's computer. It provides a way for the Web site to keep track of a user's patterns and preferences and, with the cooperation of the Web browser, to store them on the user's own hard disk.

CPU (Central Processing Unit) - The computing part of the computer. Also called the "processor," it is made up of the control unit and ALU.

Database - A database is a collection of data that is organized so that its contents can easily be accessed, managed, and updated.

Data Packet - One frame in a packet-switched message. Most data communications is based on dividing the transmitted message into packets. For example, an Ethernet packet can be from 64 to 1518 bytes in length.

Default Gateway - The routing device used to forward all traffic that is not addressed to a station within the local subnet.

Denial of Service - A protocol that directs the network to no longer respond to requests that might arise as the result of a Denial of Service attack.

Denial of Service Attack - An assault on a network that floods it with so many additional requests that regular traffic is either slowed or completely interrupted.

DHCP (Dynamic Host Configuration Protocol) - A protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet's set of protocol (TCP/IP), each machine that can connect to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine. Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

DHCP uses the concept of a "lease" or amount of time that a given IP address will be valid for a computer. The lease time can vary depending on how long a user is likely to require the Internet connection at a particular location. It's especially useful in education and other environments where users change frequently. Using very short leases, DHCP can dynamically reconfigure networks in which there are more computers than there are available IP addresses.

DHCP supports static addresses for computers containing Web servers that need a permanent IP address.

DMZ (Demilitarized Zone) - Allows one IP address (or computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. It is recommended that you set your computer with a static IP address if you want to use DMZ Hosting.

DNS - The domain name system (DNS) is the way that Internet domain name are located and translated into Internet Protocol (IP) addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

Domain - A subnetwork comprised of a group of clients and servers under the control of one security database. Dividing LANs into domains improves performance and security.

Download - To receive a file transmitted over a network. In a communications session, download means receive, upload means transmit.

Driver - A workstation or server software module that provides an interface between a network interface card and the upper-layer protocol software running in the computer; it is designed for a specific NIC, and is installed during the initial installation of a network-compatible client or server operating system.

DSSS (Direct-Sequence Spread Spectrum) - DSSS generates a redundant bit pattern for all data transmitted. This bit pattern is called a chip (or chipping code). Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the receiver can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers. However, to an intended receiver (i.e. another wireless LAN endpoint), the DSSS signal is recognized as the only valid signal, and interference is inherently rejected (ignored).

Dynamic IP Address - An IP address that is automatically assigned to a client station in a TCP/IP network, typically by a DHCP server. Network devices that serve multiple users, such as servers and printers, are usually assigned static IP addresses.

Dynamic Routing - The ability for a router to forward data via a different route based on the current conditions of the communications circuits. For example, it can adjust for overloaded traffic or failing lines and is much more flexible than static routing, which uses a fixed forwarding path.

Encryption - A security method that applies a specific algorithm to data in order to alter the data's appearance and prevent other devices from reading the information.

ESS (Extended Service Set) - A set of more than two or more BSSs (multiple access points) forming a single network.

Ethernet - IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium. Has a transfer rate of 10 Mbps. Forms the underlying transport vehicle used by several upper-level protocols, including TCP/IP and XNS.

Fast Ethernet - A 100 Mbps technology based on the 10Base-T Ethernet CSMA/CD network access method.

FHSS (Frequency Hopping Spread Spectrum) - FHSS continuously changes (hops) the carrier frequency of a conventional carrier several times per second according to a pseudo-random set of channels. Because a fixed frequency is not used, and only the transmitter and receiver know the hop patterns, interception of FHSS is extremely difficult.

Fiber Optic - The medium and the technology associated with the transmission of information as light impulses along a glass or plastic wire or fiber. Fiber optic wire carries much more information over longer distances than conventional copper wire and is far less subject to electromagnetic interference.

Fiber Optic Cable - A transmission medium that uses glass or plastic fibers rather than copper wire to transport data or voice signals. The signal is imposed on the fibers via pulses (modulation) of light from a laser or a light-emitting diode (LED). Because of its high bandwidth and lack of susceptibility to interference, fiber optic cable is used in long-haul or noisy applications.

Finger - A UNIX command widely used on the Internet to find out information about a particular user, such as telephone number, whether currently logged on or the last time logged on. The person being "fingered" must have placed his or her profile on the system. Fingering requires entering the full user@domain address.

Firewall - A firewall is a set of related programs, located at a network gateway server, that protects the resources of a network from users from other networks. (The term also implies the security policy that is used with the programs.) An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources to which its own users have access.

Basically, a firewall, working closely with a router, examines each network packet to determine whether to forward it toward its destination.

Firmware - Code that is written onto read-only memory (ROM) or programmable read-only memory (PROM). Once firmware has been written onto the ROM or PROM, it is retained even when the device is turned off.

Fragmentation - Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

FTP (File Transfer Protocol) - A protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc.). For example, after developing the HTML pages for a Web site on a local machine, they are typically uploaded to the Web server using FTP.

FTP includes functions to log onto the network, list directories and copy files. It can also convert between the ASCII and EBCDIC character codes. FTP operations can be performed by typing commands at a command prompt or via an FTP utility running under a graphical interface such as Windows. FTP transfers can also be initiated from within a Web browser by entering the URL preceded with ftp://.

Unlike e-mail programs in which graphics and program files have to be "attached," FTP is designed to handle binary files directly and does not add the overhead of encoding and decoding the data.

Full Duplex - The ability of a device or line to transmit data simultaneously in both directions.

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.

Hardware - Hardware is the physical aspect of computers, telecommunications, and other information technology devices. The term arose as a way to distinguish the "box" and the electronic circuitry and components of a computer from the program you put in it to make it do things. The program came to be known as the software.

Hop - The link between two network nodes.

HTTP (HyperText Transport Protocol) - The communications protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a Web server and transmit HTML pages to the client browser.

Hub - The device that serves as the central location for attaching wires from workstations. Can be passive, where there is no amplification of the signals; or active, where the hubs are used like repeaters to provide an extension of the cable that connects to a workstation.

ICMP (Internet Control Message Protocol) - Part of the TCP/IP protocol. Network devices such as routers or servers use ICMP to transmit error messages and control messages. For example, the PING program uses ICMP.

IEEE (The Institute of Electrical and Electronics Engineers) - The IEEE describes itself as "the world's largest technical professional society, promoting the development and application of electrotechnology and allied sciences for the benefit of humanity, the advancement of the profession, and the well-being of our members."

The IEEE fosters the development of standards that often become national and international standards. The organization publishes a number of journals, has many local chapters, and several large societies in special areas, such as the IEEE Computer Society.

IGMP (Internet Group Management Protocol) - A multicast host registration protocol that allows any host to inform its local router that it wants to receive transmissions addresses to a specific multicast group. If there is more than one multicast router on a given subnetwork, one of the routers is elected "querier" and assumes the responsibility of keeping track of group membership.

IKE (Internet Key Exchange) - A negotiation and key exchange protocol specified by the Internet Engineering Task Force. An IKE security association (SA) automatically negotiates encryption and authentication keys. With IKE, an initial exchange authenticates the VPN session and automatically negotiates keys that will be used to pass encrypted data over the Internet or any other network.

In-Band Management - Management of the network from a station attached directly to the network.

IP (Internet Protocol) - The method or protocol by which data is sent from one computer to another on the Internet. It is a standard set of rules, procedures, or conventions relating to the format and timing of data transmission between two computers that they must accept and use to be able to understand each other.

IP Address - In the most widely installed level of the Internet Protocol (IP) today, an IP address is a 32-binary digit number that identifies each sender or receiver of information that is sent in packet across the Internet. When you request an HTML page or send e-mail, the Internet Protocol part of TCP/IP includes your IP address in the message (actually, in each of the packets if more than one is required) and sends it to the IP address that is obtained by looking up the domain name in the Uniform Resource Locator you requested or in the e-mail address you're sending a note to. At the other end, the recipient can see the IP address of the Web page requestor or the e-mail sender and can respond by sending another message using the IP address it received.

IPCONFIG - A Windows NT or 2000 utility that provides for querying, defining and managing IP addresses within a network. A commonly used utility for configuring networks with static IP addresses.

IP Multicast Filtering - A process whereby the switch can pass multicast traffic along to participating hosts.

IPSec (Internet Protocol Security) - A suite of protocols used to implement secure exchange of packets at the IP layer. IPSec supports two basic modes: Transport and Tunnel. Transport encrypts the payload of each packet, leaving the header untouched, while Tunnel mode encrypts both the header and the payload and is therefore more secure. IPSec must be supported on both transmitter and receiver and must share a public key. Tunnel mode is widely deployed in VPNs (Virtual Private Networks).

LAN (Local Area Network) - A group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building).

Latency - The time delay between when the first bit of a packet is received and the last bit is forwarded.

Layer 2 - Data Link layer in the International Standards Organization (ISO) 7-Layer Data Communications Protocol, also known as the OSI (Open Systems Interconnection) model. This is a standard model to consult when designing network protocols. Layer 2 is directly related to the hardware interface for network devices and passes traffic based on MAC addresses.

Layer 3 - Network layer in the International Standards Organization (ISO) 7-Layer Data Communications Protocol, also known as the OSI (Open Systems Interconnection) model. This is a standard model to consult when designing network protocols. Layer 3 handles the routing functions for data moving from one open system to another.

MAC (Media Access Control) Address - A unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level.

Mbps (Megabits per second) - One million bits per second; unit of measurement for data transmission.

MDI (Medium Dependent Interface) - On a network hub or switch, a MDI port, also known as an uplink port, connects to another hub or switch using a straight-through cable. To connect a MDI port to a computer, use a crossover cable.

MDIX (Medium Dependent Interface Crossed) - On a network hub or switch, a MDIX port connects to a computer using a straight-through cable. To connect a MDIX port to another hub or switch, use a crossover cable.

MIB (Management Information Base) - A set of database objects. This set contains information about a specific device for utilizing SNMP.

Multicasting - Sending data to a group of nodes instead of a single destination.

Network - A system that transmits any combination of voice, video and/or data between users.

Node - A network junction or connection point, typically a computer or work station.

Out-of-Band Management - Management of the network from a station not attached to the network.

Packet - A unit of data routed between an origin and a destination in a network.

Packet Filtering - Discarding unwanted network traffic based on its originating address or range of addresses or its type (e-mail, file transfer, etc.).

Ping (Packet INternet Groper) - An Internet utility used to determine whether a particular IP address is online. It is used to test and debug a network by sending out a packet and waiting for a response.

Port - A pathway into and out of the computer or a network device such as a switch or router. For example, the serial and parallel ports on a personal computer are external sockets for plugging in communications lines, modems and printers.

Port Mirroring - Port mirroring, also known as a roving analysis port, is a method of monitoring network traffic that forwards a copy of each incoming and outgoing packet from one port of a network switch to another port where the packet can be studied. A network administrator uses port mirroring as a diagnostic tool or debugging feature, especially when fending off an attack. It enables the administrator to keep close track of switch performance and alter it if necessary. Port mirroring can be managed locally or remotely.

Port Trunk - Defines a network link aggregation and trunking method, which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

QoS (Quality of Service) - A wide variety of techniques that prioritizes specific types of network traffic. QoS is used to maximize a network's performance according to its requirements. QoS ensures better service to high-priority types of network traffic, which may involve demanding, real-time applications, such as videoconferencing.

RAID improves performance by disk striping, which interleaves bytes or groups of bytes across multiple drives, so more than one disk is reading and writing simultaneously.

RIP (Routing Information Protocol) - A simple routing protocol that is part of the TCP/IP protocol suite. It determines a route based on the smallest hop count between source and destination. RIP is a distance vector protocol that routinely broadcasts routing information to its neighboring routers.

RJ-45 (Registered Jack-45) - A connector similar to a telephone connector that holds up to eight wires, used for connecting Ethernet devices.

RMON (Remote MONitoring) - RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.

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

SMTP (Simple Mail Transfer Protocol) - The standard e-mail protocol on the Internet. It is a TCP/IP protocol that defines the message format and the message transfer agent (MTA), which stores and forwards the mail.

SNMP (Simple Network Management Protocol) - A widely used network monitoring and control protocol. Data is passed from SNMP agents, which are hardware and/or software processes reporting activity in each network device (hub, router, bridge, etc.) to the workstation console used to oversee the network. The agents return information contained in a MIB (Management Information Base), which is a data structure that defines what is obtainable from the device and what can be controlled (turned off, on, etc.).

Software - Instructions for the computer. A series of instructions that performs a particular task is called a "program." The two major categories of software are "system software" and "application software." System software is made up of control programs such as the operating system and database management system (DBMS). Application software is any program that processes data for the user.

A common misconception is that software is data. It is not. Software tells the hardware how to process the data.

SPI (Stateful Packet Inspection) - A firewall technology that monitors the state of the transaction so that it can verify that the destination of an inbound packet matches the source of a previous outbound request. It examines not just the headers of the packet, but also the contents, to determine more about the packet than just its source and destination information. It is called "stateful" because verifies that the stated destination computer has previously requested the current communication. In this way, it verifies that all communications are initiated by the recipient computer and are taking place only with sources that are known and trusted from previous interactions. In addition to being a more rigorous inspection, stateful packet inspection closes off ports until connection to the specific port is requested. This allows an added layer of protection from the threat of port scanning.

Static Routing - Forwarding data in a network via a fixed path. Static routing cannot adjust to changing line conditions as can dynamic routing.

Storage - The semi-permanent or permanent holding place for digital data.

STP - 1. (Shielded Twisted Pair) Telephone wire that is wrapped in a metal sheath to eliminate external interference. 2. (Spanning Tree Protocol) A technology that checks your network for any loops. A loop can often occur in complicated or back-up linked network systems. Spanning-tree detects and directs data along the shortest path, maximizing the performance and efficiency of the network.

Subnet Mask - The method used for splitting IP networks into a series of subgroups, or subnets. The mask is a binary pattern that is matched up with the IP address to turn part of the host ID address field into a field for subnets.

Swapping - Replacing one segment of a program in memory with another and restoring it back to the original when required.

Switch - 1. A data switch 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 (Transmission Control Protocol) - A method (protocol) used along with the IP (Internet Protocol) to send data in the form of message units (datagram) between network devices over a LAN or WAN. While IP takes care of handling the actual delivery of the data (routing), TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient delivery over the network. TCP is known as a "connection oriented" protocol due to requiring the receiver of a packet to return an acknowledgment of receipt to the sender of the packet resulting in transmission control.

TCP/IP (Transmission Control Protocol/Internet Protocol) - The basic communication language or set of protocols for communications over a network (developed specifically for the Internet). TCP/IP defines a suite or group of protocols and not only TCP and IP.

Telnet - A terminal emulation protocol commonly used on the Internet and TCP/IP-based networks. It allows a user at a terminal or computer to log onto a remote device and run a program.

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

Topology - A network's topology is a logical characterization of how the devices on the network are connected and the distances between them. The most common network devices include hubs, switches, routers, and gateways. Most large networks contain several levels of interconnection, the most important of which include edge connections, backbone connections, and wide-area connections.

TX Rate - Transmission Rate.

UDP (User Datagram Protocol) - A method (protocol) used along with the IP (Internet Protocol) to send data in the form of message units (datagram) between network devices over a LAN or WAN. While IP takes care of handling the actual delivery of the data (routing), UDP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient delivery over the network. UDP is known as a "connectionless" protocol due to NOT requiring the receiver of a packet to return an acknowledgment of receipt to the sender of the packet (as opposed to TCP).

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

Upload - To transmit a file over a network. In a communications session, upload means transmit, download means receive.

UTP - Unshielded twisted pair is the most common kind of copper telephone wiring. Twisted pair is the ordinary copper wire that connects home and many business computers to the telephone company. To reduce crosstalk or electromagnetic induction between pairs of wires, two insulated copper wires are twisted around each other. Each signal on twisted pair requires both wires. Since some telephone sets or desktop locations require multiple connections, twisted pair is sometimes installed in two or more pairs, all within a single cable.

VLAN (Virtual LAN) - A logical association that allows users to communicate as if they were physically connected to a single LAN, independent of the actual physical configuration of the network.

Specifications

Standards	IEEE: 802.1d, 802.1p, 802.1q, 802.3, 802.3ab, 802.3ad, 802.3u, 802.3x, 802.3z
Protocol	CSMA/CD
Ports	4 10/100/1000 Auto MDI/MDIX Ports, Optional 2 1000BaseTX Modules, Optional 2 1000BaseSX Modules
Cabling Type	Category 5 Ethernet Cable, Cat 5e Ethernet Cable
LEDs	Act, 10/100/1000, FDX/COL, FAN, TEMP, Power

Environmental

Dimensions	16.93" x 1.75" x 13.78" (430mm x 44.5mm x 350mm)
Unit Weight	8.82 lbs. (4Kg)
Power	AC 100~240V/75W
Certifications	FCC Class A, CE
Operating Temp	0ºC to 50ºC (32ºF to 122ºF)
Storage Temp	-40ºC to 70ºC (-40ºF to 158ºF)
Operating Humidity	20% to 95% Non-Condensing
Storage Humidity	20% to 95% Non-Condensing

Customer Support

For help with the installation or operation of your ProConnect II® Layer 2 Management 4-Port Gigabit Ethernet Switch, contact Linksys Customer Support at one of the phone numbers or Internet addresses below.

Customer Support	(800) 326-7114
Information	(800) 546-5797
Fax	(949) 261-8868
E-mail	support@linksys.com
Web	http://www.linksys.com
FTP Site	ftp.linksys.com

Linksys Warranty Information

Note: You must have your proof of purchase and a bar-code from the product's packaging on hand when calling. Return requests can not be processed without proof of purchase.

Linksys guarantees that every ProConnect II® Layer 2 Management 4-Port Gigabit Ethernet Switch   is free from physical defects in material and workmanship under normal use for FIVE yeas from the date of purchase. If the product proves defective during this warranty period, contact Linksys Customer Support to obtain a Return Authorization Number. When returning a product, mark the Return Authorization Number clearly on the outside of the package and include your original proof of purchase. All customers outside of the United States of America and Canada shall be held responsible for shipping and handling charges.

IN NO EVENT SHALL LINKSYS' LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCI-DENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE, OR ITS DOCUMENTATION. LINKSYS OFFERS NO REFUNDS FOR ITS PROD-UCTS.

⚠ **Tampering with or disassembling this product voids its warranty.**

Linksys makes no warranty or representation, expressed, implied, or statutory, with respect to its products or the contents or use of this documentation and all accompanying software, and specifically disclaims its quality, perform-ance, merchantability, or fitness for any particular purpose. Linksys reserves the right to revise or update its products, software, or documentation without obligation to notify any individual or entity.

LINKSYS®

http://www.linksys.com

© Copyright 2002 Linksys, All Rights Reserved.

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com